CS 2000 Core Manager Fault Management

What's new in CS 2000 Core Manager Fault Management in SN09

Features changes

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

- The OMDD enhancements robustness feature required the addition of new descriptions for logs SDM338, SDM631, SDM638, SDM639

Other changes

The following additional changes have been made in the documentation:

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

Fault management strategy

The core manager fault management strategy is to provide 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 logs and alarms.

Logs

The Log Delivery application, 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.

The CS 2000 Core Manager provides a network-level view of CS 2000 Core Manager, CS 2000, IW SPM, and MG 4000 fault data through the maintenance interface.

Log Delivery procedures

The following table lists tasks and procedures associated with the Log Delivery system and tools. Use this table to determine what 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 on page 46"
add a TCP, TCP-IN, or file device	"Configuring a CS 2000 Core Manager for log delivery" 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
define the set of logs sent from the CM	"Specifying the logs delivered from the CM to the CS 2000 Core Manager" in the Configuration Management document
delete a log device	"Deleting a device using logroute" in the Configuration Management document
display log records	"Retrieving and viewing log records on page 223"

Table 1 Log Delivery procedures

If you want to	Use procedure
install and configure log delivery service	"Installing and configuring the Log Delivery application" in the Configuration Management document
install and configure the pserver application	Refer to the MDM information for instructions
install the logreceiver tool	"Installing the logreceiver tool on a client workstation" 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 CS 2000 Core Manager for log delivery" in the Configuration Management document • for an existing device, use "Modifying a log device using logroute" in the Configuration Management document
store logs in a file	"Retrieving and viewing log records on page 223"
troubleshoot log delivery problems	"Troubleshooting log delivery problems" in the Fault Management NTP for your core manager.
view logs	"Retrieving and viewing log records on page 223"

SDM logs

Core manager events are recorded by the core manager in a series of log reports. The 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 a 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 can 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 general events related to the operations of the core manager. The following table lists SDM logs.

Table 2 Core manager logs

Log	Trigger	Action
SDM300	The connection from the core manager to the Core or the operating company LAN server(s) is down.	Contact your system administrator or Nortel for assistance.
SDM301	A logical volume is not mirrored.	Check hardware faults as mirroring may be lost due to a hard disk failure on the core manager. ***Note:*** If a disk has just been replaced and brought back in-service, the system can take more than 15 minutes to restore mirroring.
SDM302	The use of a system resource has exceeded its threshold.	Isolate and clear the problem.
SDM303	A core manager application or process has failed more than three times in a day, or has declared itself to be in trouble.	Authorized users can examine the log files in /usr/adm to determine the cause of the process failure. If required, contact your system administrator or Nortel for assistance.

Table 2 Core manager logs

Log	Trigger	Action
SDM304	The Log Delivery application cannot deliver logs to the specified UNIX file.	Use the Log Delivery online commissioning tool (logroute) to verify the existence and validity of the device name. Refer to the following procedures for more information: • "Configuring a CS 2000 Core Manager 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 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 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.
SDM314	A message associated with a specific link is received on a different link. This indicates that the links are not properly connected.	Check for wrongly connected links and correct.
SDM315	The Table Access Service application on the core manager has detected corruption in the Data Dictionary on the Core.	Contact your next level of support with the information provided in the log. The log information contains essential information for identifying the Data Dictionary type that is corrupt.
SDM317	The system has detected a Distributed Computing Environment (DCE) problem.	Contact your next level of support to help determine the cause of the failure.
SDM318	An operational measurements (OM) report was not generated. (The OM report failed to complete within one report interval.)	Contact Nortel.
SDM325	Indicates a lost connection to a Preside network management component.	No action required.
SDM326	Indicates that the connection was lost between the SDM and the Multiservice Data Manager (MDM) for 5-minute or 30-minute performance measurement data transfer.	No action required.
SDM332	Indicates that the system audit completed with failures.	Refer to the procedure “Viewing the system audit report and taking corrective action on page 29”

Table 2 Core manager logs

Log	Trigger	Action
SDM335	Generated if one of the following errors occurs frequently on a DS512 link between the SDM and the message switch (MS): - Bad incoming CRCs - Input overflows - Output Overflows - Code Violations - Bad Outgoing CRCs - Double Nacks - Wait for Send Timeouts - Wait for Ack Timeouts - Wait for Idle Timeouts - Wait for Message Timeouts - Availability of DS512 card (dsv0 or dsv1)	Verify the integrity of the hardware at each end of the fiber.
SDM338	Audit finds that omdata file system usage exceeds 60% or 80%.	No action required.
SDM500	Indicates the initial startup of the core manager. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required.
SDM501	Indicates a core manager state change to in service (InSv). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required.
SDM502	Indicates a core manager state change to manual busy (ManB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required.
SDM503	Indicates a core manager state change to system busy (SysB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure "Clearing a critical APPL alarm on page 269"

Table 2 Core manager logs

Log	Trigger	Action
SDM504	Indicates a core manager state change to in-service trouble (ISTb). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure "Clearing a minor or major APPL SDM alarm on page 286"
SDM505	Indicates a core manager state change to offline (OffL) state. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	No action required.
SDM550	Indicates a core manager node status change. One or more of the following can cause the status change: • core manager node state • hardware device • software component • application	Refer to the corresponding procedure in this document if required. ***Note:*** Log SDM550 is generated on the CM.
SDM600	The connection from the core manager to the Core or the operating company LAN server(s) has been reestablished. This log is generated only after a connectivity failure has been corrected, and not at system startup.	No action required.
SDM601	Mirroring has been reestablished after a logical volume mirroring failure.	No action required.
SDM602	A system software resource has returned below its alarm threshold.	No action required.
SDM603	A fault on a core manager application or process has cleared.	No action required.

Table 2 Core manager logs

Log	Trigger	Action
SDM604	The Log Delivery Application generates this log when the Core generates logs at a higher rate than can be transferred to the Log Delivery Service and the device buffer on the core is too full to accept more logs.	Increase office parameter PER_OPC_LOGDEV_BUFFER_SIZE to its maximum size of 32,000. (For more information about this parameter, refer to the *SuperNode Data Manager Log Report Reference Manual*, 297-5051-840.) If you still continue to receive SDM604 logs after you have increased the size of the parameter, or if large numbers of logs are lost, contact Nortel for assistance.
SDM605	Indicates that logs for a specific application have been lost.	No action required.
SDM608	A system image backup (S-tape) has been completed.	No action required.
SDM609	A hardware device has been returned to the in-service state.	No action required.
SDM614	A crossed link alarm has been cleared.	No action required.
SDM615	The SDM Exception Reporting Application generates a warning report at 8:00 a.m. local time when the system generates thresholded logs within the preceding 24 h.	Use LOGUTIL to disable thresholding for logs indicated in the report.
SDM616	A log delivery connection attempt was rejected.	No action required.
SDM617	A Distributed Computing Environment (DCE) problem is cleared.	No action required.
SDM618	The system generates this log report when the /var logical volume reaches 95% full on the disk.	No action required.

Table 2 Core manager logs

Log	Trigger	Action
SDM619	The OM Access Server has detected a corrupt OM Group during an OM Schema download.	No action required.
SDM620	Reports SDM system performance data such as CPU usage, number of processes, swap space occupancy, and logical volume capacities.	No action required.
SDM621	A split mode upgrade has finished.	No action required.
SDM622	The SDM log delivery application generates this log when the file device reaches its maximum size.	Check if you have configured enough space for the file device. If there is a software error causing the increase of logs, contact Nortel for help.
SDM625	Indicates a re-established connection to a Preside network management component.	No action required.
SDM630	Indicates the start time and completion time of the REX test.	No action required.
SDM631	Indicates that Audit has deleted a file in the closedNotSent directory to make more than 80% available space in the omdata file system.	No action required.
SDM632	Indicates that the system audit failure reported through SDM332 has been cleared.	No action required.
SDM633	Indicates a DS512 link condition change.	No action required.
SDM635	Indicates that the SDM512 link problem has cleared	No action required.
SDM638	Issued when Audit finds that omdata file system usage has gone below 80% or 60%.	No action required.

Table 2 Core manager logs

Log	Trigger	Action
SDM639	Issued when Audit finds that omdata file system usage exceeds 90%.	Audit deletes all of the OM files in the closedSent directory.
SDM650	SDM link maintenance requests the logging of a failed link maintenance action. An example of a link maintenance action is the system testing of a link.	No action required. ***Note:*** Log SDM650 is generated on the CM.
SDM700	Reports a Warm, Cold, or Reload restart or a norestartswact on the core.	No action required.
SDM739	This log prints the ftp user's log-in status.	No action required.
SDMO375	Indicates that OMDD discovered a problem while performing an outbound file transfer and could not ensure that the OM report was transferred downstream.	Contact your next level of support.

SDMB logs

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

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.

Table 3 SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB315	A general software-related problem has occurred.	Contact your next level of support.
SDMB316	One of the following billing processes on the CM has been manually killed: • BUFAUDI • BUFAUDIT • BUFCABKI • BUFDEVP • BUFPROC • BUFRECI • SBCPROCI • SBMTSTRI	Restart the process.
SDMB320	A billing backup-related problem occurred, which affects more than one file.	Ensure that the backup volumes configured for the stream have enough available space.
SDMB321	A billing backup-related problem occurred, which affects one file.	Ensure that the backup volume is not busy or full.
SDMB350	An SBA process has reached a death threshold and made a request to restart. A death threshold occurs after a process has died more than 3 times less than 1 minute apart.	SBA will automatically restart. Wait 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 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 by FTP. If not, set the system up to FTP files or back up files.
	• 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 by FTP. If not, set the system up to FTP files or back up files.
	• 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 by FTP. If not, set the system up to FTP files or back up files.
	• 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 by FTP. If not, set the system up to FTP files or back up files.
	• The SBA cannot close or open a file.	• Check to see if files are being sent by FTP. If not, set the system up to FTP files. If necessary, back up files. Also check file permission for the destination directories.
	• Flush file failed	• Contact your next level of support.
SDMB360	SBA has lost the connection to the Persistent Store System (PSS) and cannot restore it. When this occurs alarm SBAIF is raised.	Contact your next level of support.

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 supports all existing streams, contact Nortel for the latest appropriate software.
SDMB366	Indicates that a problem exists on the SDM. If the installed SBA supports multiple stream record formats, you can continue to process streams of the unlogged formats.	Contact your next level of support.
SDMB367	A trapable Management Information Base (MIB) object was set. The modification of some MIB objects provides notification of failures to the System Manager by way of a trap. Because there is no System Manager, the system logs messages. While most SDM logs report the stream, the logs associated with the MIB do not. Consideration for separate streams is not built into the Automatic Accounting Data Networking System (AMADNS) MIB specification.	Contact your next level of support.
SDMB370	The CDR-to-BAF conversion encountered a problem that prevents it from converting CDR to BAF. When this occurs, alarm NOSC is raised because the BAF record was not generated.	Clear the alarm.

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 this document.
SDMB530	A change in the configuration or status of a stream has occurred.	No action required.
SDMB531	The configuration for backup volumes has been corrected.	No action required.
SDMB550	The SBA has shut down either because the core manager was busied or the SBA was turned off.	Determine the reason SBA shut down.
SDMB600	This generic log provides information for billing system problems.	No action required.
SDMB610	A communication-related problem with the SBA has been resolved.	No action required.
SDMB615	A software-related condition has been resolved.	No action required.
SDMB620	A backup-related problem with the SBA has been resolved.	No action required.
SDMB621	A new backup file has been started.	No action required.
SDMB625	Recovery has started on a backup file.	No action required.
SDMB650	The SBA is restarting one or more of its processes.	No action required.

Table 3 SDM Billing Application (SBA) logs

Log	Trigger	Action
SDMB655	• The state of a billing file has changed. • Disk utilization for a particular stream has dropped below a threshold. • A billing file could not be moved to closedSent.	Contact your next level of support.
SDMB660	A problem related to communications with other SBA features was resolved.	No action required.
SDMB665	A software problem on the Core that prevents the synchronization (downloading) of FLEXCDR data at the core manager.	Restart the Core with a load that supports the SBA enhancements for CDR on the core manager.
SDMB670	Either a CDR-to-BAF conversion process used default values to create a BAF field because a CDR field was missing, or the problem was corrected.	For the missing CDR field(s), determine which are needed to generated the BAF field. Use the BAF field displayed in the log report and refer to the applicable Billing Records Application Guide for a list of the CDR fields associated with each BAF field. Update the CDR to include the missing field.
SDMB675	A problem related to file transfer was resolved.	No action required.
SDMB680	The file transfer mode has changed value.	No action required.
SDMB690	Indicates that an SBAIF alarm has cleared.	No action required.

Table 3 SDM Billing Application (SBA) logs

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

Disabling or enabling/changing the time of the system audit

Purpose

Use this procedure to disable, enable or change the time of the system audit.

Application

Refer to “System audit overview” in the CS 2000 Core Manager Basics document for more information on the system audit.

Action

At the core manager UNIX command line

1 Determine the system audit timing.

If you want to	Do
enable/change the execution time of the system audit	step 2
disable the system audit	step 4

2 Enable/change the execution time of the system audit:

```
# sysaudit -change <value>
```

where:

<value>
is the time in hours and minutes (hh:mm), or default which sets the time to 02:00 AM

Example command input:

```
# sysaudit -change 1:30
```

Example response:

```
The periodic execution of the sysaudit command
is now enabled with a daily execution time of
1:30
```

3 Display the time of the system audit:

```
# sysaudit -time
```

Example response:

```
The periodic execution of the sysaudit command
is scheduled daily at 1:30
```

4 Disable the system audit:

```
# sysaudit -disable
```

Example response:

```
The periodic execution of the sysaudit command
is now disabled.
```

Note: To enable the sysaudit, use the “-change” command as described in step 2.

5 You have completed this procedure.

Collecting DEBUG information using the PLATGATHER 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 platgather
- 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:

```
# platgather
```

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.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.

If you used the	Do
platgather command	step 4 and step 5
FXgather command	step 6 and step 7

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/platgather_<machine_name>_<date_and_time>.tar.Z

  Example
  /var/adm/platgather_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:

```
# platgather
```

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:

```
# platgather
```

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
platgather command	step 7 through step 9
FXgather command	step 10 through step 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.

Performing a system audit

Purpose

The following procedure provides instructions on how to perform a system audit. Refer to “System audit overview” in the CS 2000 Core Manager Basics document for more information on the system audit.

Action

At any workstation or console

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

2 Execute the desired system audit check:

```
# sysaudit -<option>
```

where:

<option>
is one of the following options (refer to the online help text for a brief description of each)

- hw (hardware state)
- eeprom (eeprom state)
- lvm (AIX-LVM subsystem)
- cpu (CPU split-mode integrity)
- isc (intersystem communication)
- sys (system resources)
- all (all of the above checks)

Example command input:

```
# sysaudit -all
```

Example response:

```
sysaudit command is in progress, please wait a
few minutes for it to complete...
```

3 You have completed this procedure. To view the results, refer to procedure Viewing the system audit report and taking corrective action on page 29 in this document.

Viewing the system audit report and taking corrective action

Purpose

The following procedure provides instructions on how to view the results of a system audit and take any necessary corrective action.

Prerequisites

Refer to “System audit overview” in the CS 2000 Core Manager Basics document for more information on the system audit.

Action

At the command line of the core manager

1 Display the system audit report:

```
# sysaudit -report
```

and pressing the Enter key.

Example response

```
*********************************************************
** The starting date is: Thu Nov 21 16:07:22 EST 2002 **
*********************************************************

*** CPU split mode integrity pre-check Thu Nov 21 16:07:22 EST 2002> ***
*** CPU split mode integrity pre-check PASSED ****

*********************************************************
**The completion date is: Thu Nov 32 16:07:28 EST 2002 **
*********************************************************
```

Note: The example above displays the results for the “sysaudit -cpu” command.

2 Determine the status of each check in the report.

If the result of a check indicates	Do
passed	no action is required (you have completed the procedure)
passed with warnings	step 3
failed	step 3

3 Match the message in the sysaudit report with a message in the following table:

Message in sysaudit report	Action
FAILURE: <device name> is in a failed state.	step 5
FAILURE: <disk name> has been recorded with a bogus PVID <PVID>.	Contact your next level of support
FAILURE: autolvfix, lresynclv or mklvcopy is running, while both rootvg and datavg are fully mirrored	Contact your next level of support
FAILURE: cm and telcolan entries are configured on the same IP address.	Contact your next level of support
FAILURE: CPU <cpu_number> is not flushed after the latest split-mode upgrade.	step 21
FAILURE: Failed to access device <device name>.	step 4
FAILURE: Failed to access the content of CPU-<cpu number>.	step 5
FAILURE: Failed to access the SDM hosts file.	Contact your next level of support
FAILURE: Failed to obtain output of the rmt<#> device.	step 4
FAILURE: Failed to obtain the content of physical volumes.	Contact your next level of support
FAILURE: Failed to obtain the content of the <logical volume name> logical volume.	Contact your next level of support
FAILURE: Failed to obtain the content of the <volume group name> volume group.	Contact your next level of support
FAILURE: Failed to obtain the list of filesystems in the <volume group name> volume group.	Contact your next level of support
FAILURE: Failed to obtain the output of the SDM CPU usage.	Contact your next level of support
FAILURE: Failed to obtain the output of the sys0 device	Contact your next level of support

Message in sysaudit report	Action
FAILURE: Filesystem <filesystem name> has stale partitions.	Contact your next level of support
FAILURE: Filesystem <filesystem name> is configured on rootvg, but should be configured on datavg.	Contact your next level of support
FAILURE: Filesystem <filesystem name> is not mounted.	Contact your next level of support
FAILURE: ROOTVG free space is <n> MB. ROOTVG disk upgrade is required.	See *Upgrading the CS 2000 Core Manager*, NN10060461.
FAILURE: The <user> user is not configured on the system.	Contact your next level of support
FAILURE: The autoboot attribute of CPU-<cpu_number> is NOT set, for autoboot to be ON vb=Y.	Contact your next level of support
FAILURE: The autorestart attribute of the sys0 device is set to false, it should be set to true.	Contact your next level of support
FAILURE: The block_size attribute of the rmt<#> device is currently set to <value>, but should be set to 512.	step 16
FAILURE: The cms_notify_attr attribute of sys0 device is not set to the appropriate value.	step 29
FAILURE: The cms_notify_meth attribute of sys0 device is not set to the appropriate value.	step 27
FAILURE: The hosts file is configured with more than one <entry name> entry.	Contact your next level of support.
FAILURE: The Imp process is not running on the system	Contact your next level of support.
FAILURE: The isc_sp process is currently running, although the split mode upgrade is not in progress.	step 18

Message in sysaudit report	Action
FAILURE: The maxmbuf attribute of the sys0 device is currently set to <value>, but should be set to 0.	step 10
FAILURE: The maxpout attribute of the sys0 device is currently set to <value>, but should be set to 31.	step 12
FAILURE: The maxuproc attribute of the sys0 device is currently set to <value>, but should be set to 500.	step 8
FAILURE: The minpout attribute of the sys0 device is currently set to <value>, but should be set to 15.	step 14
FAILURE: The mount point and label for logical volume <logical volume name> do not match.	step 23
FAILURE: The process with <process ID> is expected to be a runaway process.	Contact your next level of support
FAILURE: The quorum attribute of volume group <volume group name> is set to yes.	Contact your next level of support
FAILURE: The sam process is not running on the system	Contact your next level of support
FAILURE: The smm process is not running on the system	Contact your next level of support
FAILURE: The snc process is not running on the system	Contact your next level of support
FAILURE: The value of thewall is not set to the correct value and is set to <value>.	Contact your next level of support.
FAILURE: Volume group <volume group name> is not fault tolerant.	Contact your next level of support
FAILURE: Volume group <volume group name> is not mirrored.	Contact your next level of support

Message in sysaudit report	Action
WARNING: <device name> is currently integrating.	No action required
WARNING: <device name> is currently offline.	step 31
WARNING: <device name> is in an integrating state.	No action required
WARNING: CPU-0 is not online	step 5
WARNING: CPU-2 is not online	step 5
WARNING: Failures are recorded in the eeprom of module <module name>.	Contact your next level of support
WARNING: Faults are recorded in the output of the “querysdm flt” command. Please execute the “querysdm flt” command for specifics on these faults.	Execute the “querysdm flt” command
WARNING: HW module located in slot <slot number> is not available.	step 5
WARNING: ROOTVG free space is <n> MB. ROOTVG disk upgrade is recommended, future upgrades might fail.	See *Upgrading the CS 2000 Core Manager*, NN10060461.
WARNING: The system is experiencing major disk access delays.	Contact your next level of support.
WARNING: The system is experiencing unbalanced disk access problems.	Contact your next level of support.
WARNING: The system is operating under a heavy load.	Contact your next level of support
WARNING: The system is operating under an extreme load.	Contact your next level of support
WARNING: The system is operating under full capacity.	Contact your next level of support
WARNING: Volume group <volume group name> is integrating.	No action required

4 Determine if there are hardware errors.

If	Do
the hardware module that corresponds to the rmt<#> or <device name> is in a failed state (tracked and reported in the HW check)	step 5
no hardware failures are reported in the sysaudit report	Contact your next level of support

5 Access the hardware level and verify the status of the device:

```
# sdmmtc hw
```

If the device is	Do
marked as “F” (failed)	Replace the hardware module using the corresponding procedure in this document. When complete, go to step 32 of this procedure
not marked as “F” (failed)	step 6

6 Exit the maintenance interface:

```
> quit all
```

7 Further verify if any failures exist:

```
# lsstate -f
```

If	Do
no failures are reported	step 32
failures are reported	Contact your next level of support

8 Reset the maxuproc value:

```
# chdev -l sys0 -a maxuproc=”500”
```

9 Verify that the maxuproc value has been changed:

```
# lsattr -El sys0
```

If the maxuproc value is	Do
set to 500	step 32
not set to 500	Contact your next level of support.

10 Reset the maxmbuf value:

```
# chdev -l sys0 -a maxmbuf="0"
```

11 Verify that the maxmbuf value has been changed:

```
# lsattr -El sys0
```

If the maxmbuf value is	Do
set to 0	step 32
not set to 0	Contact your next level of support.

12 Reset the maxpout value:

```
# chdev -l sys0 -a maxpout="31"
```

13 Verify that the maxpout value has been changed:

```
# lsattr -El sys0
```

If the maxpout value is	Do
set to 31	step 32
not set to 31	Contact your next level of support.

14 Reset the minpout value:

```
# chdev -l sys0 -a minpout="15"
```

15 Verify that the minpout value has been changed:

```
# lsattr -El sys0
```

If the minpout value is	Do
set to 15	step 32
not set to 15	Contact your next level of support.

16 Set the block size to 512:

```
# chdev -l rmt <domain_no> -a block_size="512"
```

where:

<domain_no>
is the number of the domain (either 0 or 1)

17 Verify that the block size value has been changed:

```
# lsattr -El rmt <domain_no>
```

where:

<domain_no>
is the number of the domain (either 0 or 1)

If the block size value is	Do
set to 512	step 32
not set to 512	Contact your next level of support.

18 Stop the isc by first ensuring that the split-mode process is not currently running on the system:

Note: Stop the isc process only if the split-mode process is not currently running.

```
# ps -ef|grep soup
```

If the split-mode process is	Do
running	step 32
not running	step 19

19 Terminate the process:

```
# spstop
```

20 Verify the process was stopped:

```
# ps -ef|grep isc_sp
```

Note: If the system response is similar to the one below, the process has not been terminated.

Example response:

```
root 6830 4910 0 08:46:41 - 0:00 /usr/sbin/isc_sp
root 18600 20578 1 12:07:09 pts/0 0:00 grep isc/sp
```

If the isc process is	Do
no longer running	step 32
still running	Contact your next level of support.

21 Refresh the data on the affected CPU:

`# restart -c <cpu> -z`

where:

<cpu>
is the number of the CPU (either 0 or 2)

22 Verify the CPU has been flushed:

`# restart -c <cpu>`

Where:

<cpu>
is the number of the CPU (either 0 or 2)

If all the values of the CPU	Do
are "_"	step 32
are not "_"	Contact your next level of support

23 Match the label and mount point: display the details of the affected logical volume:

`# lslv <logical volume_name>`

where:

<logical volume_name>
is the name of the logical volume that has a mismatch between the mount point and label

Example response:

```
LOGICAL VOLUME:  lv01                    VOLUME GROUP: datavg
LV IDENTIFIER:   002e43cd61b073d9.2      PERMISSION    read/write
VG STATE:        active/complete         LV STATE:     opened/syncd
TYPE:            jfs                     WRITE VERIFY: off
MAX LPs:         512                     PP SIZE:      16 megabyte(s)
COPIES:          2                       SCHED POLICY: parallel
LPs:             126                     PPs:          252
STALE PPs:       0                       BB POLICY:    relocatable
INTER-POLICY:    minimum                 RELOCATABLE:  yes
INTRA-POLICY:    middle                  UPPER BOUND:  32
MOUNT POINT:     /data                   LABEL:        /data
MIRROR WRITE CONSISTENCY: on
EACH LP COPY ON A SEPARATE PV ?: yes
```

24 Note the Mount point and Label for the logical volume.

Note: The example above shows a mismatch between the mount point and label for logical volume “lv01”.

If the mount point and label	Do
match	step 32
do not match	step 25

25 Change the label to match the mount point:

`# chlv -L “<mount point>” <volume_name>`

where:

<mount point>
is the name of the mount point, for example, “/data”

<volume_name>
is the name of the logical volume that has a mismatch between the mount point and label

Example command:

`# chlv -L ”/data” lv01`

26 Re-display the details for the logical volume to ensure the change was made:

`# lslv <volume_name>`

where:

<volume_name>
is the name of the logical volume for which you changed the label

Example response:

```
LOGICAL VOLUME:  lv01                    VOLUME GROUP: datavg
LV IDENTIFIER:   002e43cd61b073d9.2      PERMISSION    read/write
VG STATE:        active/complete         LV STATE:     opened/syncd
TYPE:            jfs                     WRITE VERIFY: off
MAX LPs:         512                     PP SIZE:      16 megabyte(s)
COPIES:          2                       SCHED POLICY: parallel
LPs:             126                     PPs:          252
STALE PPs:       0                       BB POLICY:    relocatable
INTER-POLICY:    minimum                 RELOCATABLE:  yes
INTRA-POLICY:    middle                  UPPER BOUND:  32
MOUNT POINT:     /data                   LABEL:        /data
MIRROR WRITE CONSISTENCY: on
EACH LP COPY ON A SEPARATE PV ?: yes
```

If the mount point and label	Do
match	step 32
do not match	Contact your next level of support

27 Reset the “cms_notify_meth” attribute:

```
# chdev -l sys0 -a
cms_notify_meth=”/sdm/mtce/smm/smm_cms_notify”
```

28 Verify the attribute value changed:

```
# lsattr -El sys0
```

If the value	Do
changed	step 32
did not change	Contact your next level of support

29 Reset the “cms_notify_attr” attribute:

```
# chdev -l sys0 -a
cms_notify_attr=”condition,req_condition”
```

30 Verify the attribute value changed:

```
# lsattr -El sys0
```

If the value	Do
changed	step 32
did not change	Contact your next level of support

31 Determine why the device is offline. It may either need to be:

- replaced (replace using the corresponding procedure in this document), or
- returned to service if already replaced

32 Use the following table to determine your next step.

If you have	Do
resolved all the failures	Clear the sysaudit alarm using the procedure Clearing a system audit alarm on page 267 in this document
not resolved all the failures	step 3

33 You have completed the procedure.

Disabling or enabling a backup Required alarm

Purpose

Use this procedure to disable or enable a backup Required alarm.

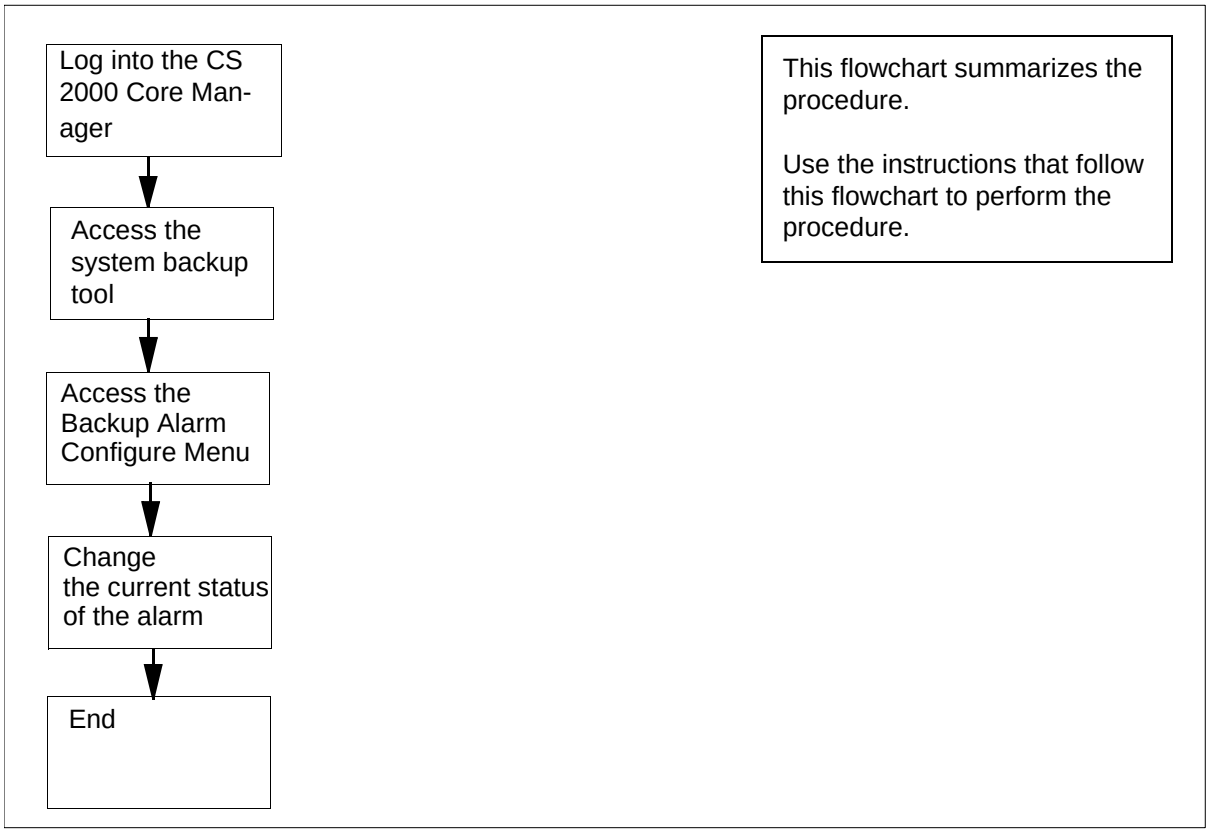
The system generates a backup Required alarm whenever any change occurs to the CS 2000 Core Manager environment (for example, a patch is applied or a logical volume changes). If you do not wish to clear the alarm manually, or to initiate a system backup every time a change occurs, you can disable the backup Required alarm.

Note: Even if you disable the backup Required alarm, the backup In Progress and backup Failed alarms will still be generated.

Action

The following task flow diagram provides an overview of the process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of disabling or enabling a backup Required alarm



Procedure

Disabling or enabling a backup Required alarm

At the VT100 console

1 Log into the CS 2000 Core Manager as the root user.

2 Access the system backup tool:

```
# sysbkup
```

Example response

```
System Image Backup and Restore Menu

0. Exit
1. Help
2. Backup & Restore System image
3. Alarm Configure

Please enter your selection (0 to 3) ? ==>
```

3 Access the Backup Alarm Configure Menu:

```
> 3
```

Example response

```
The current alarm status is: Enabled

You want to Disable it?

Please Enter your selection [y/n] ==>
```

4 Change the current status of the alarm:

```
> y
```

Note: If you do not want to change the current status of the alarm, enter **n**. Go to step 6.

Example response

```
The current alarm status is: Enabled

You want to Disable it? y

Confirm ? ...[y/n] ==>

Please Enter your selection [y/n] ==>
```

5 Confirm your command:

```
> y
```

Note: If you wish to abort your command, enter **n**.

6 The system returns to the System Image Backup and Restore Menu.

If you wish to make more changes, repeat steps 3 through 5 for each change you wish to make. Otherwise, continue the procedure.

7 Exit the system backup tool:

```
> 0
```

8 You have completed this procedure.

Performing a REX test

Purpose

The following procedure provides instructions on how to execute a REX test and view the results.

Application

Refer to “Routine exercise (REX) test overview” in the CS 2000 Core Manager Basics document for more information on the REX test.

Action

At any workstation or console

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

2 Execute the desired REX test:

```
# sdmrex <option>
```

where:

<option>
is one of the following options (refer to the online help text for a brief description of each)

- cpu
- ethr
- all (both the CPU and Ethernet tests)

Note: The Ethernet test requires a configured edge node. Refer to the procedure to configure edge nodes in the SDM Configuration Management document.

Example command input:

```
# sdmrex cpu
```

Example response:

```
executing CPU Rex test...
CPU is integrating. Pls wait for a few
minutes...
```

3 Access the /var/adm directory:

```
# cd /var/adm
```

4 View the rexresultlog file:

```
# view rexresultlog
```

Example response:

```
*****************************************
Mon Dec 9 07:17:17 CST 2002
SDM REX started

Mon Dec 9 07:17:18 CST 2002
Ethernet REX
RC: 0 <Test Passed>
Domain: 0
Link: N/A
Reason: SWACT Ethernet passed (ETH1)

Mon Dec 9 07:17:18 CST 2002
==== Rex Outcome for Ethernet REX: 0 <Test
Passed> ====

Mon Dec 9 07:17:18 CST 2002
SDM REX complete
*****************************************
```

If	Do
no failures are reported	you have completed this procedure
failures are reported	contact your next level of support

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

Purpose

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

Application

The TCP and TCP-In log devices can be accessed from either a local, or a remote location (console). The following procedures describe how to access these log devices from a remote location. These procedures can be used when you are performing the related procedures listed in the table Remote access to log devices procedures on page 46.

Remote access to log devices procedures

Log device	Procedure	Applies to
TCP	Accessing a TCP device from a remote location	“Configuring a core manager for log delivery” in the Configuration Management document Displaying or storing log records using logreceiver on page 69
TCP-IN	Accessing a TCP-IN device from a remote location	“Configuring a core manager for log delivery” in the Configuration Management document “Deleting a device using logroute” in the Configuration Management document

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

Procedure

Accessing a TCP device from a remote location

At the remote workstation

1 Start the logreceiver tool:

`logreceiver <port_number>`

where:

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

2 Continue with the desired procedure listed in the table Remote access to log devices procedures on page 46.

3 You have completed this procedure.

Accessing a TCP-IN device from a remote location

At the remote workstation

1 Use telnet to access the core manager:

`telnet <ip_address> <port_number>`

where:

<ip_address>
is the address of the core manager

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

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

3 Start the logroute tool:

`logroute`

4 Continue with the desired procedure from the table Remote access to log devices procedures on page 46.

5 You have completed this procedure.

SBA alarm troubleshooting

Purpose

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

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

Application

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

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

A problem in the FTP process

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

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

Insufficient amount of storage

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

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

- Verifying the file transfer protocol on page 402
- Verifying the FTP Schedule on page 409

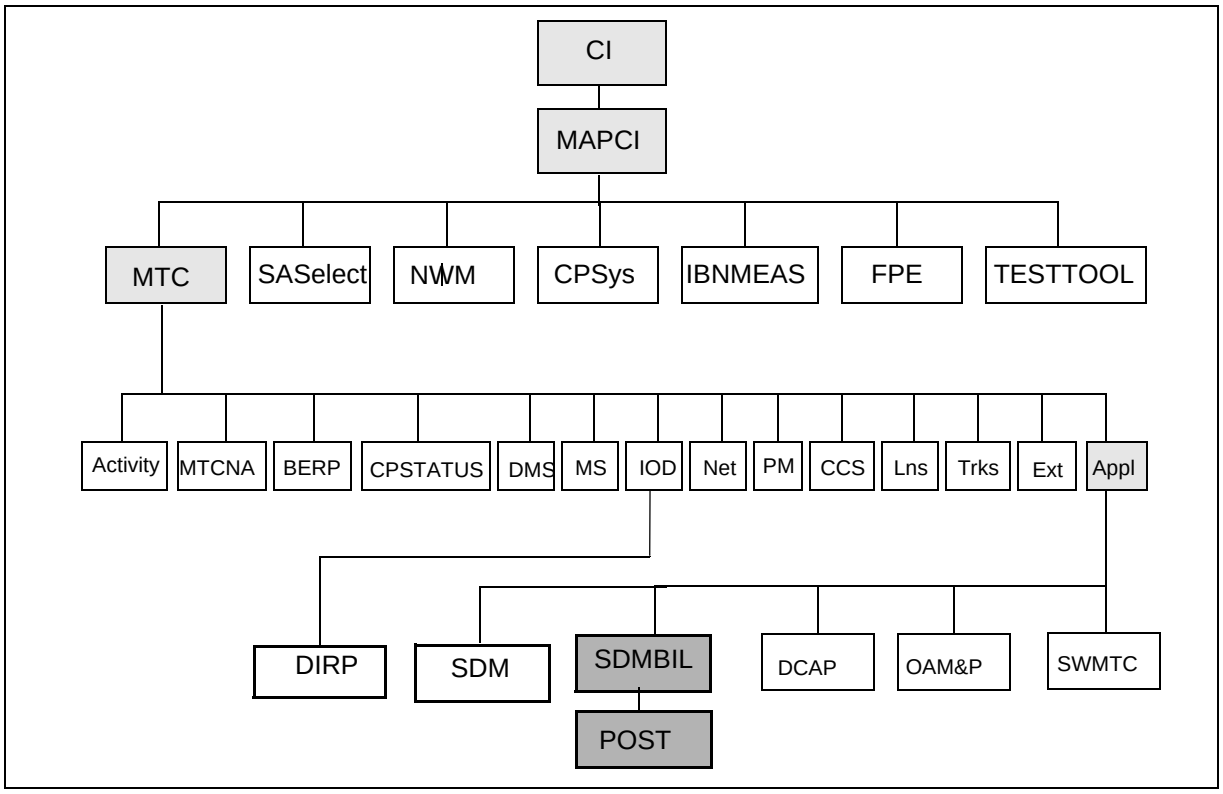
Use the following procedures to clear alarms based on communication problems between the core and the core manager:

- Clearing a DSKWR alarm on page 328
- Clearing a NOCOM alarm (Applicable to the CS 2000 Core Manager and the Core and Billing Manager 800)
- Clearing a major SBACP alarm on page 389
- Clearing a minor SBACP alarm on page 392

APPL Menu level alarms

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

Alarms layout



Maintenance for SBA

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

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

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

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

Alarm severity

There are three levels of severity for SBA alarms:

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

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

CM MAP states

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

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

where

<stream_name> is the name of the stream

The possible state values and their definition are as follows:

- Offline pending (OffP):
  the stream has been turned off and is waiting for the core manager to complete processing its data
- Offline (OffL):
  the stream is offline
- Manual busy (ManB):
  the stream has been manually busied by a user from the CM; data is being written to backup files
- System busy (SysB):
  the stream has been busied by the SBA system due to a communications or internal software error; data is being written to backup files
- Remote busy (RBsy):
  the stream has been busied by the SBA system due to a communications or internal software error; data is being written to backup files
- Backup (Bkup):
  the stream is writing data to backup files due to performance and communication problems
- Recovery (Rcvy):
  the stream is in service and is also sending backup files previously created to the core manager
- In-service (InSv):
  the stream is in a normal working state
- In-service trouble (ISTb):
  the core manager communication is in service trouble because it is 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 402 helps you determine that the FTP process is configured correctly and is able to transfer files
- Verifying the FTP Schedule on page 409 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 310
- Clearing a BAK70 alarm on page 314
- Clearing a BAK90 alarm on page 318
- Clearing a BAKUP alarm on page 322
- Clearing a NOBAK alarm on page 357
- Clearing a NOREC alarm on page 370
- Clearing a NOSTOR alarm on page 372
- Clearing a NOVOL alarm on page 376

Clearing zombie processes

Purpose

Use this procedure to clear zombie processes.

Application

When the MTX is aborted back to software release MTX10 from MTX11, the threshold for the number of zombie processes in the SDMMTC SYS level of the Communication Server 2000 Core Manager (CS 2000 Core Manager) is exceeded.The CS 2000 Core Manager must be manually busied and returned to service after an ABORT SWACT if the threshold is exceeded.

Use this procedure when the CS 2000 Core Manager contains the SDMX11 load.

Action

Use the following procedure to clear zombie processes after an ABORT SWACT.

Clearing zombie processes

At any workstation or console

1 Log in to the SDM as either root or maint user.

2 Access the SYS level menu:

```
# sdmmtc sys
```

Example response:

```
# Description                    Current / Threshold
1    CPU (run queue entries):        0 /   5
2    Number of Processes:           82 / 250
3    Number of Zombies:              4 /   3 !
4    Number of Swap Queue Entries:   0 /   2
```

In this response, the **current** number of zombies is **4** and the zombie **threshold** is **3**. Because the threshold has been exceeded in this example, an exclamation mark (**!**) also appears.

3 Look for the current number of zombie processes.

If the threshold	Do
has been exceeded	step 4
has not been exceeded	step 7

4 Access the APPL level menu:

```
# appl
```

Example response:

```
 2            # Application                    State
 3            1 Table Access Service           .
 4 Logs       2 OM Access Service              .
 5            3 Generic Data Delivery          .
 6            4 Secure File Transfer           .
 7 Bsy        5 Image Dump Service           OffL
 8 RTS        6 Log Delivery Service         OffL
 9 OffL       7 SDM_SBA MTX Application        .
10            8 OM Delivery                    .
11            9 DMS DataServer                 .
12 Up        10 OM Mass Export                 .
```

5 Busy the SDM_SBA MTX Application:

```
# bsy <application_number>
```

where:

<application_number> is the Application number of the SDM_SBA MTX Application. The number of an application can vary by configuration.

Example command:

```
# bsy 7
```

6 Return the SDM_SBA MTX application to service:

```
# rts <application_number>
```

where:

<application_number> = the menu number of the SDM_SBA MTX Application. The number of an application can vary by configuration.

Example command:

```
# rts 7
```

7 You have completed this procedure.

Displaying SBA alarms

Purpose

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

Application

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

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

Prerequisites

Logging on to the CS 2000 Core Manager

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

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

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

Logging on to the Core and Billing Manager

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

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

Procedure

Displaying SBA alarms

At any workstation or console

1 Log into the core manager. Refer to Prerequisites for details.

2 Access the billing maintenance interface:

```
billmtc
```

3 Display the alarms:

```
dispal
```

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

4 You have completed this procedure.

Displaying SBA log reports

Purpose

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

Application

The MIB parameter “sendBillingLogsToCM” affects the displogs command.

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

Prerequisites

Logging on to the CS 2000 Core Manager

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

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

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

Logging on to the Core and Billing Manager

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

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

Procedure

Displaying SBA logs

At any workstation or console

1 Log into the core manager. Refer to Prerequisites for details.

2 Access the billing maintenance interface:

```
billmtc
```

3 Display the logs:

```
displogs
```

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

4 You have completed this procedure.

Cleaning the DAT drive

Purpose

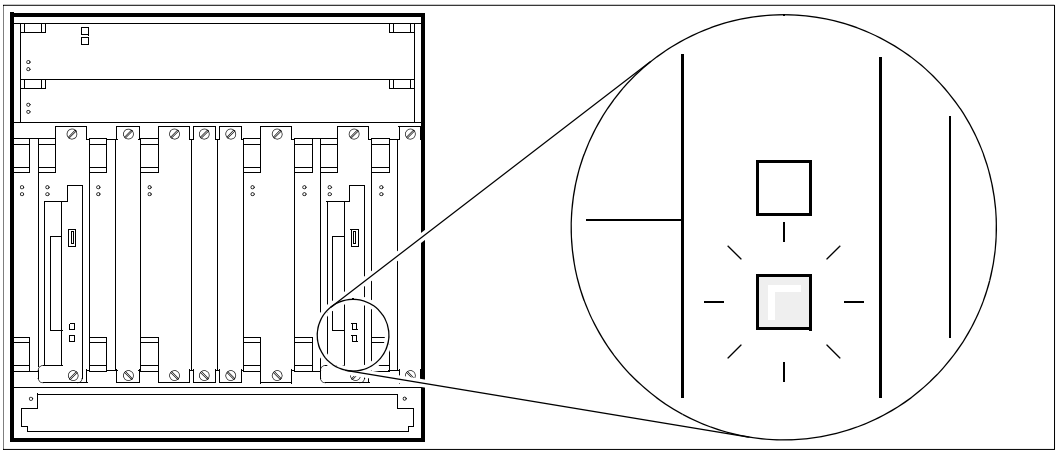
Use this procedure to clean the digital audio tape (DAT) drive in an NTRX50FQ I/O controller module.

Application

Clean the DAT drive using an appropriate DAT drive cleaning cartridge such as the Maxell cleaning cartridge (part number HS-4/SL) or equivalent. Refer to the documentation that accompanies the cleaning cartridge for additional information about its use, and the life expectancy of the cleaning tape.

Clean the tape drive heads after the first four hours of tape movement of a new cartridge, and then after each 25 hours of use.

DAT drive detail



A slowly flashing green LED can indicate that the tape is damaged or needs replacing. If the LED continues to flash after you have cleaned the DAT drive, replace the cleaning cartridge.

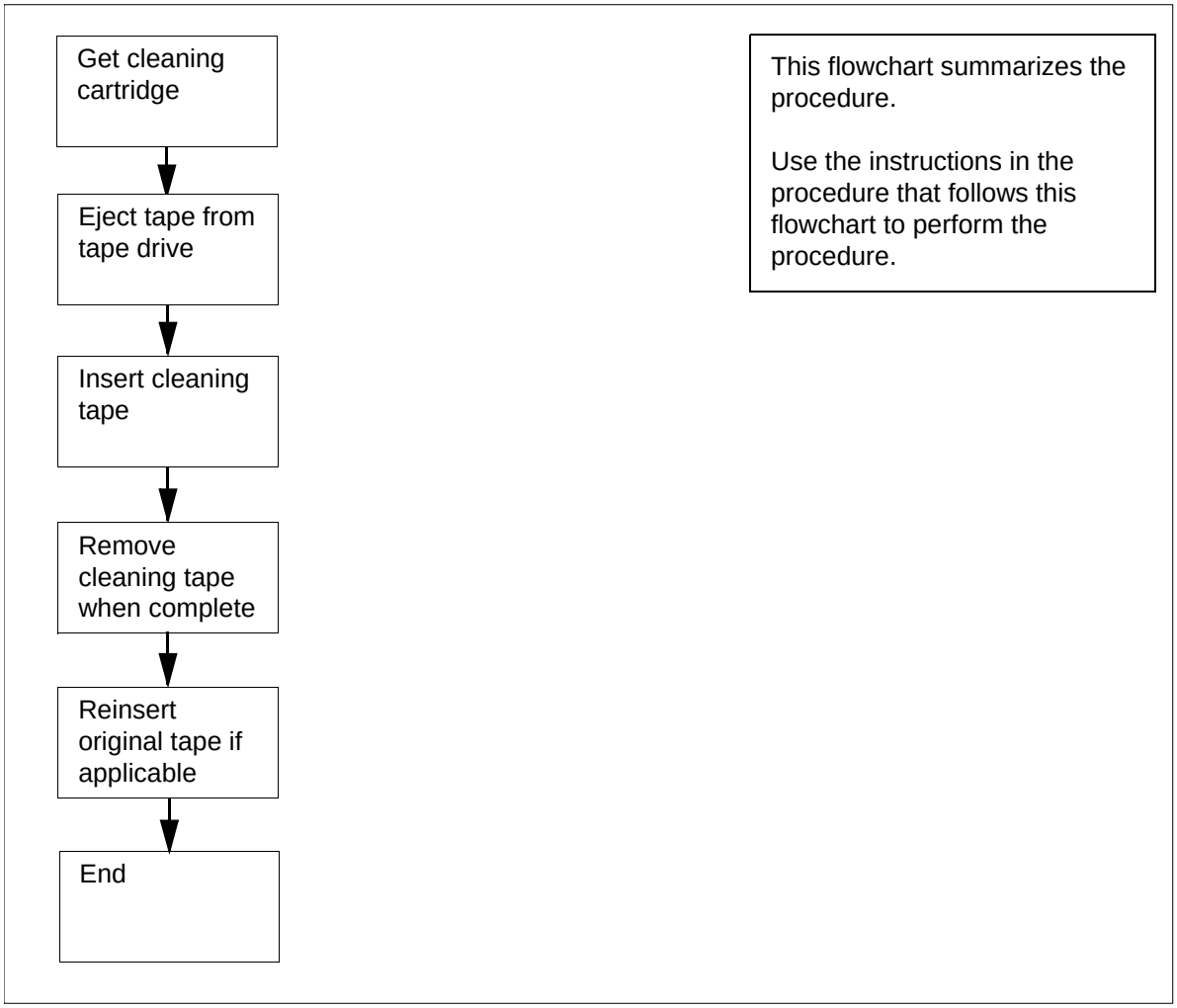
- a solid green LED indicates that a tape is inserted with no errors.
- slowly flashing green and amber LEDs indicates that a prerecorded audio cartridge is inserted and is being played automatically.
- a rapidly flashing green LED indicates that the drive cannot write to the tape correctly. Clean the DAT drive.
- a solid amber LED indicates that the drive is reading or writing the tape.
- a rapidly flashing amber light indicates that a hardware fault has occurred.

Note: A flashing LED does not affect operations, and does not indicate that data has been lost.

Action

This procedure contains a summary flowchart as an overview of the procedure. Follow the specific steps to perform this procedure.

Summary of cleaning the DAT drive



Cleaning the DAT drive

At the I/O Controller Module

1 Obtain a cleaning cartridge (Maxell part number HS-4/CL or equivalent).

2 Press the eject button on the DAT drive, and remove the tape cartridge, if applicable.

3 Insert the cleaning cartridge into the DAT drive.

Note: Cleaning begins automatically. When cleaning is complete, the cartridge is automatically ejected.

4 Remove the cartridge from the DAT drive.

5 If applicable, reinsert the tape that you removed in step 2.

6 You have completed this procedure.

Controlling the SDM Billing Application

Purpose

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

Application

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

Action

At any workstation or console

1 Log in to the core manager.

2 Access the Application level:

```
# sdmmtc appl
```

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

Example response:

```
# Application                                    State
1 Enhanced Terminal Access                         .
2 Log Delivery Service                             .
3 OM Access Service                                .
4 OM Delivery                                      .
5 Generic Data Delivery                            .
6 Secure File Transfer                             .
7 GR740 Pass Through                               .
8 SDM Billing Application                          .
```

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 SBA:

> bsy <SBA_no>

where:

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

Example response:

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

4 Confirm the busy command:

> y

If the SBA	Do
busied successfully and you want to return the SBA to service	step 5
busied successfully but you do not want to return the SBA to service at this time	step 14
did not busy successfully	contact your next level of support

5 Return the SBA to service:

> rts <SBA_no>

where:

<SBA_no>
is the number next to the SDM 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 if 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 Check for Log SDMB375.

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

7 Perform step 8 through step 13 to return the RTB streams to service:

8 Exit the application level:

```
> quit all
```

9 Access the billing maintenance level:

```
# billmtc
```

10 Access the schedule level:

```
> schedule
```

11 Access the real-time billing level:

```
> rtb
```

12 Busy the stream:

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

where:

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

13 Return the stream to service:

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

where:

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

If the billing stream configured for RTB	Do
returns to service successfully	step 14
does not return to service successfully	contact your next level of support

14 Quit the billing maintenance level:

```
> quit all
```

15 You have completed this procedure

Disabling and enabling dcemonitor

Purpose

Use this procedure to disable or enable the dcemonitor software.

This procedure prevents dcemonitor from restarting and killing DCE daemons by suspending these operations for 1 hour. After 1 hour, dcemonitor resumes these activities.

Application

ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator.

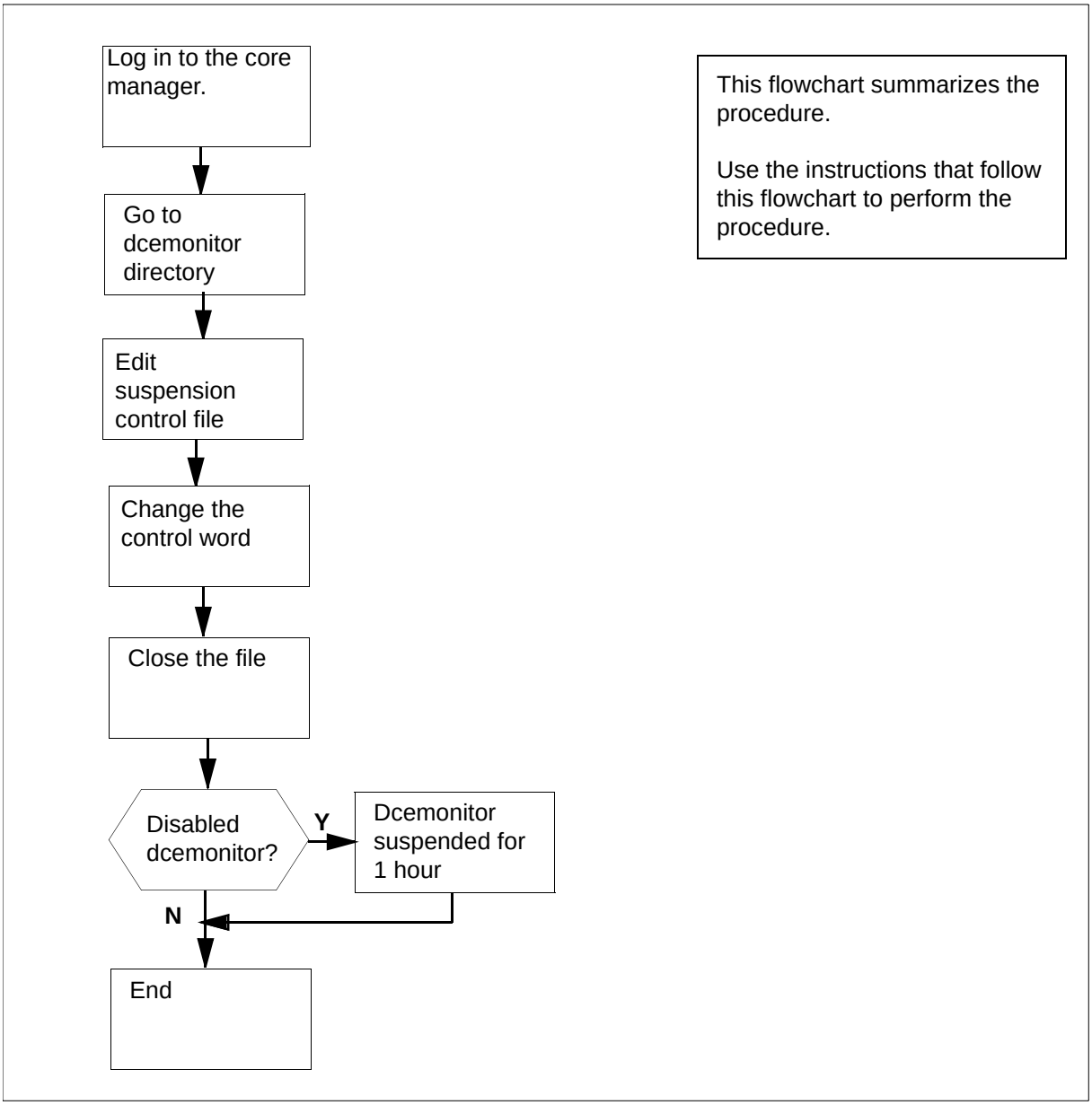
If dcemonitor cannot solve a service-affecting DCE problem, it kills the DCE daemons using /etc/dce.clean, and restarts them using /etc/rc.dce. If this does not solve the problem, dcemonitor waits 3 minutes, and repeats these operations, indefinitely.

The “DCE Monitor present action:” line in the dce_mon_status file is configured as “restart” if dcemonitor is doing recovery by restarts. If dcemonitor constantly kills DCE daemons, the DCE environment on the core manager becomes unstable. This can seriously impair your ability to fix the original problem.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of disabling and enabling dcemonitor



Disabling and enabling dcemonitor

At the local VT100 console or remote client workstation

1 Log in to the core manager as the root user.

2 Access the dcemonitor data directory:

```
# cd /sdm/configdata/dce
```

3 Edit the dcemonitor suspension control file. For example:

```
# vi dce_mon_suspend
```

This file contains one word.

4 Determine dcemonitor status.

If you want to	Do
enable dcemonitor	step 5
disable dcemonitor	step 7

5 To enable dcemonitor, modify the control word:

```
cw
```

The word suspend is replaced by “suspen$”.

6 Enable dcemonitor by changing the activation control word:

```
active
```

The $ from “suspen$” remains.

Go to step 9.

7 To disable dcemonitor, modify the control word:

```
cw
```

The word active is replaced by “activ$”.

8 Disable dcemonitor:

```
suspend
```

9 Close the file by pressing the Esc key and enter:

```
: wq
```

Dcemonitor stops killing and restarting DCE daemons for one hour.

Note: After an hour dcemonitor continues to restart and kill DCE daemons. The “active$” and “$” disappear when you press the Esc key.

10 You have completed this procedure.

Displaying or storing log records using logreceiver

Purpose

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

Application

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

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

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

Storage file

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

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

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

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

Procedure

Checking the port numbers in use on a workstation

At the client workstation

1 Check the port numbers in use:

```
> more/etc/services
```

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

Storing logs in a file

At the client workstation

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

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

where

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

<filename> is the name of the file

Displaying log records on a workstation

At the client workstation

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

```
logreceiver <port>
```

where

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

2 You have completed this procedure.

Logging a session to an output file

Purpose

Use this procedure to log a session to an ASCII output file.

Action

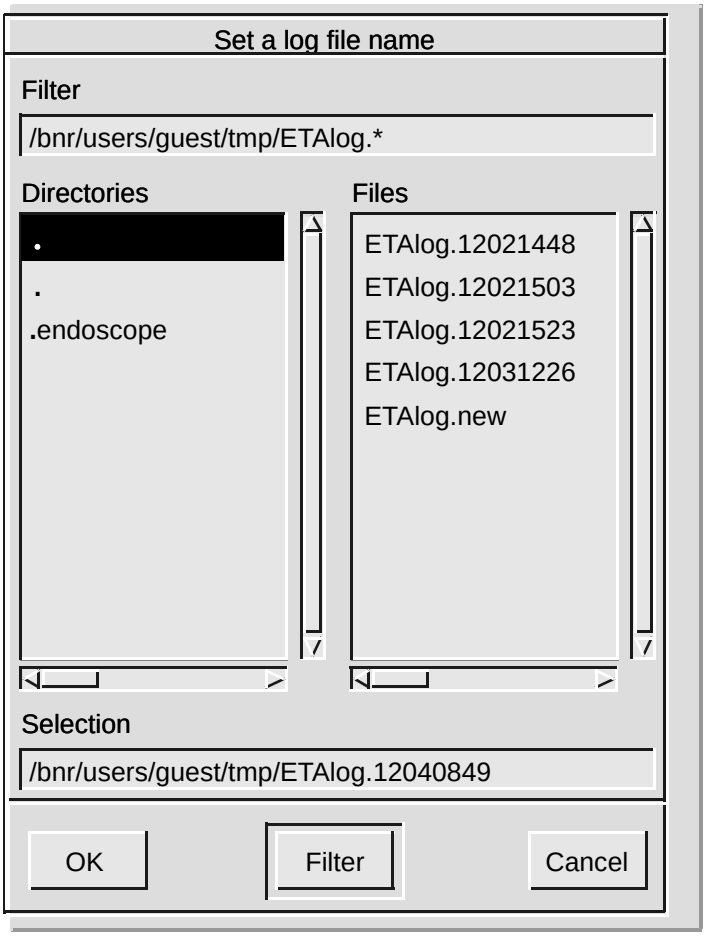
Logging a session to an output file

At your work station

1 Use the ETA client application to access the core manager or Core.

2 From the File menu in the SDM or CI/MAP Session window, select the Start logging to file... menu item.

The Set a log file name dialog appears.



Note: You are prompted for the file name. Accept the default file name in the current directory. Delete the files in the current directory that are no longer required. An error can occur if you do not have read and write permission in the specified directory.

If you want to	Do
select the default file name	step 3
select an existing file name in the current directory	step 5
specify a new file name	step 8

3 Select the default file name by clicking OK.

A message appears in the status area at the bottom of the SDM Session window. The message indicates that the output is being logged to a file.

Note: The default file name appears under the Selection heading in the Set a log file name window. The default file name format is ETAlog.mmddhhmm, where mmddhhmm is the current month, day, hour, and minute.

In the example in step 2, Logging to file /bnr/users/guest/tmp/ETAlog.12040849 indicates that

- /bnr/users/guest/tmp is the directory where the file is located
- ETAlog is the file prefix, and
- 12040849 is the file extension

The file extension indicates that the file was opened on December 4 (1204), at 8:49 a.m. (0849).

4 Go to step 9.

5 Select an existing file name by clicking on a file name displayed under the Files heading in the Set a log file name window.

Note: If you choose an existing file name, the new session output is appended to the existing file.

6 Click OK.

7 Go to step 9.

8 Enter a new file name in the Selection heading area of the Set a log file name window. Position the cursor on the default file name extension mmddhhmm, and press backspace to erase.

9 Determine if you want to save a current view of the RMI or MAP display while you are logging an SDM session to an output file.

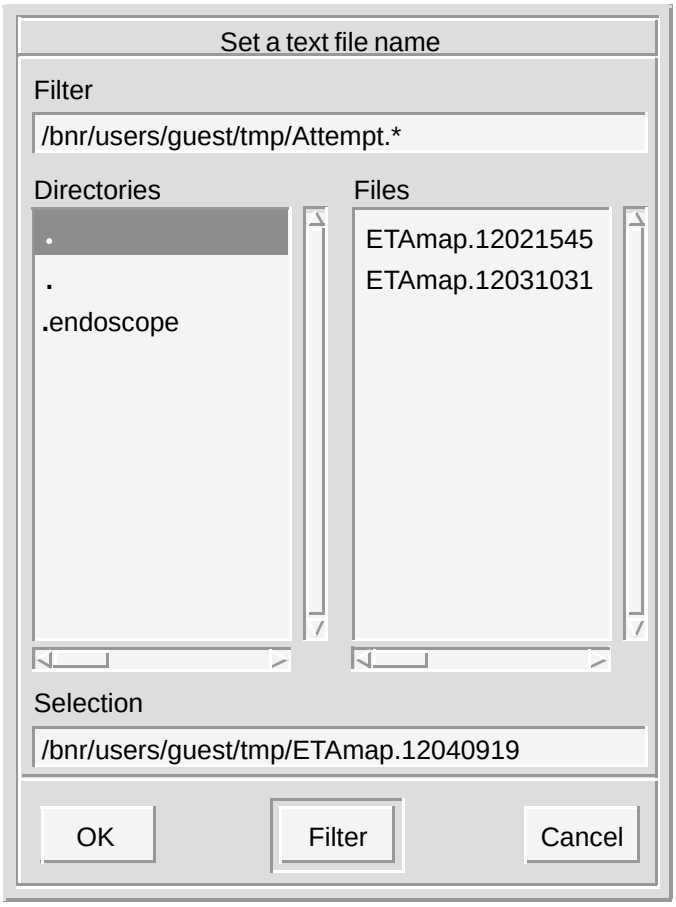
Note: The Logging an SDM session to an output file procedure does not save the RMI and the MAP display view.

If you	Do
want to save a view of the RMI or MAP display	step 10
do not want to save a current view of the RMI or MAP display	step 12

10 Select the Save current view... menu item from the File menu in the SDM Session window.

The Set a text file name window appears.

Set a text file name window



11 Select the default file name in the current directory by clicking OK.

Note: You can append different snapshots of the RMI or MAP display view to the same file by reusing the same file name.

12 Stop logging the file by selecting the Stop logging to file... menu item from the File menu in the SDM Session window.

Note: You cannot start logging another file session until you stop the current logging session.

13 Close the current ETA session window.

If	Do
you are in a CS 2000 Core Manager session	step 14
you are in a CI/MAP session	step 15

14 Exit the core manager session:

 # exit

15 Exit the CI/MAP session:

> logout

16 You have completed this procedure.

Performing a full restore of the software from S-tape

Purpose

Use this procedure to perform a full restore of the core manager software load from the system image backup tape (S-tape).

Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the core manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

Application

ATTENTION
You must be a trained AIX system administrator authorized to perform fault-admin actions.

ATTENTION
You must mirror all volume groups on the core manager before you perform this procedure. If you perform this procedure when disk mirroring is not at the Mirrored state, the system displays an error message.

ATTENTION
If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

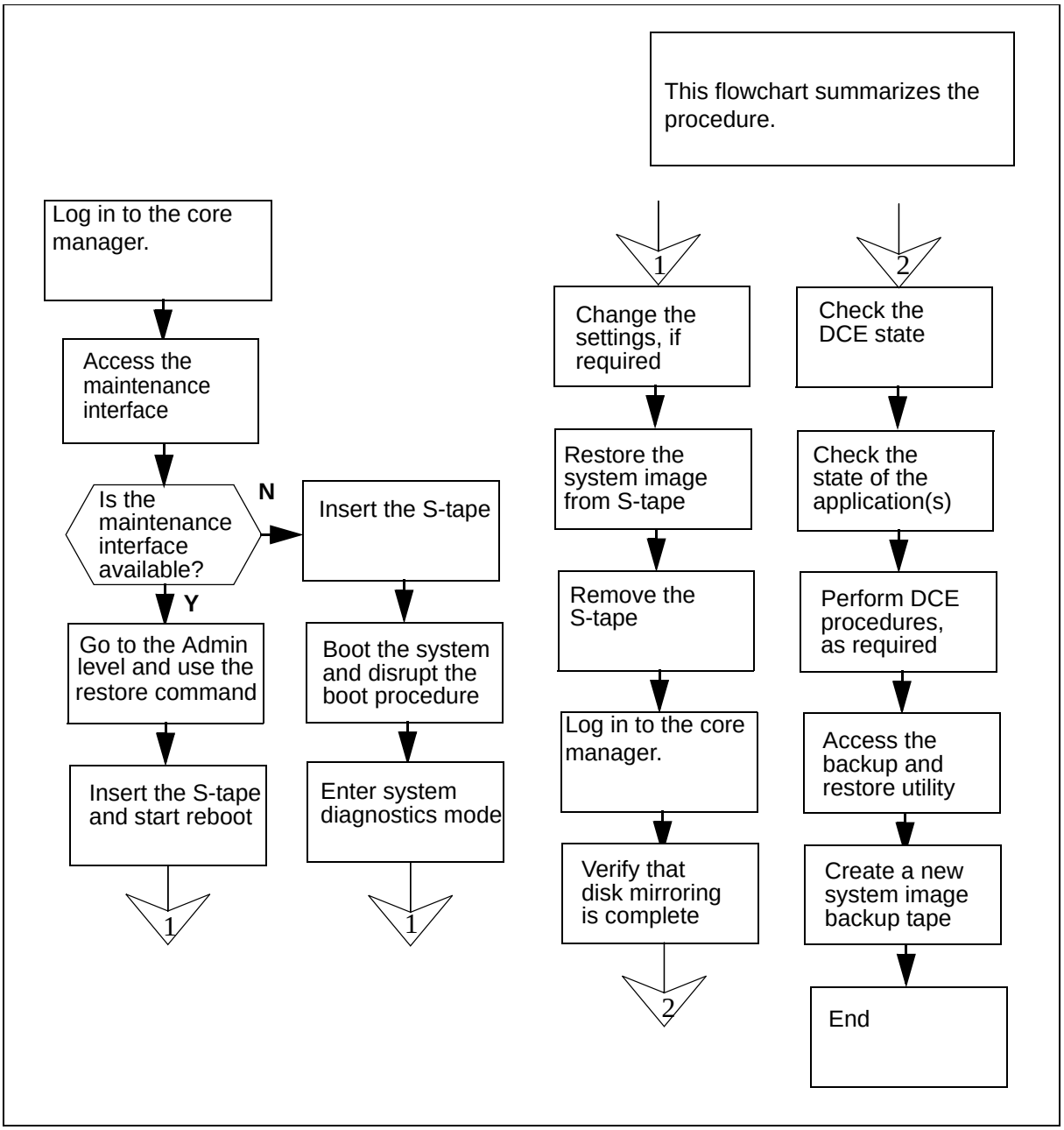
Interval

Perform this procedure when the core manager is out-of-service due to a corrupted software load.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the recovery tasks.

Summary of performing a full restore of the software from the S-tape



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

Performing a full restore of the software from S-tape

At the local VT100 console

1 Log into the CS 2000 Core Manager as a user authorized to perform fault-admin actions.

2 Access the maintenance interface:

`sdmmtc`

3 Determine if the core manager maintenance interface is available.

If	Do
core manager maintenance interface is available	step 4
core manager maintenance interface is not available	step 10

4 Access the administration (Admin) level:

`admin`

5 Perform a full restore of the core manager:

`restore`

Example response:

```
Select the tape drive you want to restore from,
or type Abort to abort:

Enter 0 for the tape drive in the main chassis
slot 2.
Enter 1 for the tape drive in the main chassis
slot 3.
```

6 Choose the tape drive to use.

If	Do
you want to use the tape drive in slot 2	enter 0
you want to use the tape drive in slot 13	enter 1

7 When prompted, confirm that you want to proceed:

y

Example response:

```
Insert the backup-tape into the tape drive in
the main chassis slot 2. When completed press
[Enter] to start the restore.
```

8 Insert the back-up tape (S-tape) into the tape drive you specified (slot 2 or 13).

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

9 Press the Enter key to start the restore process, and proceed to step 17.

Note: When you press the Enter key, the system starts the restore procedure by rebooting the core manager from the selected tape drive.

At the core manager

10 Ensure that one of the core manager tape drives (slot 2 or 13 in the main chassis) contains the system image backup tape (S-tape).

Note: Use tape drive DAT0 (option for performing a full restore from an S-tape) if your system also includes SBA.

At the Modular Supervisory Panel

11 Reboot the core manager. If the prompt is available at a local VT100 console, reboot the core manager:

```
shutdown -Fr
```

If the prompt is not available, reboot the core manager by turning the power off, then on, using the MSP breaker that supplies power to the core manager.

At the local VT100 console

12 When the system displays “COLD Start”, press the Break key or the Esc key twice to interrupt the boot process. The system takes about 4 minutes to initialize.

13 Continue depending on the prompt displayed on the monitor.

If the prompt is	Do
FX-Bug	step 16
FX-Bug and you are in a menu	step 14
FX-Diag	step 15

14 From the selection menu, select Go to System Debugger:

3

Go to step 16.

15 Switch the directory to FX-Bug:

sd

16 View the input/output devices on the core manager to verify the address of the tape drive from the FX-Bug prompt. Enter:

Fx-Bug> ioi

Example response:

```
CLUN DLUN CNTRL-TYPE DADDR DTYPE RM Inquiry-Data
   1    0  IO        0     $00   N  SEAGATE
ST11200N ST
                                     31200 0660
   3    0  IO        0     $00   N  SEAGATE
ST12400N
                                     ST32430
0660
   1    50 IO        5     $01   Y  ARCHIVE
Python
                                     28388-XXX
5.45
   6    0  IO        0     $00   N  SEAGATE
ST11200N
                                     ST31230
0660
   8    0  IO        0     $00   N  SEAGATE
ST12400N
                                     ST32430
0660
   6    50 IO        5     $01   Y  ARCHIVE
Python
                                     28388-XXX
5.45
```

Note: In the example response, the tape drive is ARCHIVE.

17 If you receive the FX-Bug prompt, then continue with this step. Otherwise, go to step 19.

Fx-Bug> pboot <address_for_Archive_Python>

In the example, the following are valid choices:

- pboot 1 50 if the tape drive is located in slot 2
- pboot 6 50 if the tape drive is located in slot 13

18 Wait about 4 minutes until the system completes the reboot.

19 The system prompts you to define the console setting and the language setting. Define the console setting by selecting option 1 and pressing the Enter key.

Note 1: In case of any failures, contact your next level of support.

Note 2: When you define the console setting, the system does not echo the entry “1" on the screen.

20 Enter 1 to select the language setting, and press the Enter key. The Welcome to Base Operating System Installation and Maintenance menu is then displayed.

21 Select “Change/Show Installation Settings and Install”:

2

The system displays the System Backup Installation and Settings menu.

Example response:

```
        System Backup Installation and Settings

Either type 0 and press Enter to install with
the current settings, or type the number of the
setting you want to change and press Enter.

  Setting:                                Current
Choice(s):
1 Disk(s) where you want to install   hdisk0...
         Use Maps                       No
2 Shrink File System                    No


>>> 0 Install with the settings listed above.
```

Note: The string “..." shown under Current Choice(s) indicates that more than one disk is currently in use.

22 The default disk for the installation is hdisk0 which is located in slot 2 of the main chassis. If your core manager contains one disk drive in each domain of the main chassis, accept the default setting. If you have additional disk drives, you may wish to change the settings.

If	Do
you want to change the current settings	step 23

If	Do
you want to use the current settings	step 27

23 Change the disks where you want to install the backup image:

1

The system displays the Change Disk(s) Where You Want to Install menu.

Example response:

```
            Change Disk(s) Where You Want to
Install

Type one or more numbers for the disk(s) to be
used for installation and press Enter. To cancel
a choice, type the corresponding number and
Press Enter. At least one bootable disk must be
selected. The current choice is indicated by
>>>.

   Name     Location Code Size(MB) VGStatus
Bootable Maps
>>>1 hdisk0 c1-f2-00-0,0  4056     rootvg
   Yes     No
>>>2 hdisk5 c1-f13-00-0,0 4056
  rootvg    Yes     No
   3 hdisk1 c1-f4-00-0,0  4056     other
vg  Yes     No
   4 hdisk2 c1-f4-00-1,0  4056     other vg
Yes     No
   5 hdisk3 c2-f1-00-0    02043    other vg
 Yes     No
```

This menu displays the list of all available disks on which you can install the system backup image. The currently selected disks are indicated by >>> symbols.

Note: The system backup must be installed on one disk in each domain to achieve fault-tolerant operation. Valid choices in the example in step 23 are hdisk0 and hdisk5. The rootvg disks for installation must have location codes

- c1-f2-00-0 for domain 0, and
- c1-f13-00-0 for domain 1.

24 To select a disk or disks, enter the number of the disk, and press the Enter key.

25 To deselect a selected disk, enter its number again and press the Enter key.

26 When you have finished entering the settings, the System Backup Installation and Settings menu is displayed. Enter

```
0
```

and return to step 22.

27 Accept the current settings:

```
0
```

This begins the restore process and lasts at least 30 min. During the restore process, the monitor displays the approximate percentage of the tasks completed, and the elapsed time.

Note 1: If an error message appears at the end of the restore process, datavg did not import successfully. Contact the next level of support.

Note 2: You must manually re-boot the system if you are performing this procedure as part of the “Removing an I/O expansion chassis (NTRX50EC)” procedure in the Upgrades document. In this scenario, go to step 28.

Note 3: As part of the restore process, the system reboots automatically and displays the login prompt. Continue with step 29.

28 At the FX-bug prompt, manually boot the system:

```
FX-bug> pboot 1 0
```

At the core manager

29 Remove the S-tape from the tape drive when the reboot is completed, and store it in a secure location.

At the local or remote terminal

30 Log in to the core manager as a user authorized to perform fault-admin actions. Press the Enter key when you see the “TERM=(vt100)” prompt.

31 Start the core manager maintenance interface:

```
sdmmtc
```

32 Access the storage level:

`> storage`

Example response:

```
volume Groups      Status          Free(MB)
rootvg             Mirrored         2032
datavg             Mirrored         11712

Logical Volume    Location  Size(MB)   % full/
threshold 1 /               rootvg        88
       11/80
2 /usr             rootvg        600       29/90
3 /var             rootvg        200       5/70
4 /tmp             rootvg        24        5/90
5 /home            rootvg        304       5/70
6 /sdm             rootvg        504       24/90
7 /data            datavg        208       7/ 80
                  Logical volumes showing: 1 to
7 or 7
```

33 Determine the mirror status of the disks.

If the disks are	Do
Mirrored	step 35
Integrating or Not Mirrored	step 34

34 You cannot continue this procedure until disk mirroring is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is at the Mirrored state, continue this procedure.

35 Access the LAN level:

`lan`

36 Check the state of DCE.

Example response:

```
DCE State: SysB
```

37 Access the application (APPL) level to check the state of any DCE-based applications:

`appl`

and pressing the Enter key.

Example response:

```
# Application                          State
1 Table Access Service                   .
2 Log Delivery Service                   .
3 OM Access Service                      .
4 Secure File Transfer                  Fail
5 Enhanced Terminal Access              Fail
6 Exception Reporting Fail
                Applications showing 1 to 6 of 6
```

38

ATTENTION

DCE and DCE-based applications can fail if the key tab files restored from tape contain obsolete keys.

If the DCE state is displayed as SysB at the LAN menu level of the RMI (step 35), and the logs displayed indicate an error with the security client service in DCE, restore the service by performing the following procedures in the CS 2000 Core Manager Configuration Management document:

- “Removing a CS 2000 Core Manager from a DCE cell”
- “Configuring a CS 2000 Core Manager in a DCE cell”

39 If some DCE-based applications are faulty (Fail state, see step 37), try to restore them by busying (BSY) and returning to service (RTS) the applications from the SDM APPL level (see step 37).

40 If this approach fails, restore them by performing the procedure to add the application server to the DCE cell in the CS 2000 Core Manager Configuration Management document.

41 Reset passwords for users SDM01-04 on the core and SDM. Refer to procedure Resetting SDM user passwords for DDMS on page 411.

42 You must create a new system image backup tape. Refer to the procedure “Creating system image backup tapes (S-Tapes)” in the CS 2000 Core Manager Security and Administration document.

43 You have completed this procedure.

Performing a partial restore of the software from S-tape

Purpose

Use this procedure to restore individual files or sets of files from the system image backup tape (S-tape).

Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

Procedures related to this procedure

Procedure	Document
Logging in to the Packet SDMX	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

Procedures related to this procedure

Procedure	Document
Logging in to the Packet SDMX	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

CAUTION
Possible loss of data
Use this procedure at the discretion of the system administrator.

Perform a partial restore only if you are familiar with the files, and know exactly which files are to be restored. If you restore the wrong files, you may inadvertently corrupt core manager software.

ATTENTION
This procedure must be performed by a trained AIX system administrator authorized to perform fault-admin actions.

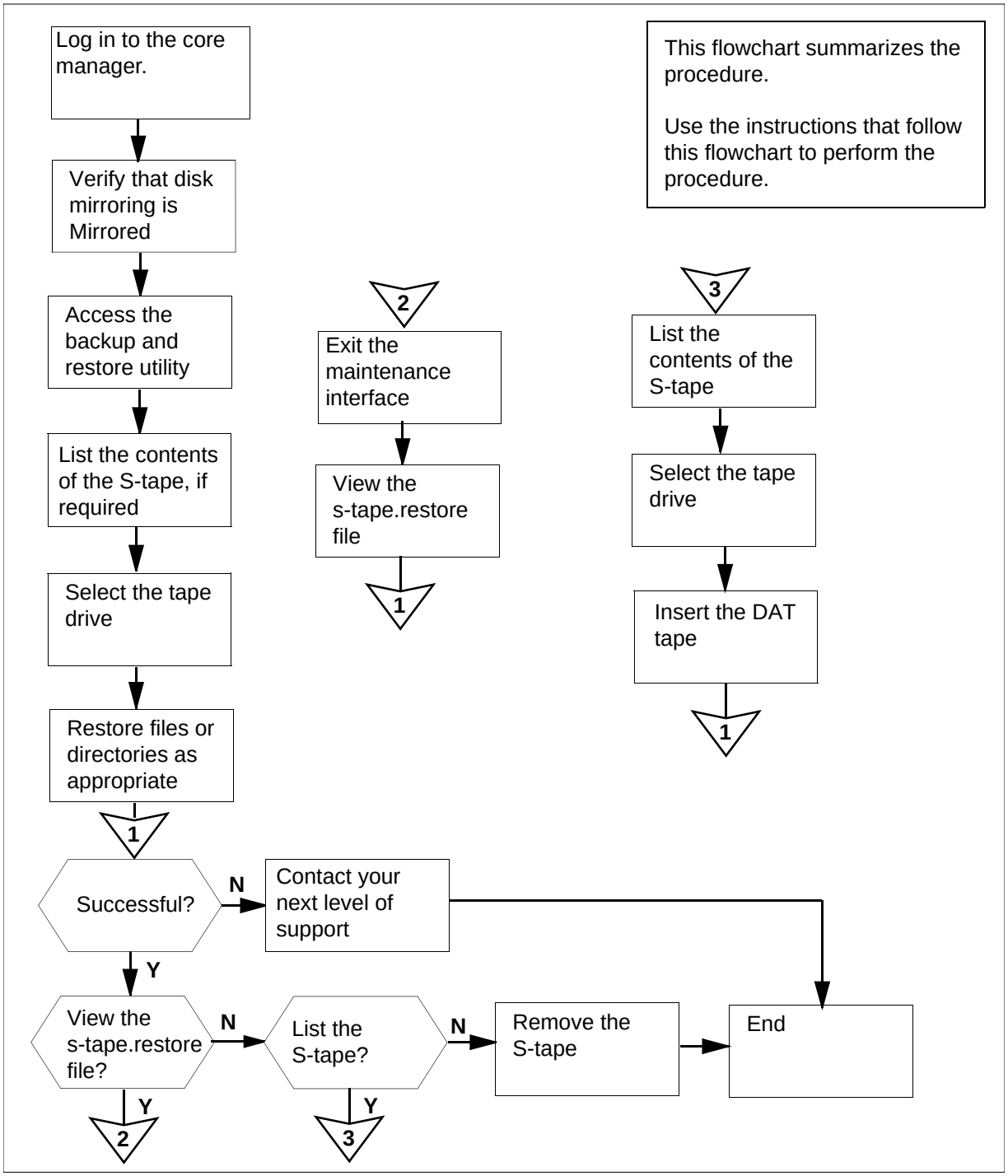
ATTENTION
All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If you attempt to perform this procedure when disk mirroring is not Mirrored, an error message is displayed on the screen.

ATTENTION
If your system includes the SuperNode Billing Application (SBA), use tape drive DAT0 to perform this procedure.

Action

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

Summary of Partial restore from the system image tape (S-tape)



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

Partial restore from the system image tape (S-tape)

At the local or remote console

1 Log into the core manager as the user authorized to perform fault-admin actions.

2 Access the maintenance interface:

`sdmmtc`

3 Access the storage level:

`storage`

Example response:

```
Volume Groups        Status              Free
(MB)
rootvg               Mirrored            2032
datavg               Mirrored            11712

Logical Volume    Location
   Size(MB)   %full/threshold 1 /
                rootvg       88          11/80
2 /usr              rootvg      600
          29/90
3 /var              rootvg      200
           5/70
4 /tmp              rootvg       24
           5/90
5 /home             rootvg      304
           5/70
6 /sdm              rootvg      504
          24/90
7 /data             datavg      208
           7/80
                     Logical volumes showing: 1
to 7 of 7
```

4 Determine the Mirror status of the disks.

If the disks are	Do
Mirrored	step 6
not Mirrored	step 5

5

CAUTION
Possible loss of data
You cannot perform this procedure until disk mirroring of all volume groups is Mirrored.

If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

6 Access the administration (Admin) menu level of the RMI:

```
admin
```

7 Access the System Image Backup and Restore Menu:

```
backup
```

Note 1: If disk mirroring for all volume groups is not Mirrored, the system displays an error message. The system then prompts you to return to the System Image Backup and Restore menu.

Note 2: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

```
Currently there is a backup running on bnode73.
Please execute yours later.
Exiting...
```

8 Determine the contents of the tape.

If you	Do
wish to list the S-tape	step 9
do not wish to list the S-tape	step 17

9 From the System Image Backup and Restore Menu, select “List Contents of the System Image Tape (S-tape)”:

3

10 After you select option 3, you are prompted to select the tape drive.

Example response:

```
Select a tape drive you wish to use:

       Enter 0 to return to previous menu
       Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
       Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
       ( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

11 Enter the number for the tape drive you want to use (1 or 2), and press the Enter key.

Note: If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

Response:

```
You have selected DAT 1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.

If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing
records will not be lost during the backup
restore operation.

Do you wish to continue with DAT 1? ( y | n )
```

- if you wish to continue using DAT1, enter y
- if you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

12 After you select the tape drive, the system prompts you to insert the S-tape into the appropriate tape drive.

Example response:

```
Please insert your System Image Backup tape
(S-tape) into the tape drive DAT0 and allow at
least 5 minutes to complete the listing.

A log file will be saved in /tmp/s-tape.toc.

Are you ready to proceed? ( y | n )
```

At the core manager

13 Insert the S-tape into the tape drive you selected.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

At the local or remote VT100 console

14 When you are ready to continue this procedure, enter:

y

The contents of the S-tape are listed on the screen. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

Example response:

```
Would you like to return to the previous menu?
( y | n )
```

15 Return to the System Image Backup and Restore Menu:

y

16 Determine if the file or directory has been restored.

If you are listing the contents of the tape to verify	Do
that the file has been restored	step 25
the file name or directory that you wish to restore	step 17

17 From the System Image Backup and Restore Menu, select “Restore Files from the System Image Tape (S-tape)”:

4

18 After you select option 4, you are prompted to select the tape drive.

Example response:

```
Select a tape drive you wish to use:

       Enter 0 to return to previous menu
       Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
       Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
       ( 0, 1 or 2 ) ==>
```

Note: Use tape drive DAT0 (option 1) if your system also includes SBA.

19 Enter the number for the tape drive you want to use (1 or 2).

Note: If your system includes SBA, and you still wish to use tape drive DAT1 (option 2), the following message is displayed:

Example response:

```
You have selected DAT 1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.

If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing
records will not be lost during the
backup/restore operation.

Do you wish to continue with DAT 1? ( y | n )
```

- if you wish to continue using DAT1, enter y
- I If you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

20 After you select the tape drive, you are prompted to insert the S-tape into the appropriate tape drive. A warning is displayed advising that this procedure must only be completed by qualified core manager system administrators. The warning also advises that files and directories must be entered exactly as they appear in the file listing. Insert the S-tape in the appropriate tape drive.

Note: Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

Example response:

```
Are you ready to enter the name of the file or
directory? ( y | n )
```

21 Continue this procedure:

y

Example response:

```
Enter the name of the directory or file that you
wish to restore as
./<your-full-path>/<your-file-or-directory>.

Note: Tape processing may take a few minutes to
complete.       A log file /tmp/s-tape.restore
will be created.
==>
```

22 Enter the full path name of the directory or file that you wish to restore, exactly as shown in the file listing, including "/" at the beginning.

Note 1: A log file /tmp/s-tape.restore is created when the restore is completed.

Note 2: An error message is displayed if the restore is unsuccessful. If this occurs, go to step 25.

23 During the restore process, the screen does not display any additional information. When the file restore is complete, the file you have restored is displayed. The system then prompts you to return to the System Image Backup and Restore Menu.

Example response:

```
Would you like to return to the previous menu?
( y | n )
```

Note: If the restore has failed, an error message is displayed before the prompt, advising you to list the contents of the tape, and perform the procedure again.

24 Return to the System Image Backup and Restore Menu:

y

25 Determine if the restore was successful. The system displays the file that you have restored, as described in step 23. You may

also wish to view the s-tape.restore file or list the files on the S-tape.

If	Do
the restore is successful	step 32
the restore failed	contact your next level of support
you wish to view the s-tape.restore file	step 26
you wish to list the S-tape	step 9

26 Exit the System Image Backup and Restore Menu:

```
0
```

27 Exit the maintenance interface:

```
quit all
```

28 Access the s-tape.restore file:

```
cd /tmp
```

29 Scroll through the file:

```
more s-tape.restore
```

30 Continue pressing the Enter key until the files that you have restored, and the date of the restore, are displayed.

31 Determine if the restore was successful.

If	Do
successful	step 33
failed	contact your next level of support

32 Exit the System Image Backup and Restore Menu:

```
0
```

Note: If you then wish to exit the maintenance interface, type quit all and press the Enter key.

At the core manager

33 Remove the S-tape and store it in a secure place.

34 You have completed this procedure.

Recovering a standalone X.25 SYNC personality module

Purpose

Use this procedure to recover a standalone X.25 personality module (SYNC X25 PM).

Application

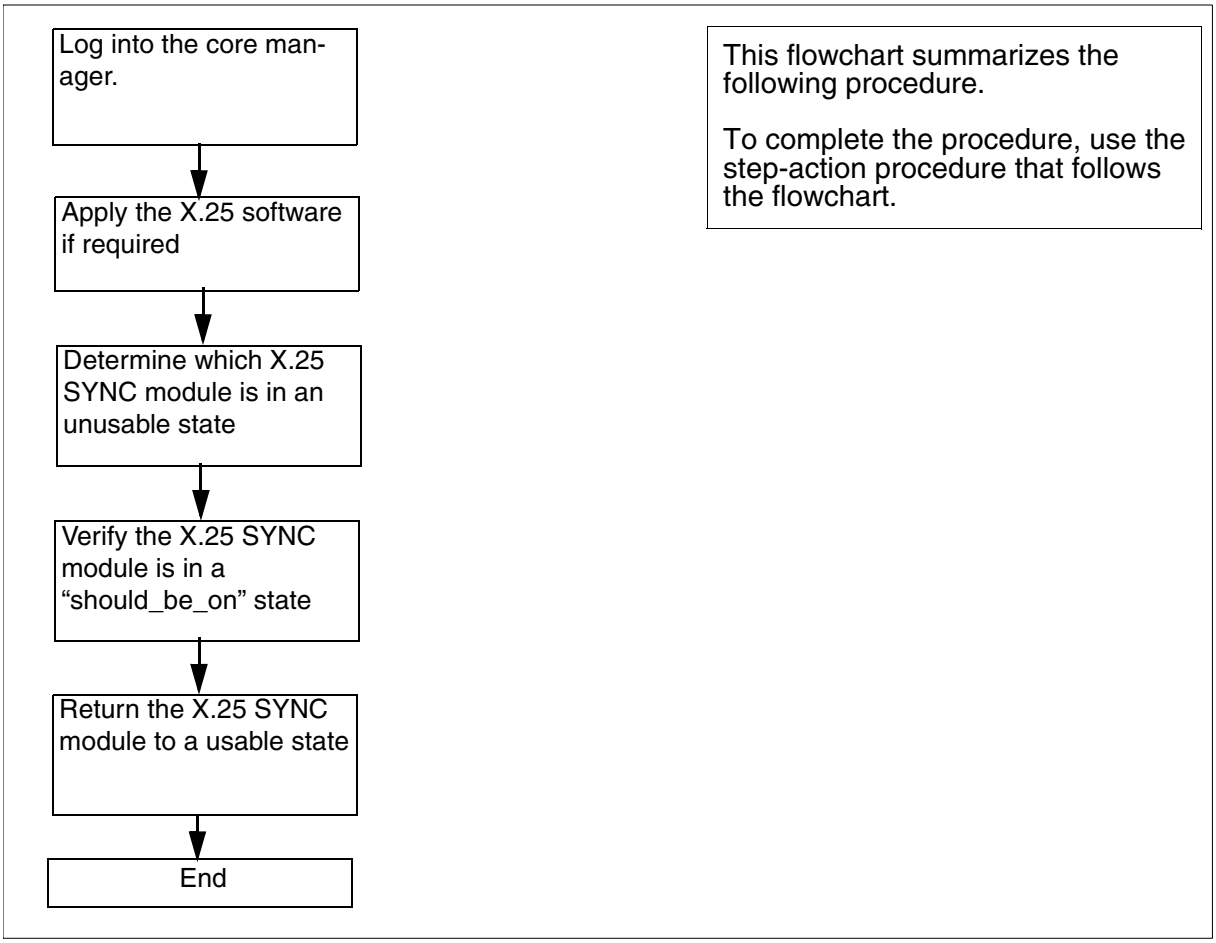
Use this procedure to recover a standalone X.25 personality module (SYNC X25 PM) from any of the following conditions:

- the module is at a failed state and the RTS (return to service) command failed
- the module was pulled from the shelf without stopping the X.25 daemon and busying the module first

Action

The following flowchart is only a summary of the procedure. To recover the X.25 personality module, use the instructions in the procedure that follows the flowchart.

Summary of recovering an X.25 SYNC personality module



Recovering a standalone X.25 SYNC personality module

At the local or remote VT100 console

1 Log into the core manager.

2 Determine which X.25 SYNC module is in an unusable state:

```
# lsstate -s | grep SYNC-
```

Example response:

```
SYNC-0 cl-fl Available* should_be_on X.25
Controller Module
SYNC-1 cl-fl2 Available online X.25 Controller
Module
```

Note: The example above indicates that SYNC-0 is not in an online state.

3 Verify the X.25 SYNC module is in the “should_be_on” state before you proceed:

```
# lsmod -D1 SYNC-0
```

Example response:

```
SYNC-0 cl-fl Available* should_be_on X.25
Controller Module
SYNCPM-0 cl-rl Defined + inaccessible X.25
Personality Module pgen0 cl-fl Available X.25
MVME1603/VMEBridge
pcomm0 cl-fl Available X.25 Download and Startup
```

Note: Wait until the X.25 SYNC module has reached the “should_be_on” state before you proceed. This can take several minutes.

4 Once the X.25 SYNC module is in the “should_be_on” state, return the module to a usable state:

```
# /usr/lpp/psx25/tmp/fixsync
SYNC-<SYNC_module_no>
```

where

<SYNC_module_no>
is the number of the SYNC module you determined was in an unusable state (either 0 or 1) in step 2

If the SYNC module	Do
returns to a usable state	you have completed this procedure
does not return to a usable state	contact your next level of support

Replacing an MFIO/UMFIO LAN personality module

Purpose

Use this procedure to replace either a fault-tolerant core manager

- Multifunction Input/Output (MFIO) LAN personality module, or
- Ultra-Multifunction Input/Output (UMFIO) LAN personality module

Application

The Multifunction Input/Output (MFIO) LAN personality module or an Ultra-Multifunction Input/Output (UMFIO) LAN personality module are located at the rear of the main chassis, and the I/O expansion chassis.

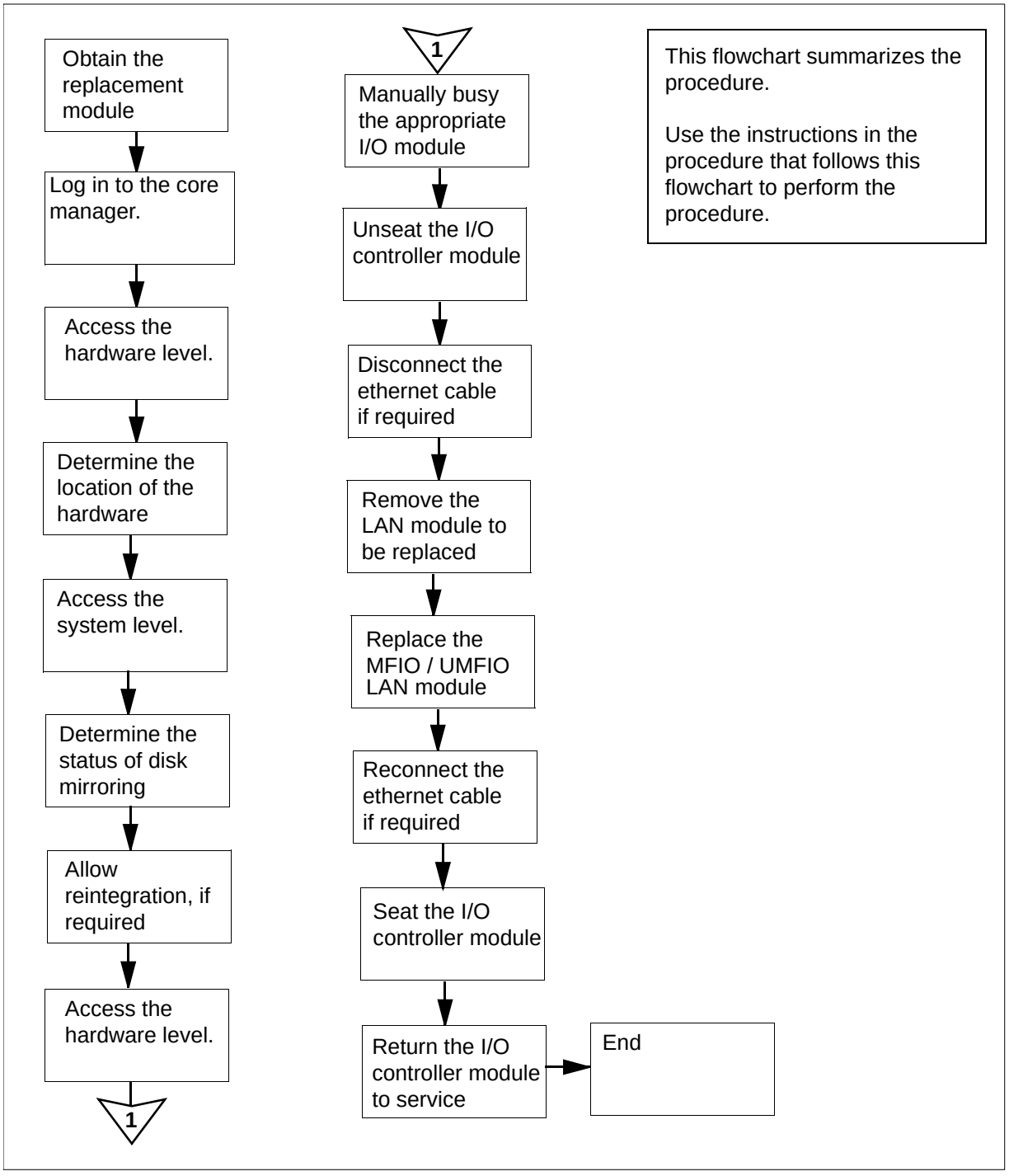
Nortel PEC	Name
NTRX50NK/NTRX50NN	UMFIO LAN personality module

Note: Each I/O controller module must have an associated LAN personality module (NTRX50NK/NTRX50NN) installed at the back of the core manager.

Action

The following flowchart is a summary of the procedure. To replace the MFIO / UMFIO LAN personality module, use the instructions in the procedure that follows the flowchart.

Summary of replacing an MFIO / UMFIO LAN personality module



Replacing an MFIO or UMFIO LAN personality module

Obtain a replacement MFIO or UMFIO LAN personality module

1 Obtain a replacement MFIO / UMFIO LAN personality module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed at the top of the module.

At the local or remote VT100 console

2 Log into the core manager as the root or maint user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the hardware (Hw) level:

```
> hw
```

5 Display the hardware location information for the core manager:

```
> locate
```

6 Determine the PEC and location of the I/O controller module associated with the LAN controller module you wish to locate.

Note: The MFIO / UMFIO LAN personality module is indicated by its slot number with location BACK. Its associated I/O controller module is located in the same slot with location FRNT (front).

The example shows a partial display of the information generated from the Locate command. The PEC of the I/O controller module is NTRX50FQ, and the module is located at the front of the main chassis in slot 13.

Press the Enter key to return to the command line.

Example response:

```
Site  Flr  RPos Bay_id Shf Description Slot
EQPEC
HOST  01   A02  CSDM SDMM              13
NTRX50FQ FRNT
HOST  01   A02   CSDM SDMM                 13
NTRX50NK BACK
```

7 Access the storage level:

```
> storage
```

Example response:

```
Disk mirroring (rootvg):        Integrating
```

8 Determine the disk mirroring status for the volume group stored on the I/O controller module determined in step 6.

If disk mirroring is in the	Do
Integrating state	step 9
Mirrored or Not Mirrored state	step 10

9

CAUTION
Potential loss of service
Do not continue this procedure beyond this point while the disks are reintegrating. If you remove an I/O controller module from service during the reintegration process, you will cause a reintegration failure which may require service-affecting manual recovery action.

The hard disks that provide mirrored storage for the system are reintegrating. Allow the reintegration process to complete before continuing this procedure. The reintegration process takes about 20 minutes for each Gbyte. The actual time required depends on the amount of data in the volume group, and the current processor load.

Go to step 8.

10 Access the hardware (Hw) level:

```
> hw
```

11 Busy the I/O controller module associated with the MFIO or UMFIO LAN personality module you want to replace:

```
> bsy <domain_no> <eth>
```

where

<domain_no>
is the domain number (0 or 1) of the MFIO or UMFIO LAN personality module that you are replacing

Use the following list to determine the domain number. The domain number is

- main chassis:
  - 0 if the module is located in slot 2
  - 1 if the module is located in slot 13
- I/O expansion chassis
  - 0 if the module is located in any two slots from 1 to 8
  - 1 if the module is located in any two slots from 9 to 16

<eth>
is the Ethernet number that corresponds to the MFIO or UMFIO LAN personality module to be replaced.

Note: The parameter **<eth>** selects the ethernet MFIO or UMFIO LAN controller device on the I/O controller module. All other devices on the I/O controller module are busied automatically.

Example response:

```
Hardware Bsy - Domain 0 Device ETH
Busying ETH(0) will also busy DSK(0), DAT(0)

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

12 Confirm the busy command:

> y

Example response:

```
Hardware Bsy : Domain 0 Device ETH - Command
initiated.
Please wait...
```

When the Bsy command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware Bsy : Domain 0 Device ETH - Command
complete.
Request will make ent0 not fault tolerant -
Command complete.
```

Note: At the hardware menu level of the RMI, the state of all devices on the I/O controller module changes to “M”.

At the front of the core manager

13

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Press the eject button to remove the tape (if present) from the tape drive.

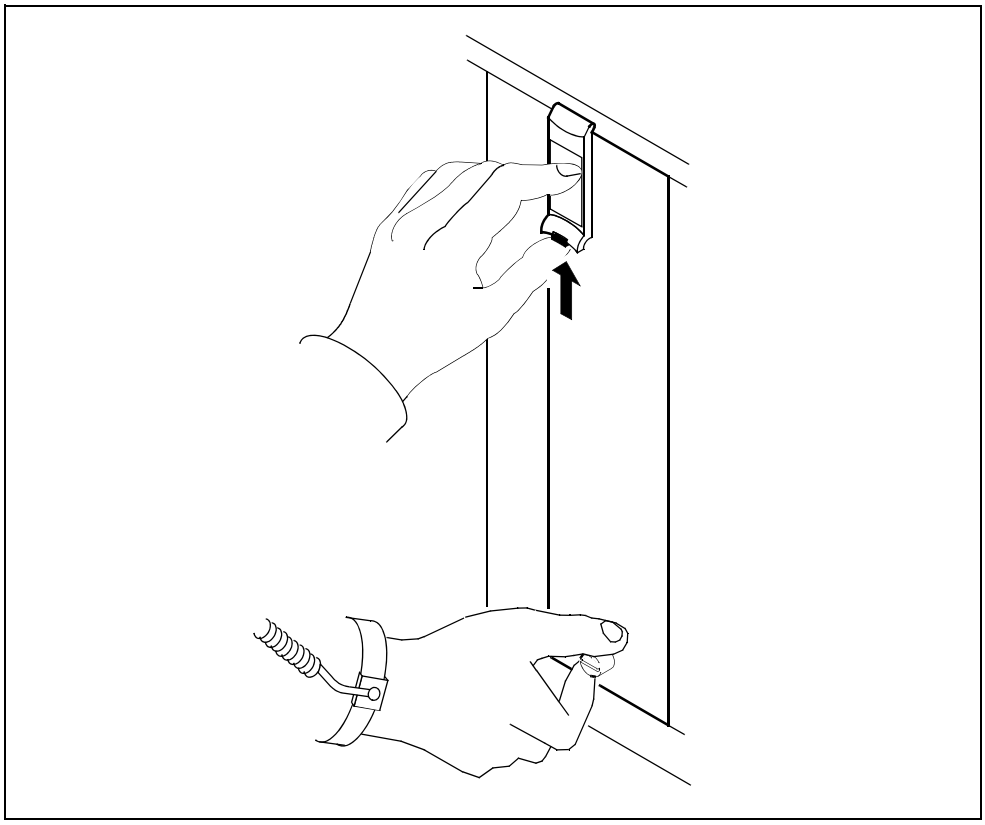
14

CAUTION
Potential service interruption
Unseat only the I/O controller module that you busied in step 11, and not the corresponding I/O controller module in the other I/O domain. The in-service LED on the module busied in step 11 is off, and the out-of-service LED is on (red).

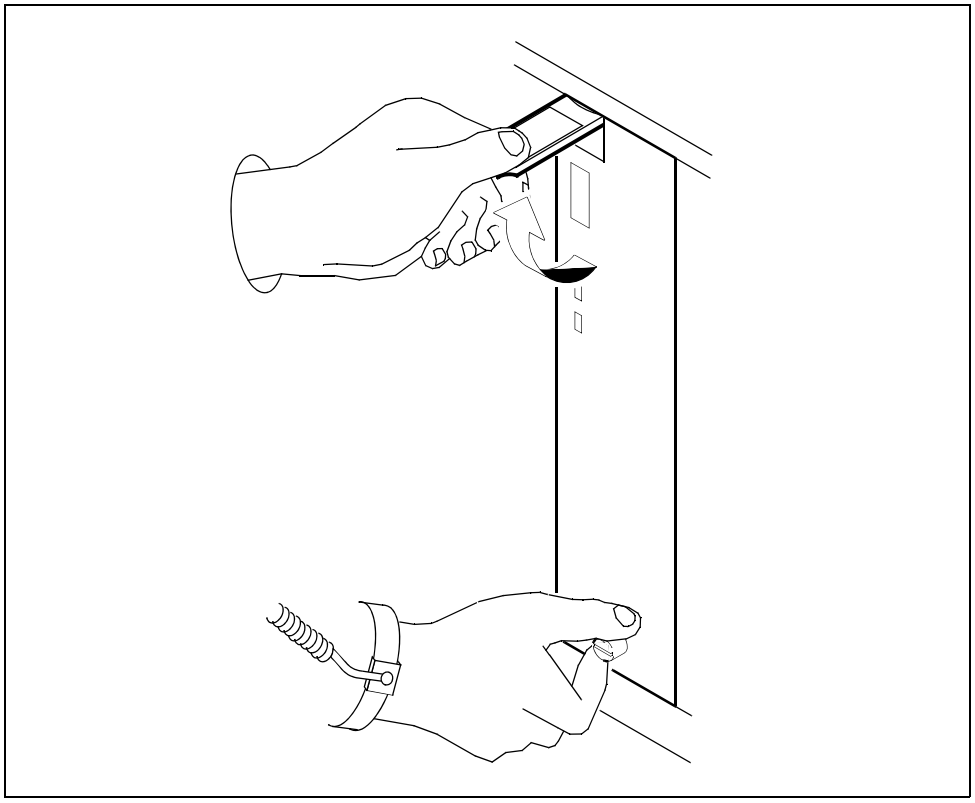
Undo the thumbscrews located on the top and bottom of the I/O controller module associated with the MFIO or UMFIO LAN personality module you want to replace.

Note: The thumbscrews are captive and cannot be removed from the module.

15 Depress the tip of the locking lever on the face of the I/O controller module.



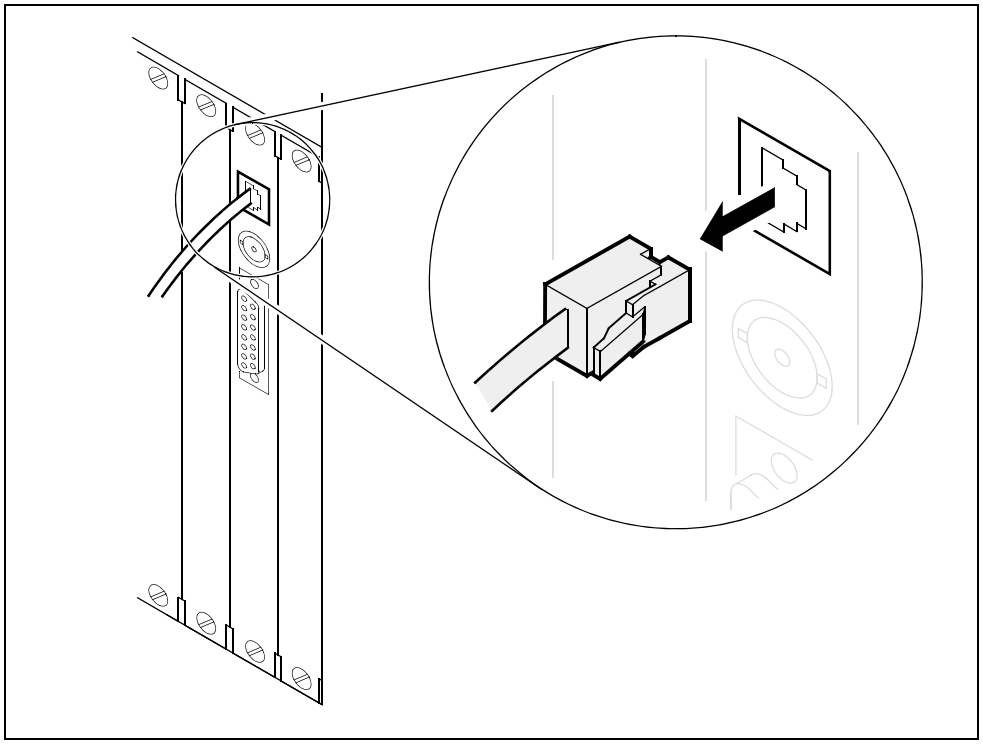
16 Open the locking lever on the face of the module by moving the lever outwards.



At the back of the core manager

17 Label the Ethernet cable connected to the LAN personality module you want to replace.

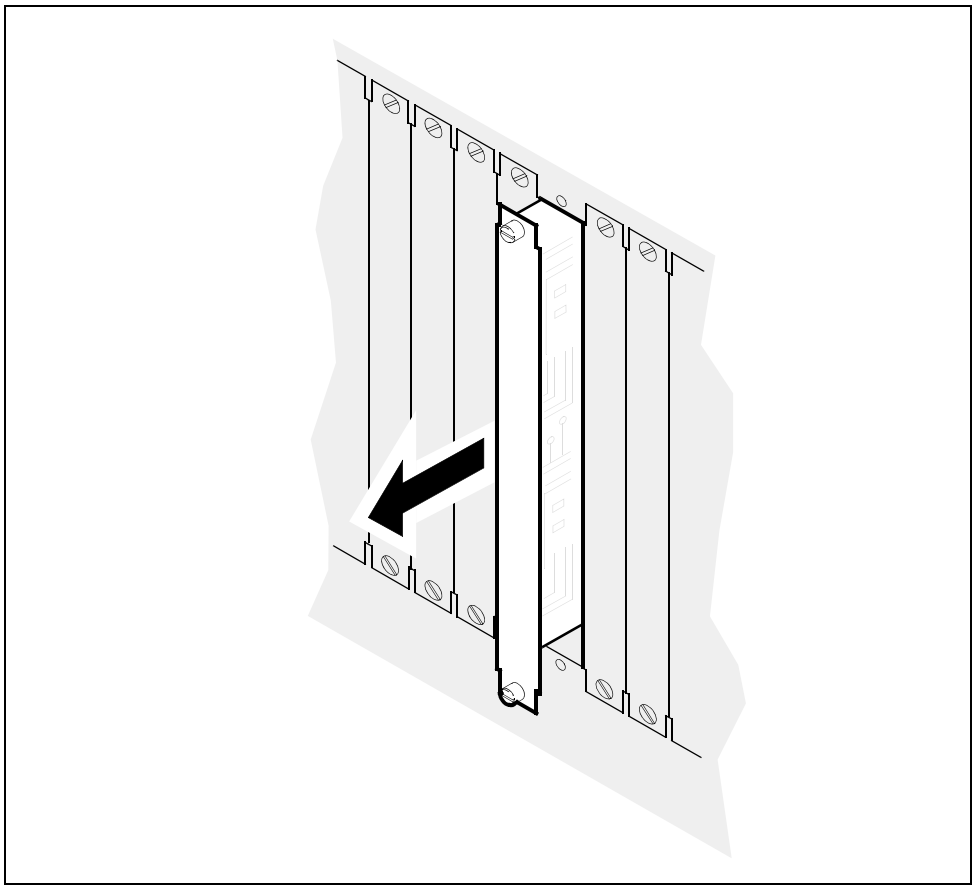
18 Disconnect the Ethernet cable, as shown in the following diagram.



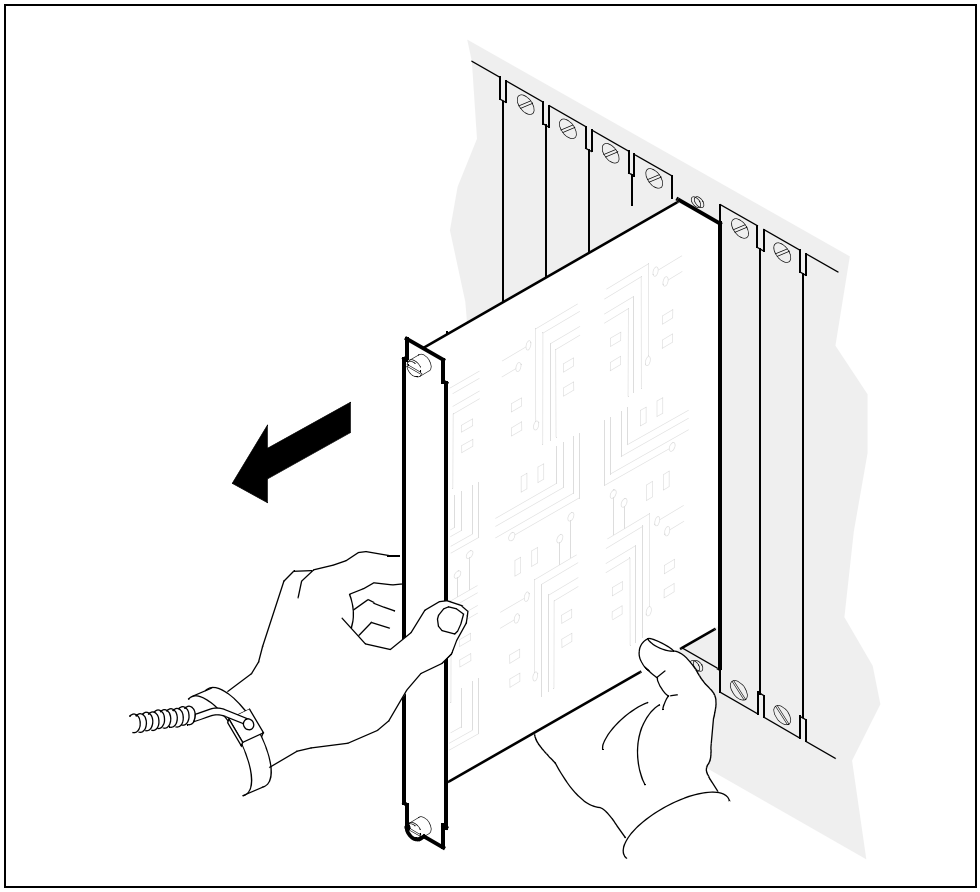
19 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module.

Note: The thumbscrews are captive and cannot be removed from the module.

20 While grasping the thumbscrews, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the core manager shelf.



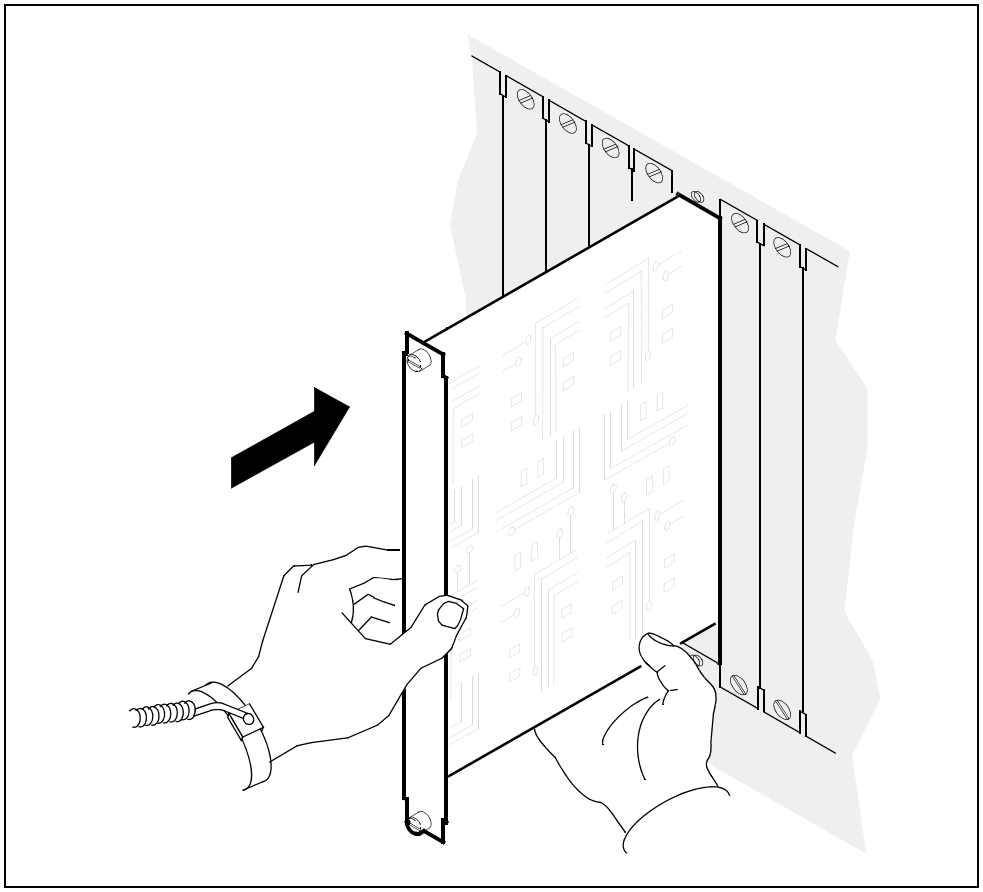
21 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



22 Place the module you have removed in an ESD protective container.

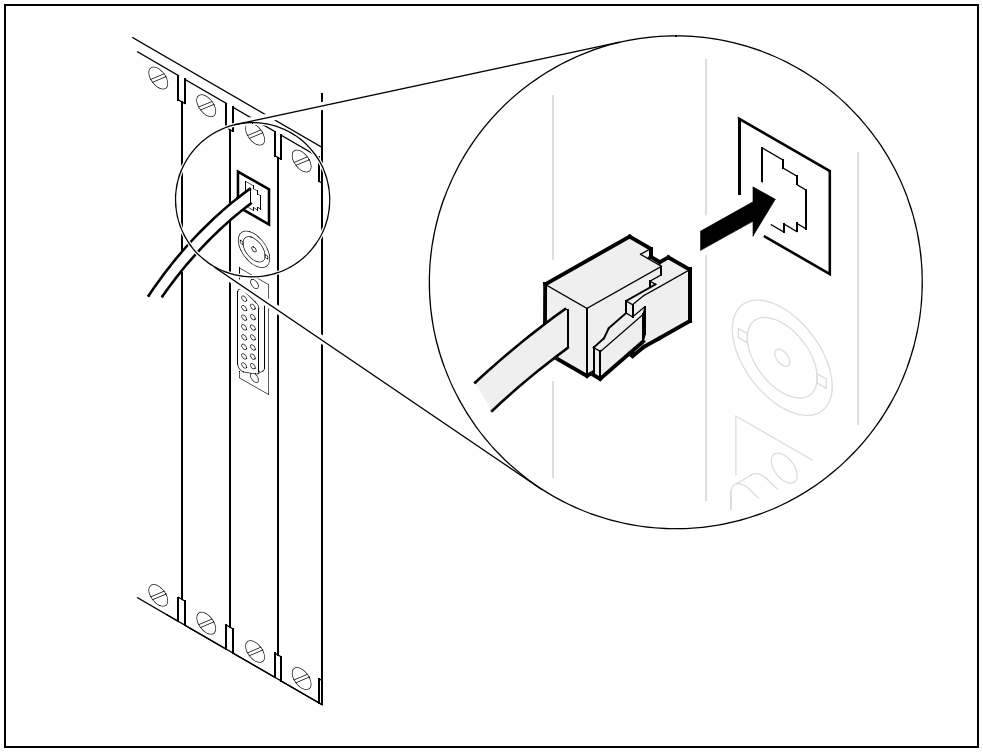
23 Insert the replacement MFIO or UMFIO LAN personality module into the core manager shelf.

24 Gently slide the module into the shelf until it is fully inserted.



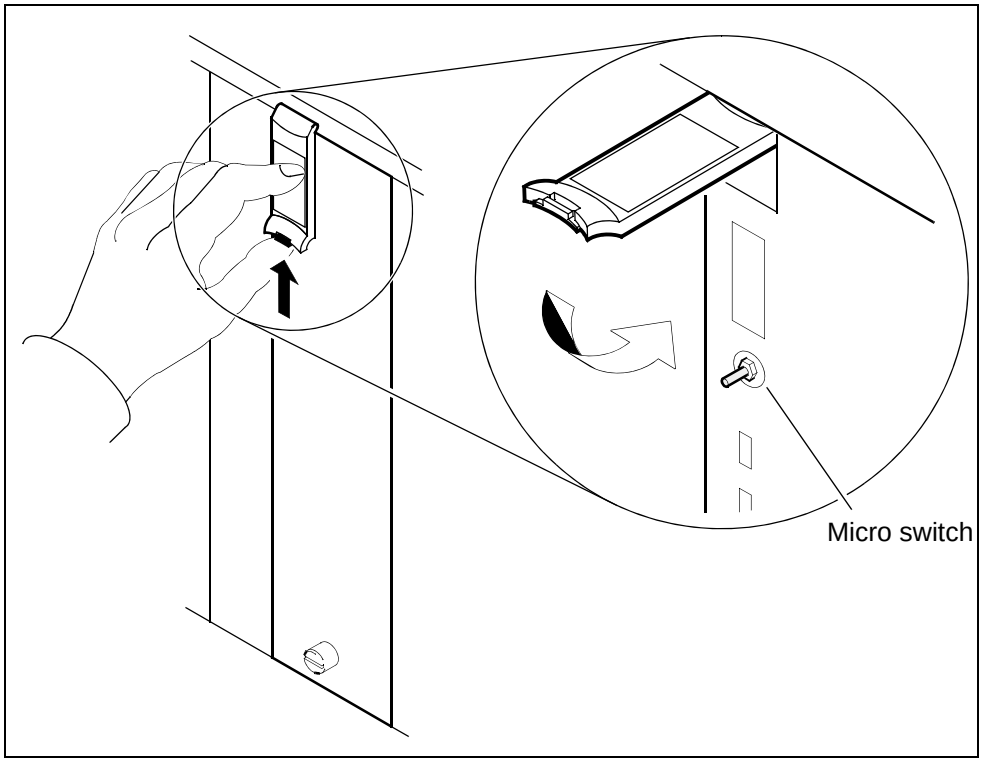
25 Tighten the thumbscrews at the top and the bottom of the module.

26 Reconnect the Ethernet cable to the module. If you wish, remove the label that you put on the cable in step 17.



At the front of the core manager

27 Close the locking lever to secure the I/O controller module you unseated in step 14. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.



28 Tighten the thumbscrews on the I/O controller module.

Note: When the replacement I/O controller module is inserted, both LEDs on the module turn on and off briefly, indicating that the module is

- seated correctly,
- receiving power, and
- passed its self tests

The in-service light on the I/O controller module turns off, and its out-of-service light turns on (red).

At the local or remote VT100 console

29 Return the I/O controller module to service:

```
> rts <domain_no> <eth>
```

where

<domain_no>
is the domain number (0 or 1) of the I/O controller module you previously busied.

<eth>
is the Ethernet number (used in step 11) that corresponds to the MFIO or UMFIO LAN personality module to be replaced

Example response:

```
Hardware RTS : Domain 0 Device ETH - Command
initiated.
Please wait...
```

When the RTS command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware RTS : Domain 0 Device ETH - Command
complete.
```

Note: The system begins to integrate the disks affected by this procedure. The actual time required to complete the integration depends on the amount of data in the volume group, and the current processor load.

30 You have completed this procedure.

Replacing a fan tray

Purpose

Use this procedure to replace a fan tray located at the front of the main and I/O expansion chassis of the core manager.

Application

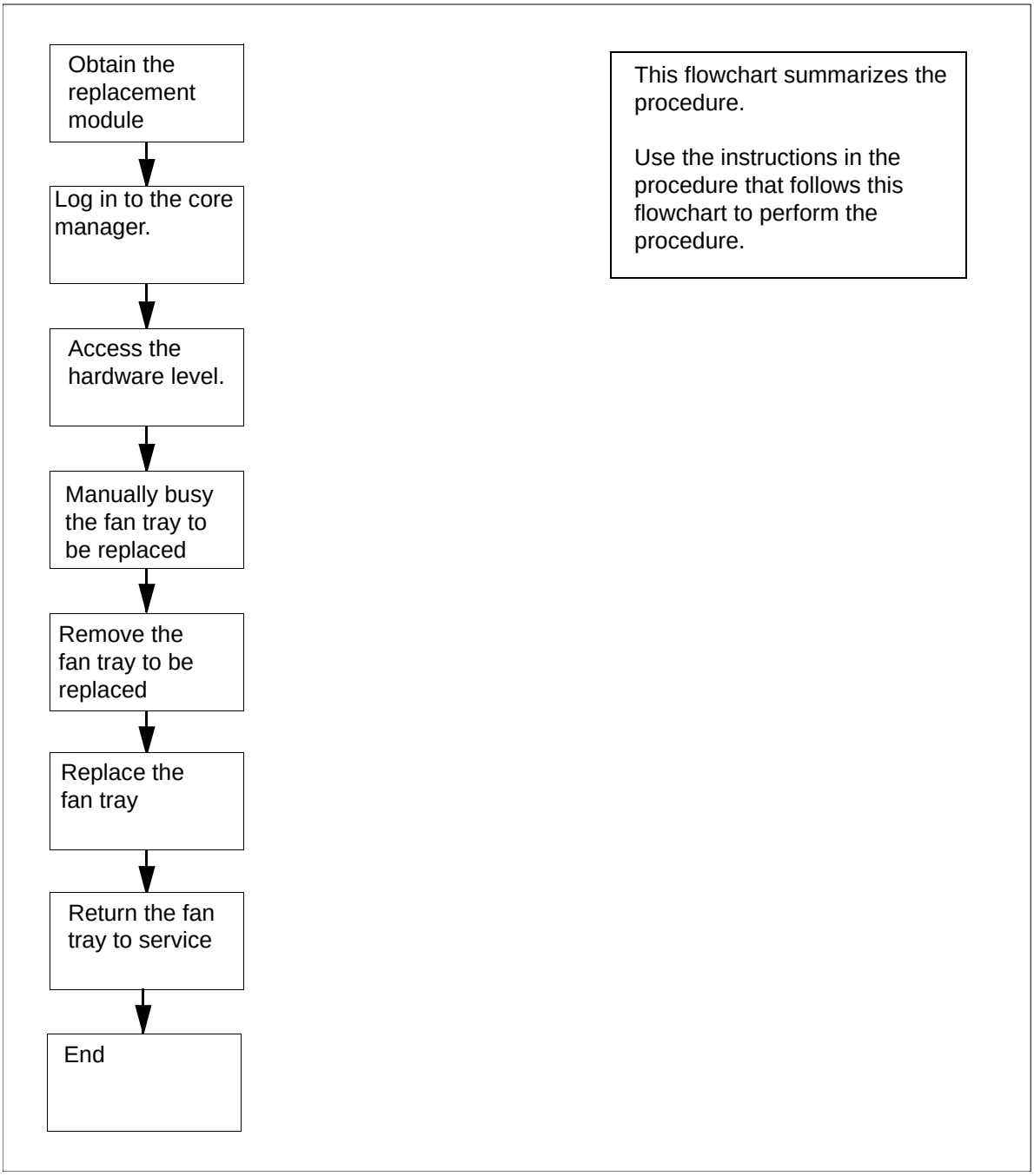
Select the correct fan tray.

Nortel PEC	Name
NTRX50FF	Fan tray 1 in main or I/O expansion chassis (lower)
NTRX50FE	Fan tray 0 in main chassis (upper)
NTRX50KD	Fan tray 0 in I/O expansion chassis (upper)

Action

The following flowchart is a summary of the procedure. To replace the fan tray, use the instructions in the procedure that follows the flowchart.

Summary of replacing a fan tray



Obtain a replacement fan tray

1 Obtain a replacement fan tray with the same product engineering code (PEC), including suffix, as the unit to be removed. The PEC is printed on the left-hand-side locking lever of the fan tray.

At the local or remote VT100 console

2 Log into the core manager as the root or maint user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the hardware level:

```
> hw
```

5 Busy the fan tray module:

```
> bsy <domain> fan
```

where

<domain>
is the number of the domain where the fan tray resides (0 or 1).

Note: This syntax is valid for single chassis configurations (main chassis only).

For systems with a main chassis and an I/O expansion chassis, the parameter “fan” must be specified as either “fan1” or “fan2”, for the main or I/O expansion chassis respectively.

Example response:

```
Hardware Bsy - Domain 1 Device FAN

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

6 Confirm the busy command:

```
> y
```

Example response:

```
Hardware Bsy : Domain 1 Device FAN - Command
initiated.
Please wait...

Hardware Bsy : Domain 1 Device FAN - Command
complete.
```

Note: At the hardware level of the maintenance interface, the state of the fan tray changes to “M”. The out-of-service LED on the fan tray turns orange. The out-of-service LED only applies to a fan tray in the main chassis, as the fan trays in the I/O expansion chassis do not have system LEDs.

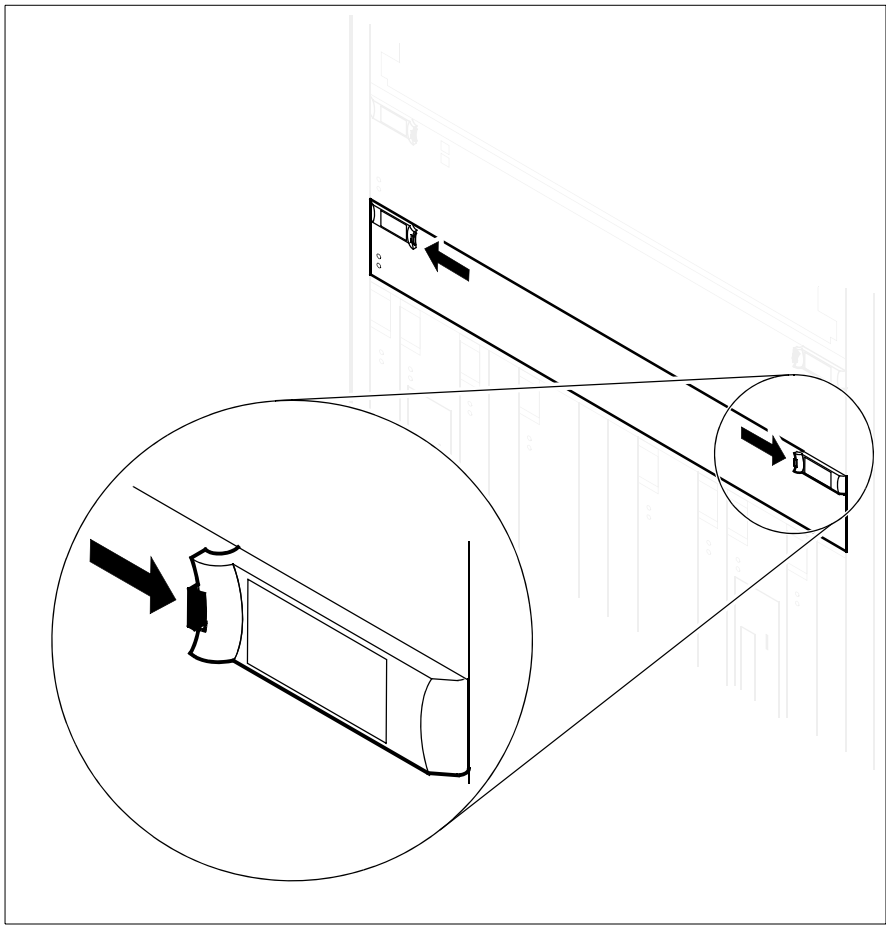
At the front of the core manager

7

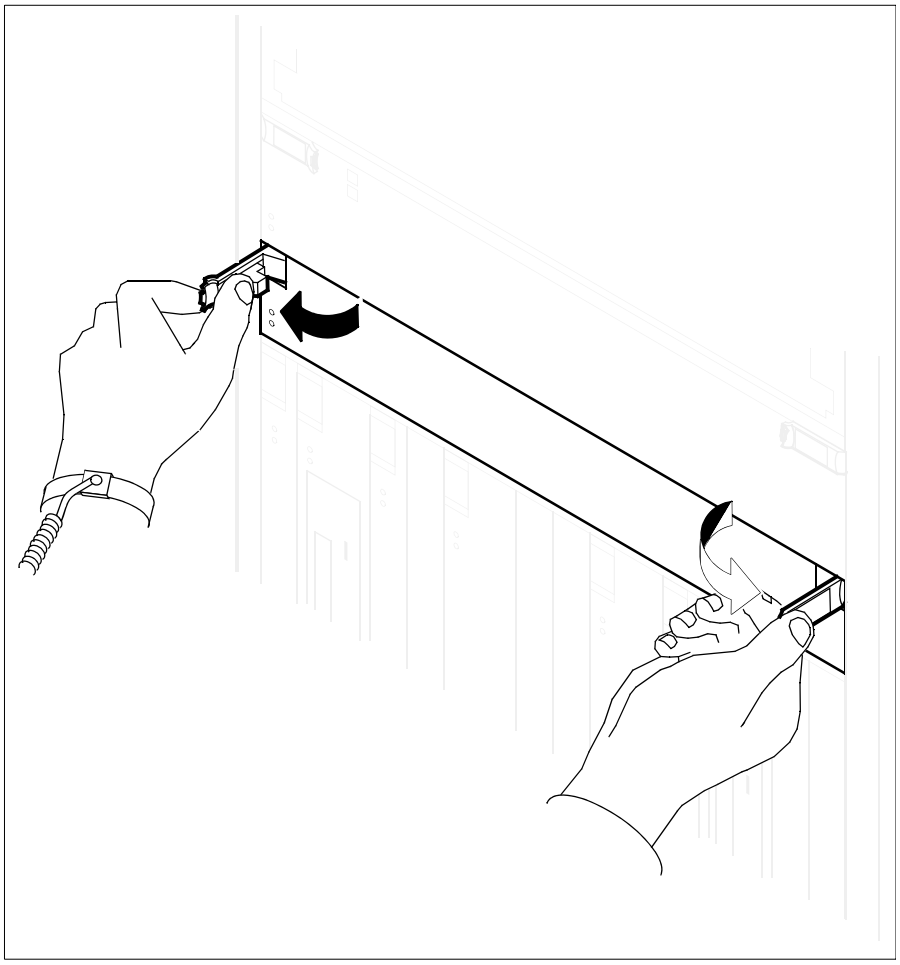
WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

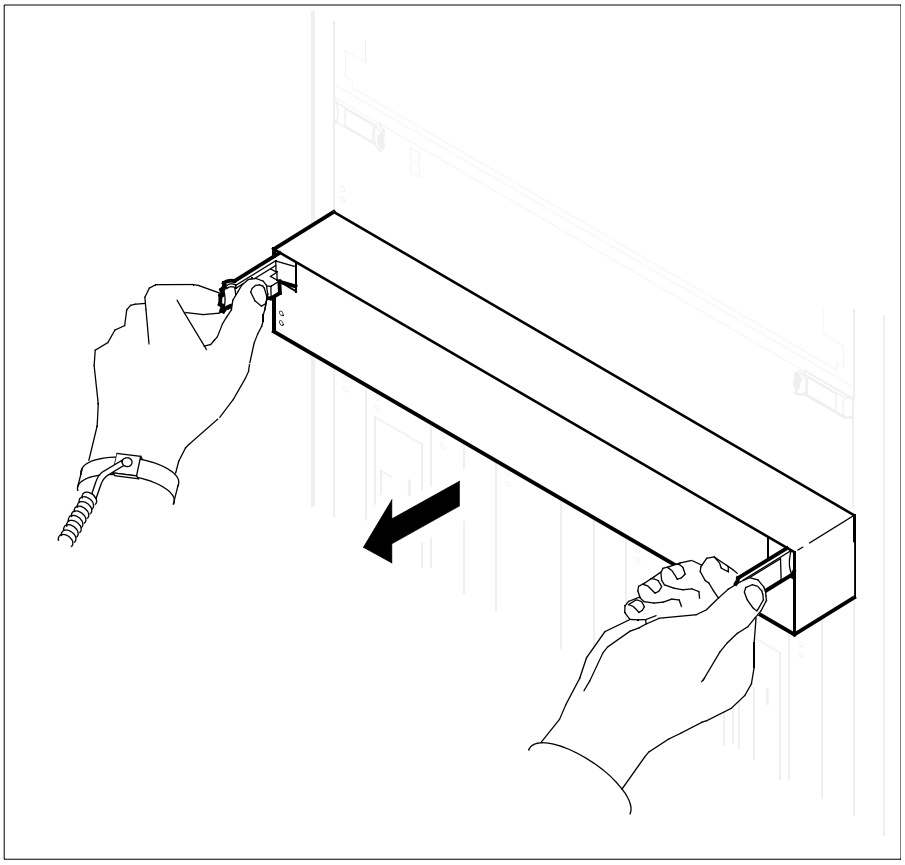
8 Depress the tips of the locking levers on the face of the fan tray.



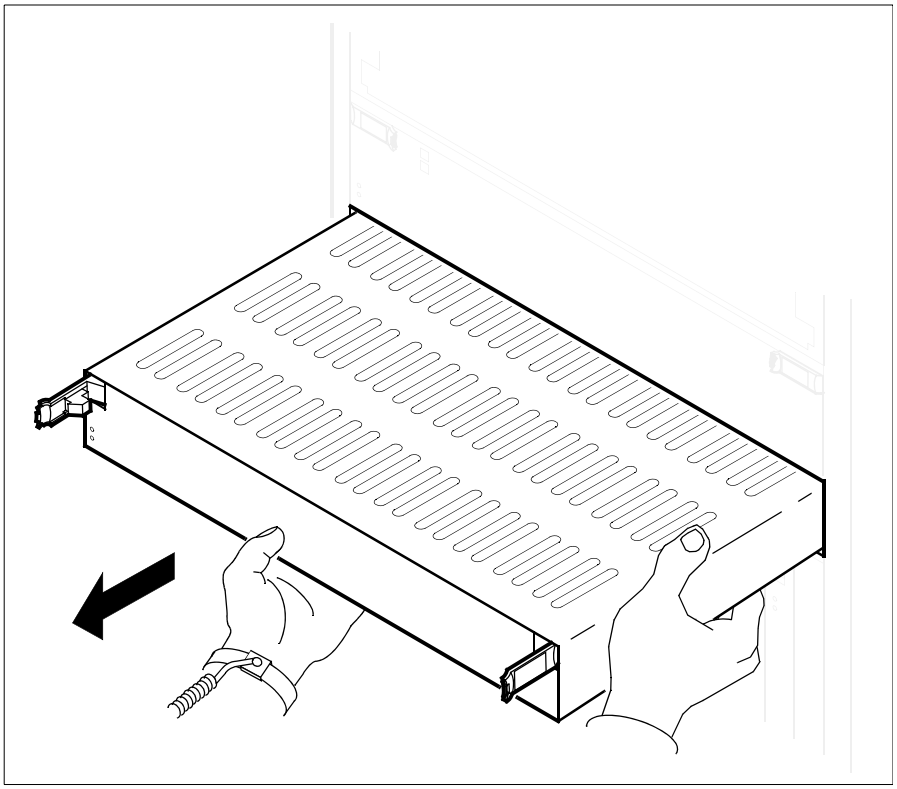
9 Open the locking levers on the face of the fan tray by moving the levers outwards.



10 While grasping the locking levers, gently pull the fan tray towards you until the fan tray protrudes about 2 inches (5 cm) from the equipment shelf.



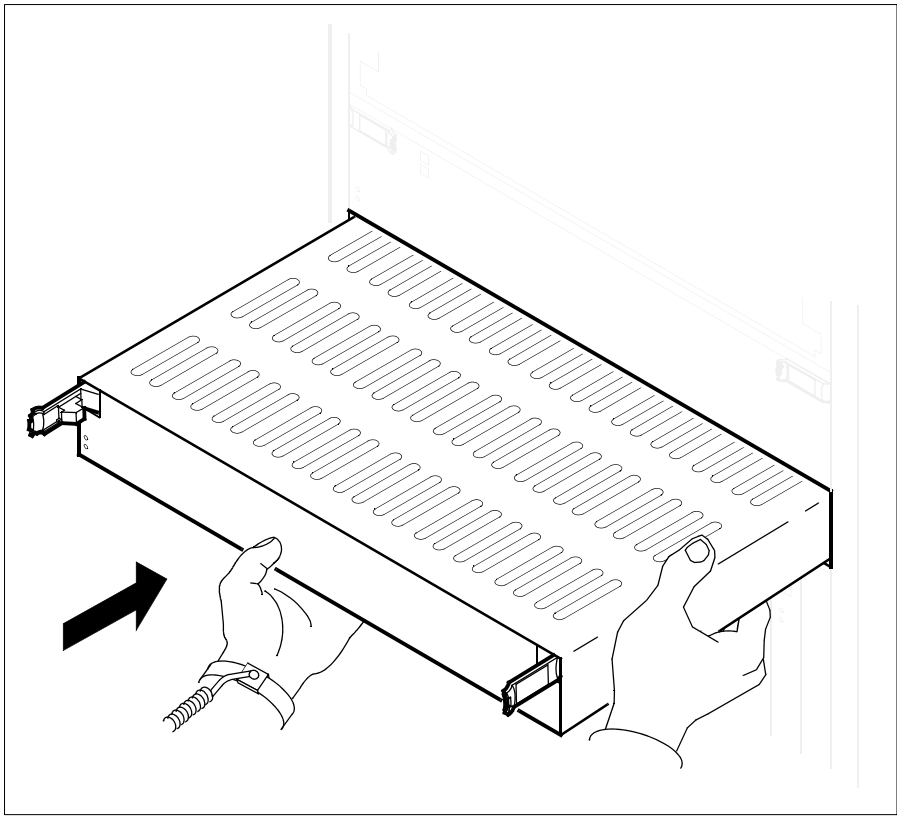
11 Hold the fan tray by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the fan tray toward you until it clears the shelf.



12 Place the fan tray you have removed in an ESD protective container.

13 Insert the replacement fan tray into the shelf.

14 Gently slide the fan tray into the shelf until it is almost inserted.



15 Partially close the locking levers, and continue to slide the fan tray until it is fully inserted into the shelf. The locking levers lock by themselves when the fan tray is fully inserted.

At the local or remote VT100 console

16 Return the fan tray to service:

```
> rts <domain> fan
```

where

<domain>
is the number of the domain where the fan tray resides (0 or 1).

Note: This syntax is valid for single chassis configurations (main chassis only). For systems with a main chassis and an I/O expansion chassis, the parameter “fan” must be specified

as either “fan1” or “fan1”, for the main or I/O expansion chassis respectively.

Example response:

```
Hardware RTS : Domain 1 Device FAN - Command
initiated.
Please wait...

Hardware RTS : Domain 1 Device FAN - Command
complete.
```

Note: At the hardware level of the maintenance interface, the state of the fan tray changes to a dot (.), indicating the fan tray has returned to service. The in-service LED on the fan tray turns green. The out-of-service LED only applies to a fan tray in the main chassis, as the fan trays in the I/O expansion chassis do not have system LEDs.

17 You have completed this procedure.

Replacing a standalone X.25 controller module

Purpose

Use this procedure to replace a standalone X.25 controller module (SYNC X.25).

Application

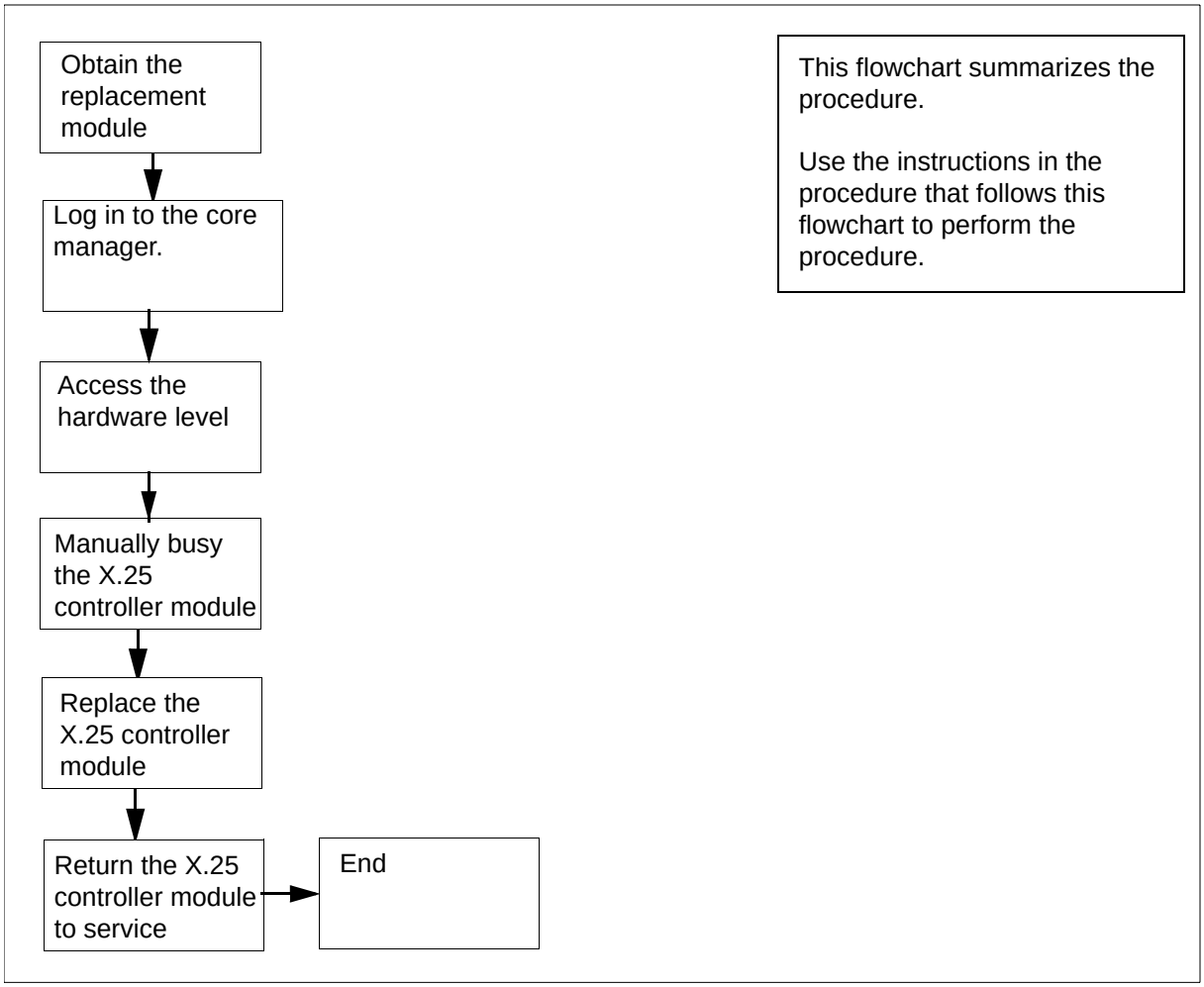
The X.25 controller module (SYNC X.25) is located at the front of the main, or expansion, chassis of the core manager.

Nortel PEC	Name
NTRX50FY	X.25 SYNC controller module

Action

The following flowchart is a summary of the procedure. To replace the X.25 controller module, use the instructions in the procedure that follows the flowchart.

Summary of Replacing an X.25 controller module



Replacing an X.25 controller module

Obtain a replacement X.25 controller module

1 Obtain a replacement X.25 controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed on the top locking lever.

At the local or remote VT100 console

2 Log into the core manager as the root or maintenance user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the hardware (Hw) level:

> hw

5 Use the following list to determine the domain number. The domain number is:

- 0 if the module is located in one of slots
  - — 1 to 6 on the main chassis, or
  - — 1 to 8 on the expansion chassis
- 1 if the module is located in one of slots
  - — 10 to 16 on the main chassis, or
  - — 9 to 16 on the expansion chassis

6 Busy the X.25 controller module:

> bsy <domain_no> X25

where

<domain_no>
is the domain number (0 or 1) of the X.25 controller module that you are replacing

Example response:

```
Hardware Bsy - Domain 0 Device X25
This action will bring service down for all X.25
Ports
in I/O domain 0.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

7 Confirm the Bsy command:

> y

Example response:

```
Hardware Bsy : Domain 0 Device X25 - Command
initiated.
Please wait...
```

After the system completes the Bsy command, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then to *complete*.

Example response:

```
Hardware Bsy : Domain 0 Device X25 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the X.25 controller module changes to “M”.

At the front of the core manager

8

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

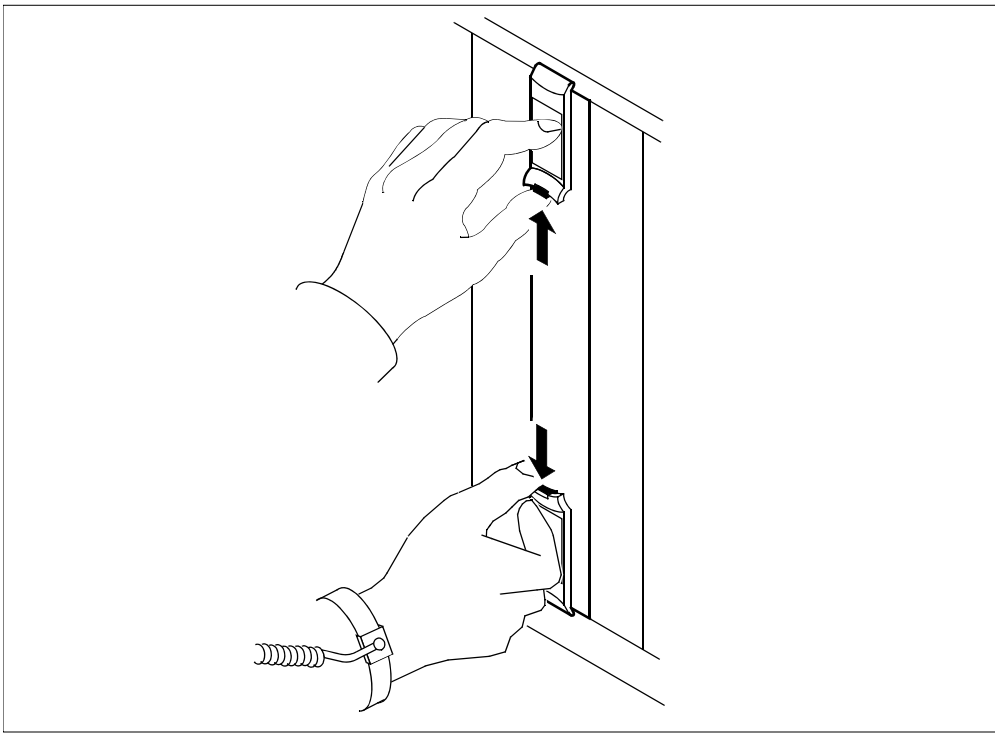
Put on an electrostatic discharge grounding wrist strap.

9

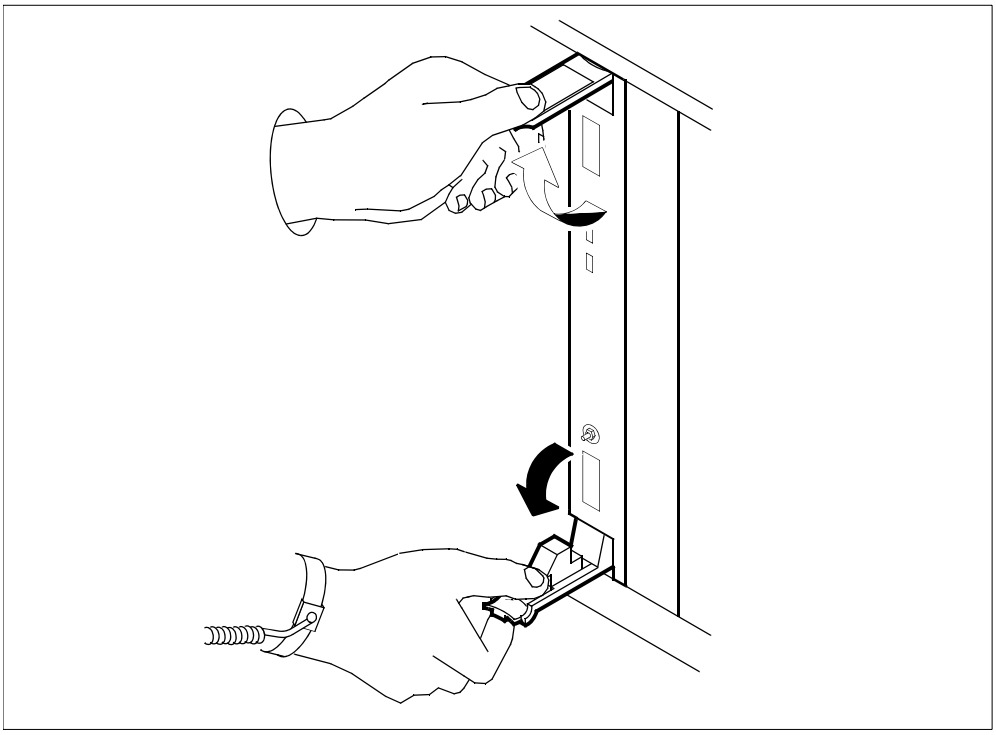
CAUTION
Potential service interruption
Unseat only the X.25 controller module that you busied in step 6, and not the corresponding X.25 controller module in the other I/O domain. The in-service LED on the module busied in step 6 is off, and the out-of-service LED is on (red).

Unseat the correct X.25 controller module.

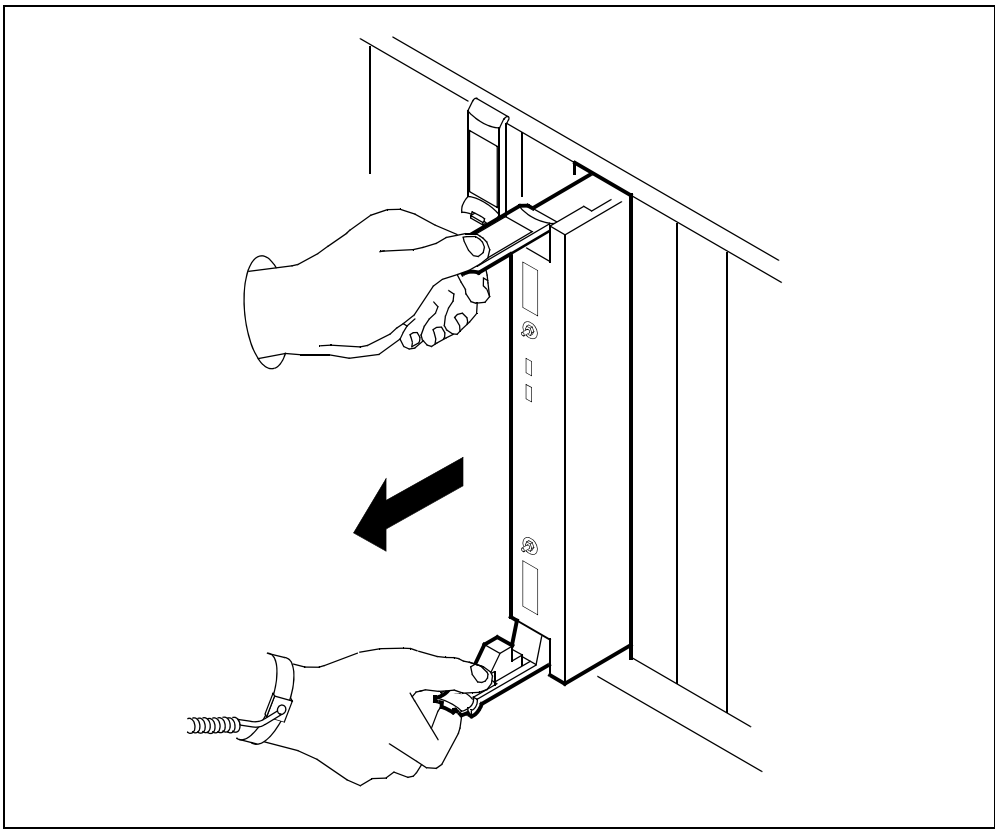
10 Depress the tips of the locking levers on the face of the X.25 controller module.



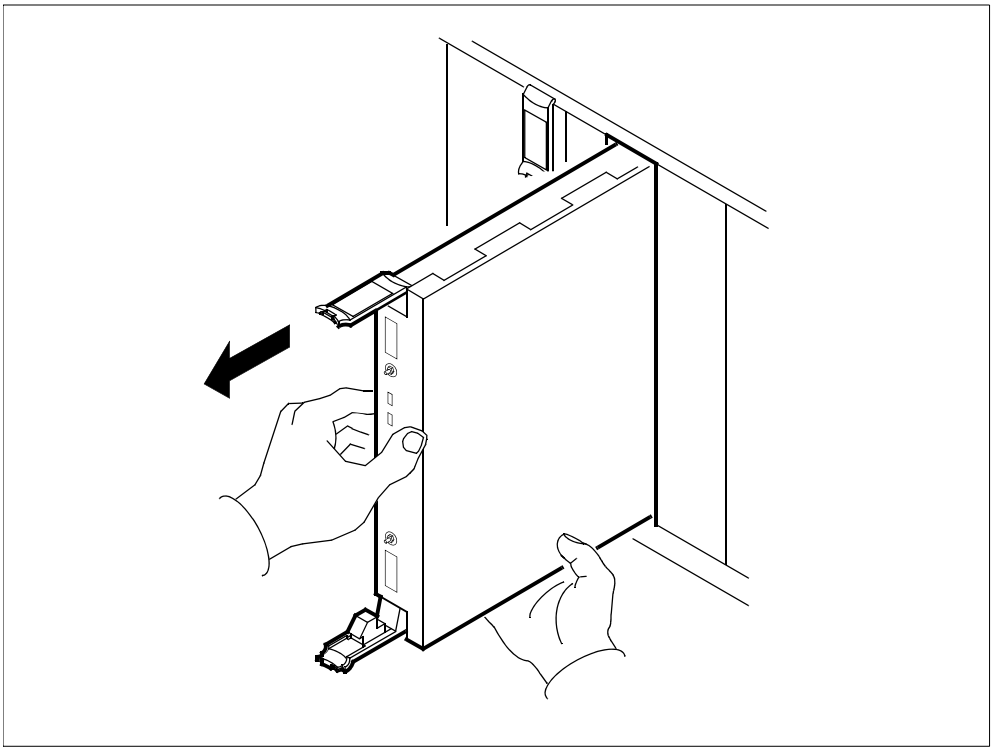
11 Open the locking levers on the face of the module by moving the levers outwards.



12 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 inches (5 cm) from the core manager shelf.



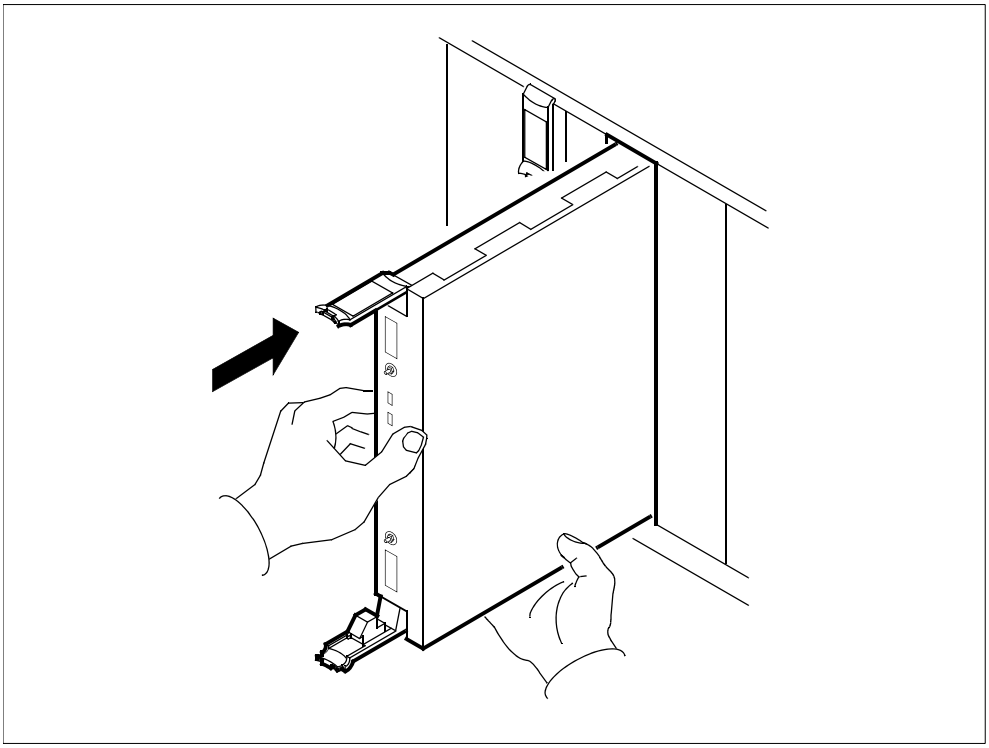
13 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



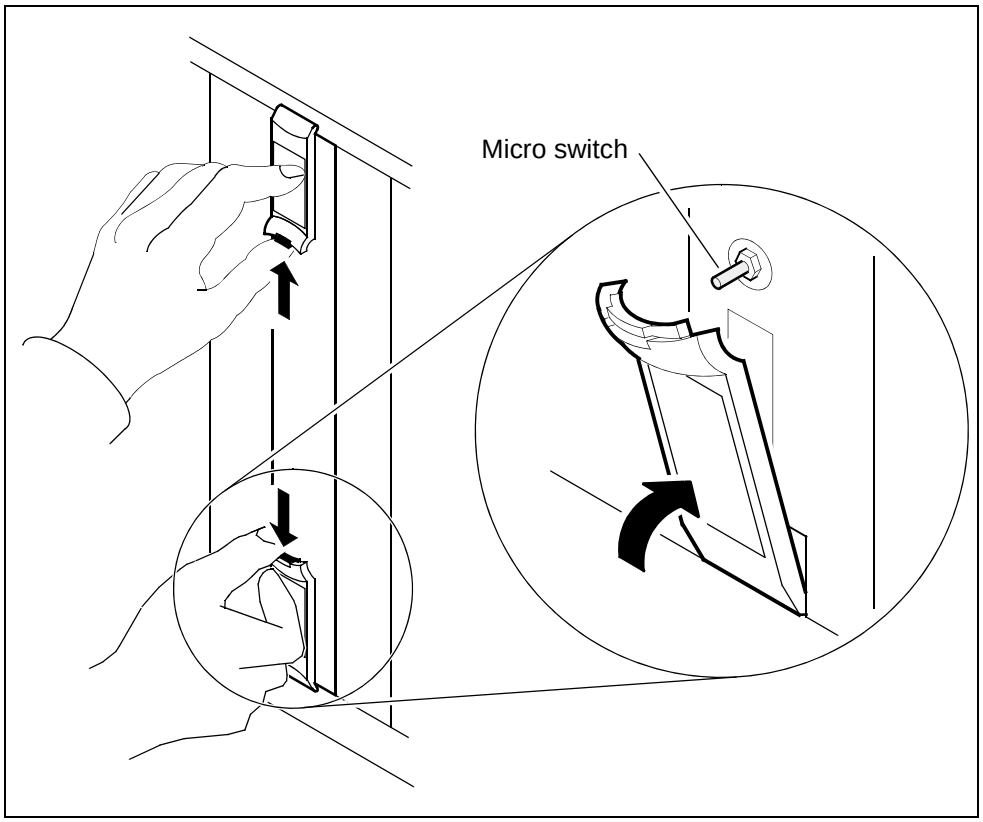
14 Place the module you have removed in an ESD protective container.

15 Insert the replacement module into the core manager shelf.

16 Gently slide the module into the shelf until it is fully inserted.



17 Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



At the local or remote VT100 console

18 Return the X.25 controller module to service:

```
> rts <domain_no> X25
```

where

<domain_no>
is the SDM domain number (0 or 1) of the X.25 controller module you replaced in step 6.

Example response:

```
Hardware RTS : Domain 0 Device X25 - Command
initiated.
Please wait...
```

After the system completes the RTS command, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then to *complete*.

Example response:

```
Hardware RTS : Domain 0 Device X25 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the X.25 controller module changes to a dot (.), indicating the module has returned to service. The in service LED on the X.25 controller module is on (green).

19 You have completed this procedure.

Replacing a standalone X.25 personality module

Purpose

Use this procedure to replace a standalone X.25 personality module (SYNC X25 PM).

Application

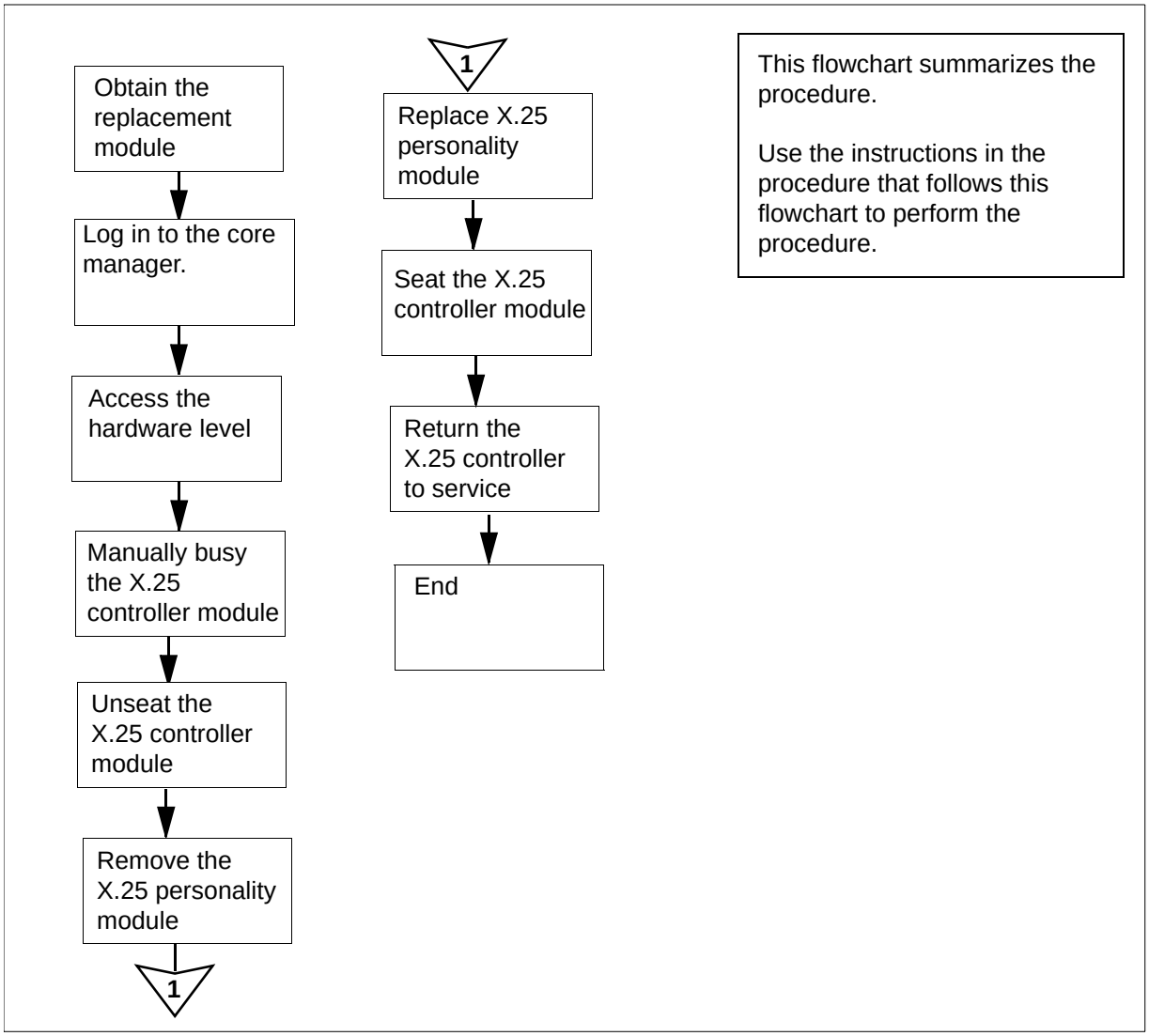
Use this procedure to replace a standalone X.25 personality module (SYNC X25 PM), located at the rear of the main or expansion chassis of the core manager.

Nortel PEC	Name
NTRX50FZ	X.25 SYNC personality module

Action

The following flowchart provides a summary of the procedure. To replace the X.25 personality module, use the instructions in the procedure that follows the flowchart.

Summary of replacing a standalone X.25 personality module



Replacing a standalone X.25 personality module

Obtain a replacement X.25 personality module

1 Obtain a replacement X.25 personality module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed at the top of the module.

At the local or remote VT100 console

2 Log into the core manager as the root or maintenance user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the hardware (Hw) level:

```
> hw
```

5 Use the following list to determine the domain number. The domain number is

- 0 if the module is located in one of the slots
  - 1 to 6 on the main chassis or
  - 1 to 8 on the expansion chassis
- 1 if the module is located in one of the slots
  - 10 to 16 of the main chassis, or
  - 9 to 16 on the expansion chassis

6 Busy the X.25 controller module:

```
> bsy <domain_no> X25
```

where

<domain_no>
is the SDM domain number (0 or 1) of the X.25 personality module you are replacing

Example response:

```
Hardware Bsy - Domain 0 Device X25
This action will bring service down for all X.25
Ports
in I/O domain 0.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

7 Confirm the Bsy command:

```
> y
```

Example response:

```
Hardware Bsy : Domain 0 Device X25 - Command
initiated.
Please wait...
```

After the system completes the Bsy command, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *to complete*.

Example response:

```
Hardware Bsy : Domain 0 Device X25 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the X.25 controller module changes to “M”. The out-of-service LED on the module is on (red).

At the front of the core manager

8

WARNING
Static electricity damage
Wear an electrostatic (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

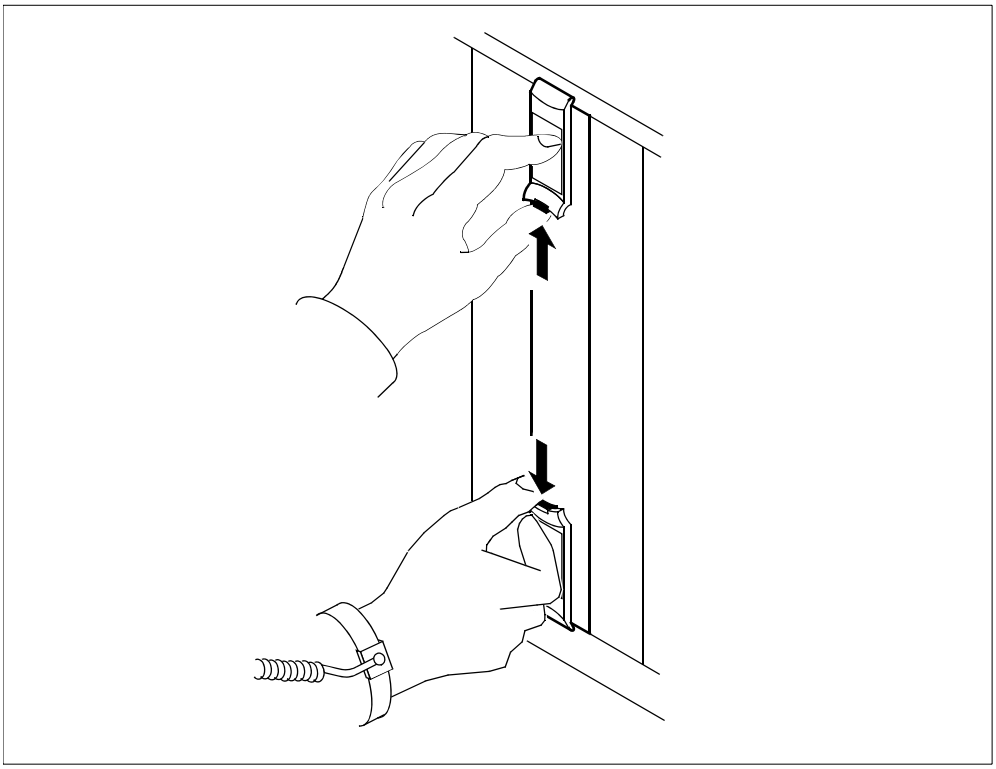
Put on an electrostatic grounding wrist strap.

9

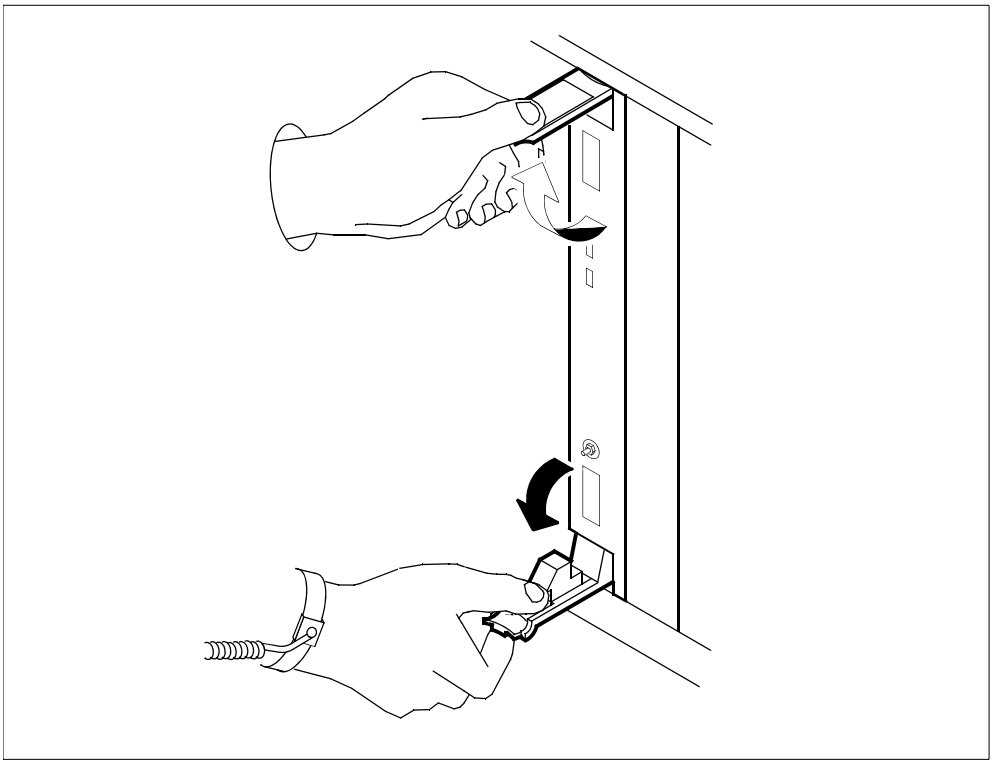
CAUTION
Potential service interruption
Unseat only the X.25 controller module that you busied in step 6, and not the corresponding X.25 controller module in the other domain. The in-service LED on the module busied in step 6 is off, and the out-of-service LED is on (red).

Unseat the correct X.25 controller module.

10 Depress the tips of the locking levers on the face of the X.25 controller module.



11 Open the locking levers on the face of the X.25 controller module by moving the levers outwards.



At the back of the core manager

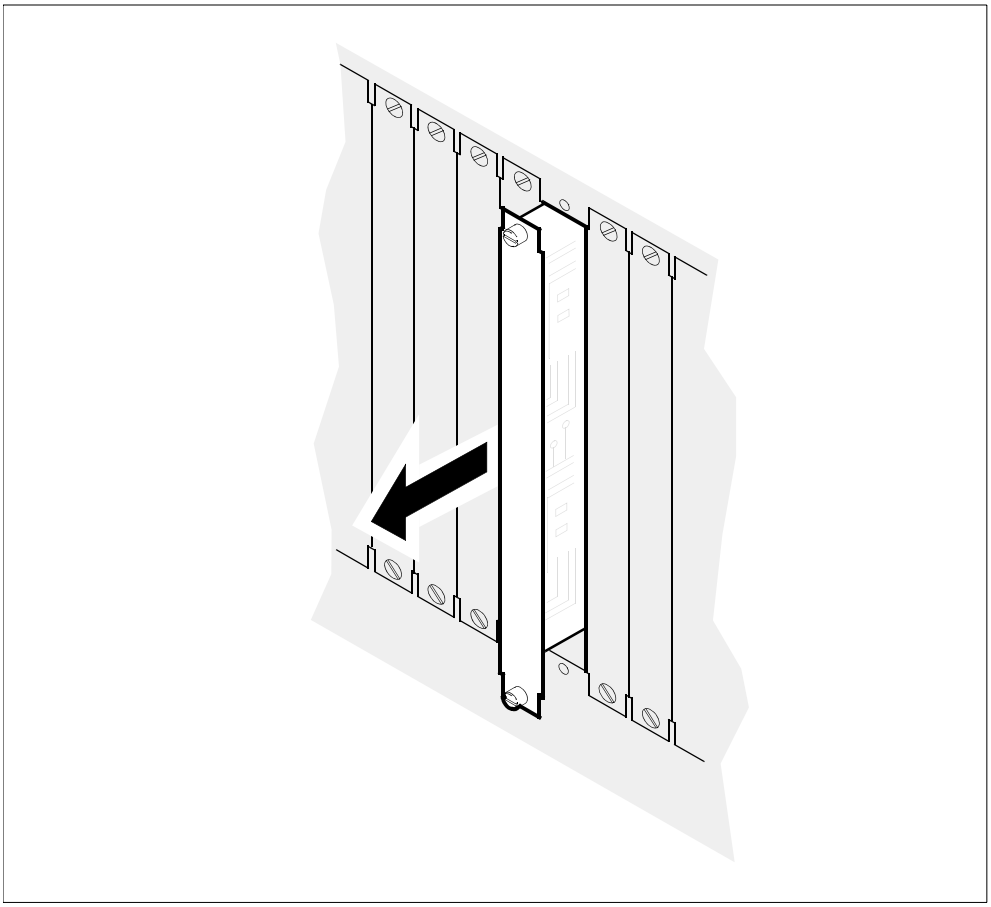
12 Loosen the two thumbscrews located at the top and the bottom of the X.25 personality module.

Note: The thumbscrews are captive and cannot be removed from the module.

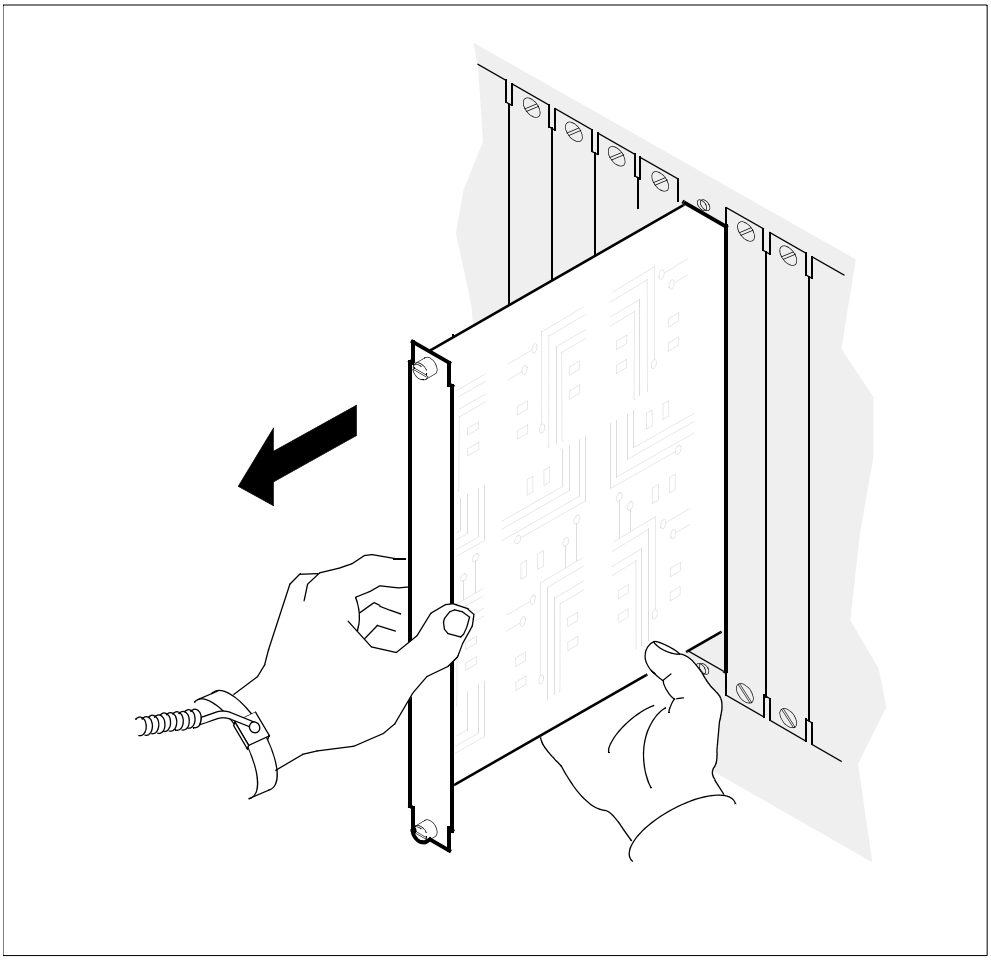
13 Disconnect the X.25 modem connection cables from the X.25 personality module.

Note: You need to disconnect either one or two modem cables, depending on whether the X.25 card is commissioned to use one or both of its X.25 ports.

14 While grasping the thumbscrews, gently pull the X.25 personality module towards you until it protrudes about 2 inches (5 cm) from the core manager shelf.



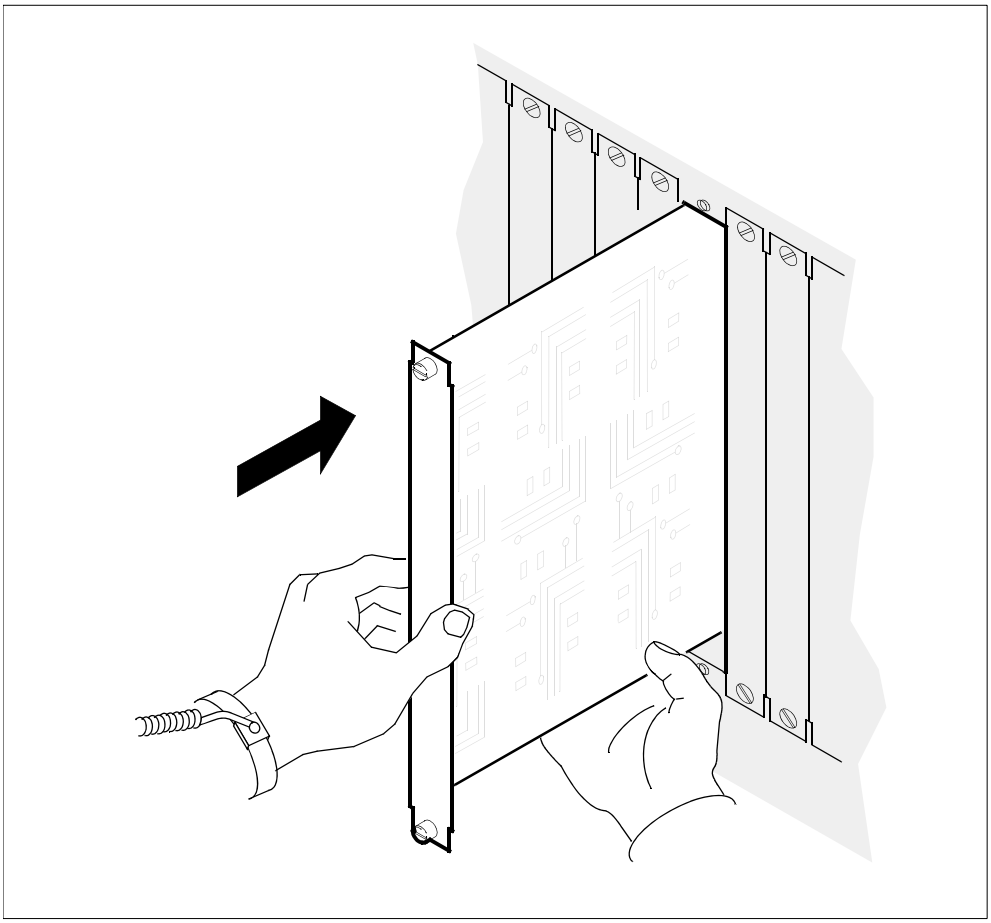
15 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the X.25 personality module toward you until it clears the shelf.



16 Place the X.25 personality module you have removed in an ESD protective container.

17 Insert the replacement X.25 personality module into the core manager shelf.

18 Gently slide the X.25 personality module into the shelf until it is fully inserted.

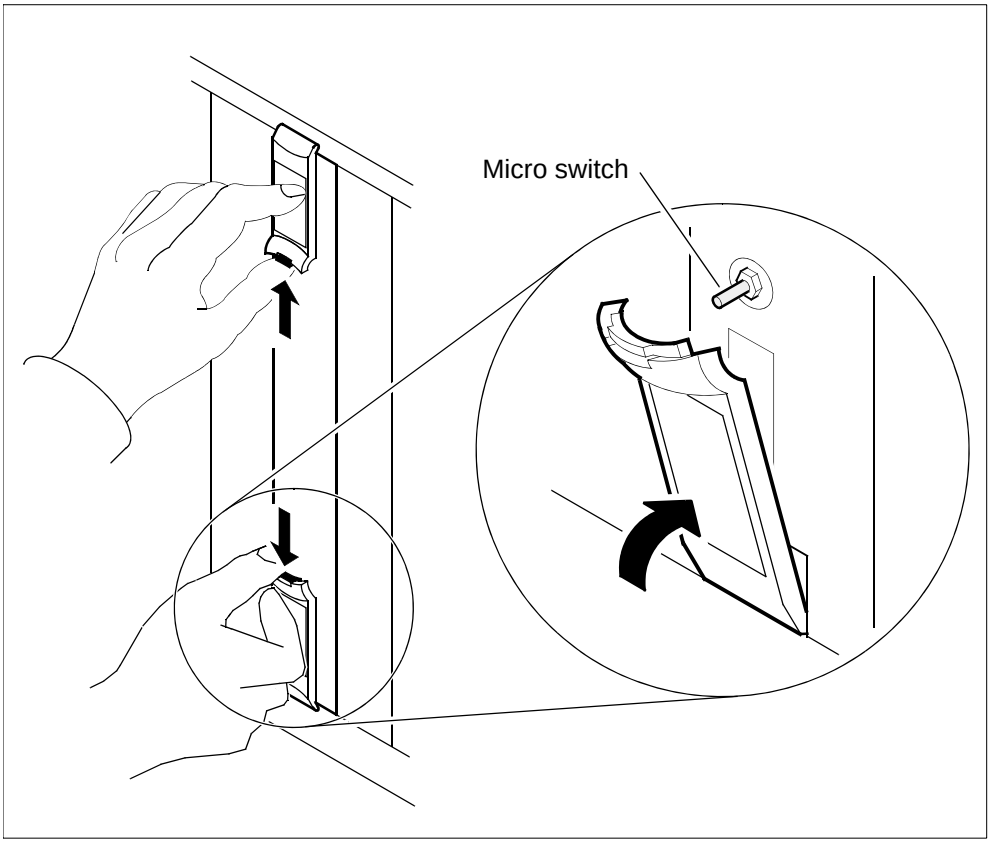


19 Tighten the thumbscrews at the top and the bottom of the X.25 personality module.

20 Reconnect the X.25 modem connection cables to the X.25 personality module.

At the front of the core manager

21 Close the locking levers to secure the X.25 controller module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



At the local or remote VT100 console

22 Return the X.25 controller module to service:

```
> rts <domain_no> X25
```

where

<domain_no>
is the SDM domain number (0 or 1) of the X.25 controller module that you replaced. (See step 6.)

Example response:

```
Hardware RTS : Domain 0 Device X25 - Command
initiated.
Please wait...
```

After the system completes the RTS command, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *to complete*.

Example response:

```
Hardware RTS : Domain 0 Device X25 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the X.25 controller module changes to a dot (.), indicating the module has returned to service. The in-service LED on the X.25 controller module is on (green).

23 You have completed this procedure.

Replacing an interconnect module

Purpose

Use this procedure to replace an interconnect module (ICM) located at the rear of the main or I/O expansion chassis of the core manager.

Application

Select the applicable ICM.

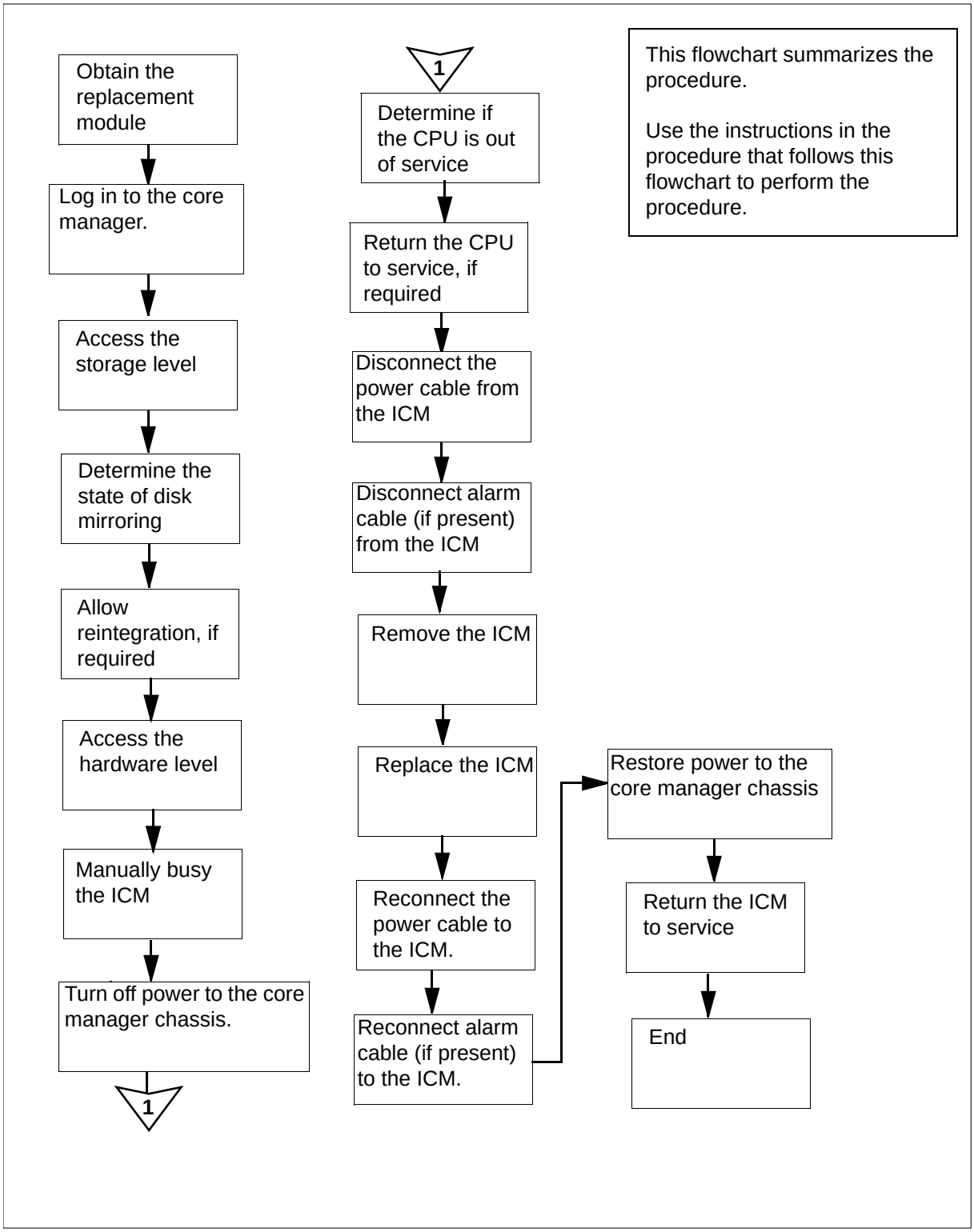
Nortel PEC	Name
NTRX50FG	Interconnect module in domain 0 . Located on the right-hand side at the rear of the main chassis or I/O expansion chassis.
NTRX50FH	Interconnect module in domain 1. Located on the left-hand side at the rear of the main chassis or I/O expansion chassis.

Note: If you are replacing the ICM because it is indicated as failed (F) at the hardware menu level of the core manager maintenance interface, verify that the ICM failure has not been caused by a loss of DC input power.

Action

The following flowchart is a summary of the procedure. To replace the interconnect module, use the instructions in the procedure that follows the flowchart.

Summary of replacing an interconnect module



Replacing an interconnect module

Obtain a replacement interconnect module

1 Obtain a replacement interconnect module. Ensure that the replacement has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed at the top left-hand side of the ICM.

At the local or remote VT100 console

2 Log into the core manager as the root or maint user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the storage level:

```
> storage
```

Example response:

```
Disk mirroring
(rootvg):                Integrating
```

5 Verify the disk mirroring status for each volume group commissioned on the core manager.

If the status of disk mirroring indicates	Do
Integrating	step 6
Mirrored or Not Mirrored	step 7

6

CAUTION
Potential loss of service
Do not continue this procedure while the disks are reintegrating. If you interrupt power to one ICM during the reintegration process, you will cause a reintegration failure that may require service-affecting manual recovery action.

The hard disks that provide mirrored storage for the system are reintegrating.

Wait until the reintegration process is complete before continuing this procedure. The reintegration process takes about

20 minutes for each Gbyte of data. The actual time required depends on the amount of data in the volume group, and the current processor load.

7 Access the hardware (Hw) level:

```
> hw
```

8 Busy the ICM:

```
> bsy <domain_no> icm
```

where

<domain_no>
is the domain number of the ICM (0 or 1)

Example response:

```
Hardware Bsy - Domain 0 Device ICM
This action will affect all devices in I/O
domain 0.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

Note: This syntax is valid for single chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

9 Confirm the busy command:

```
> y
```

Note 1: When you busy the ICM in a domain, all subtending devices with the exception of the CPU (FAN, ETH, DSK1, DSK2, DSK3, DAT, and 512) in that domain are put in the CBsy state.

Note 2: For systems with an IO expansion chassis:

- the second ICM in the domain displays an F to indicate that ICM 2 is in a fault state.
- all subtending devices with the exception of the CPU (FAN, ETH, DSK1, DSK2, DSK3, DAT, and 512) in that domain are placed in CBsy State.

Example response:

```
Hardware Bsy : Domain 0 Device ICM - Command
initiated.
Please wait...
```

```
Hardware Bsy : Domain 0 Device ICM - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the interconnect module changes and all subtending devices changes to “M”. The out-of-service LED on the module is on (red).

At the front of the MSP

10 Turn off power to the core manager chassis where the ICM is located.

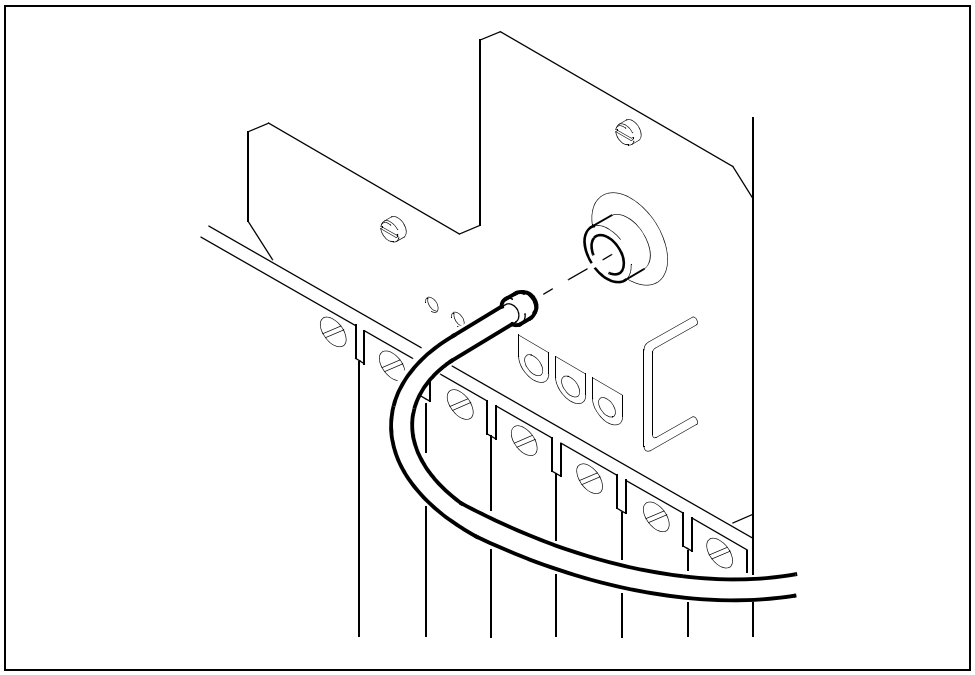
If you are replacing	Turn
Domain 0 ICM in the main chassis	top left breaker off
Domain 0 ICM in the I/O expansion chassis	bottom left breaker off
Domain 1 ICM in the main chassis	top right breaker off
Domain 1 ICM in the I/O expansion chassis	bottom right breaker off

At the back of the core manager

11

CAUTION
Potential service interruption
Ensure that you disconnect power to only the ICM you are replacing. If you disconnect power to the other ICM, the entire core manager shuts down.

Disconnect the power cable from the ICM you are replacing.



At the local or remote VT100 console

12 Determine if one CPU controller module has dropped out of service (indicated by an “F” (failed) under its header at the hardware menu level).

If	Do
one CPU is out of service	step 13
both CPUs are in service	step 15

13

CAUTION
Possible service degradation
If an ICM fails, the corresponding CPU controller module may be brought down by the system and must be returned to service manually.

Return the out-of-service CPU to service, and start CPU reintegration:

```
> rts <domain_no> CPU
```

where

<domain_no>
is the domain number (0 or 1) of the CPU controller module that you are returning to service

Return the CPU controller module to service at the hardware (Hw) menu level of the core manager maintenance interface, or the platform MAP level under the core manager MAP level

Example response:

```
Hardware RTS : Domain 0 Device CPU - Command
initiated.
Please wait...

Hardware RTS : Domain 0 Device CPU - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the CPU state changes to “S”, indicating that the CPUs are reintegrating. The reintegration process takes about 2 minutes to complete, after which the CPU status changes to in-service (indicated by a dot). The in-service LED on ICM 0 is on (green).

14 Check if the ICM has an alarm cable.

If the ICM you are replacing	Do
has an alarm cable	step 15
does not have an alarm cable	step 17

Note: If you are replacing an ICM in an I/O expansion chassis, the alarm cable is not present.

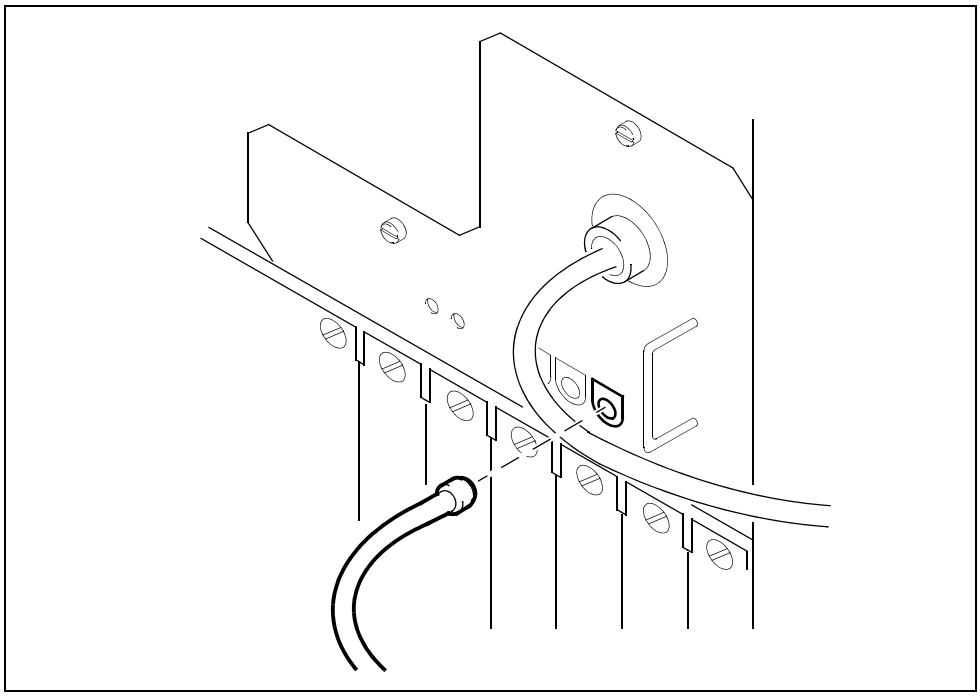
At the back of the core manager

15

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist.

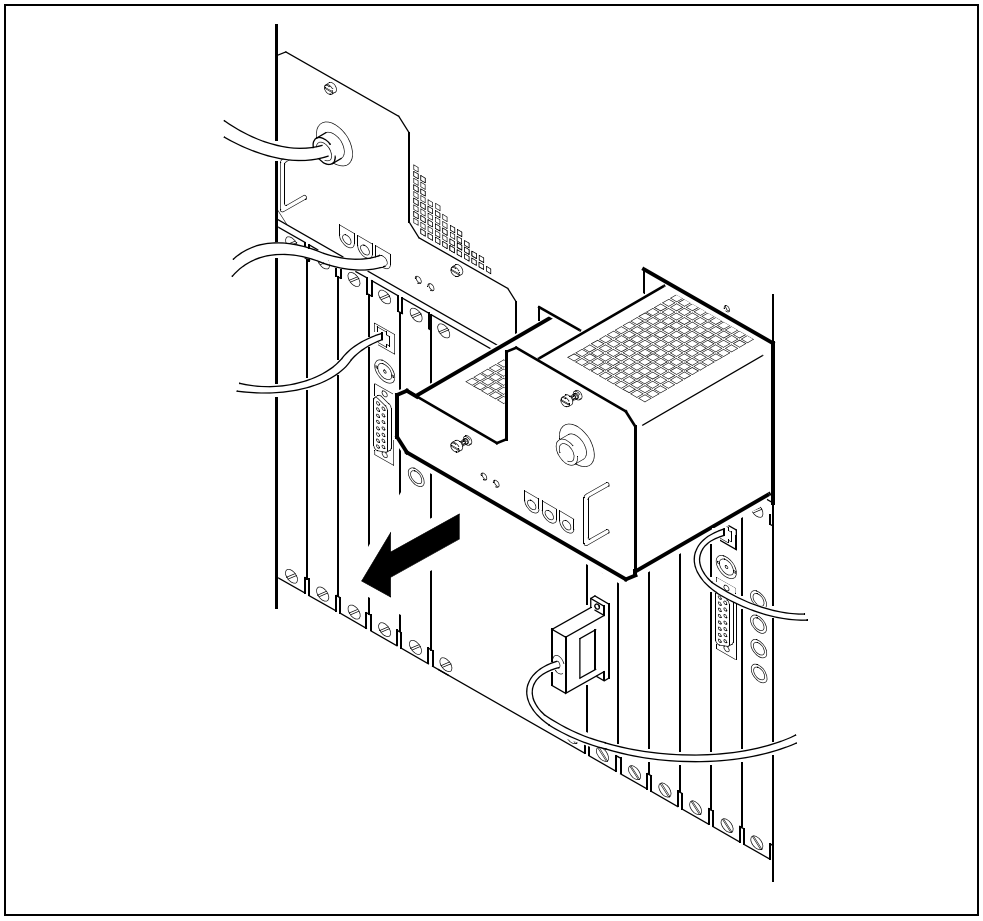
16 Disconnect the alarm cable from the ICM you are replacing.



17 Loosen the two thumbscrews on the ICM you are replacing.

Note: The thumbscrews are captive and cannot be removed from the module.

18 Remove the ICM by gently sliding it out of the chassis.



19 Place the ICM you have removed in an ESD protective container.

20 Gently insert and seat the replacement ICM.

21 Secure the replacement ICM by tightening the two captive screws.

22 Reconnect the alarm cable, if present, to the ICM.

23 Reconnect the power cable to the ICM.

At the front of the MSP

24 Restore power to core manager chassis.

If you are replacing	Turn
Domain 0 ICM in the main chassis	top left breaker on

If you are replacing	Turn
Domain 0 ICM in the I/O expansion chassis	bottom left breaker on
Domain 1 ICM in the main chassis	top right breaker on
Domain 1 ICM in the I/O expansion chassis	bottom right breaker on

At the local or remote VT100 console

25 Return the ICM to service:

```
> rts <domain_no> icm
```

where

<domain_no>
is the domain number of the ICM (0 or 1)

Note: This syntax is valid for single chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

Example response:

```
Hardware RTS : Domain 0 Device ICM - Command
initiated.
Please wait...

Hardware RTS : Domain 0 Device ICM - Command
complete.
```

26 Wait approximately five minutes for the interconnect modules to reintegrate. Check the LEDs on the ICM that you replaced.

If	Do
the ICM in-service LED is on (solid green), and the out-of-service LED is off	step 28
the ICM in-service LED is off, and the out-of-service LED is on (solid red or flashing red)	contact your next level of support
both LEDs on the CPU controller module are off	step 27

27 Reseat the ICM that you replaced, and repeat step 25.

28 You can determine the disk mirroring status for each volume group commissioned on the core manager by accessing the storage menu level of the core manager maintenance interface. Access the storage menu level:

```
> storage
```

Example response:

```
Volume Groups        Status
Free (MB)  rootvg              Integrating
(12%)      2252    datavg
           Integrating (5%)       1488
```

Note: The reintegration process takes several minutes to begin and takes approximately 20 minutes per Gigabyte to complete. The actual time required depends on the amount of data in the volume group, and the current processor load.

29 You have completed this procedure.

Replacing an NTRX42 breaker module

The NTRX42 breaker module resides in a modular supervisory panel (MSP). The NTRX42 contains two circuit breakers of -48v or -60v that provide two 15A power feeds. The primary functions of the NTRX42 are as follows:

- monitor and detect converter failures
- trip breakers when over-current conditions occur
- trip breakers upon converter failure
- provide termination points for power distribution center (PDC) feeds
- provide battery feed samples for the alarm module
- respond to automatic recovery from low battery (ARLB) conditions

The following procedure outlines the steps that must be performed to replace an NTRX42 breaker module.

Prerequisites

You must be a user authorized to perform fault-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

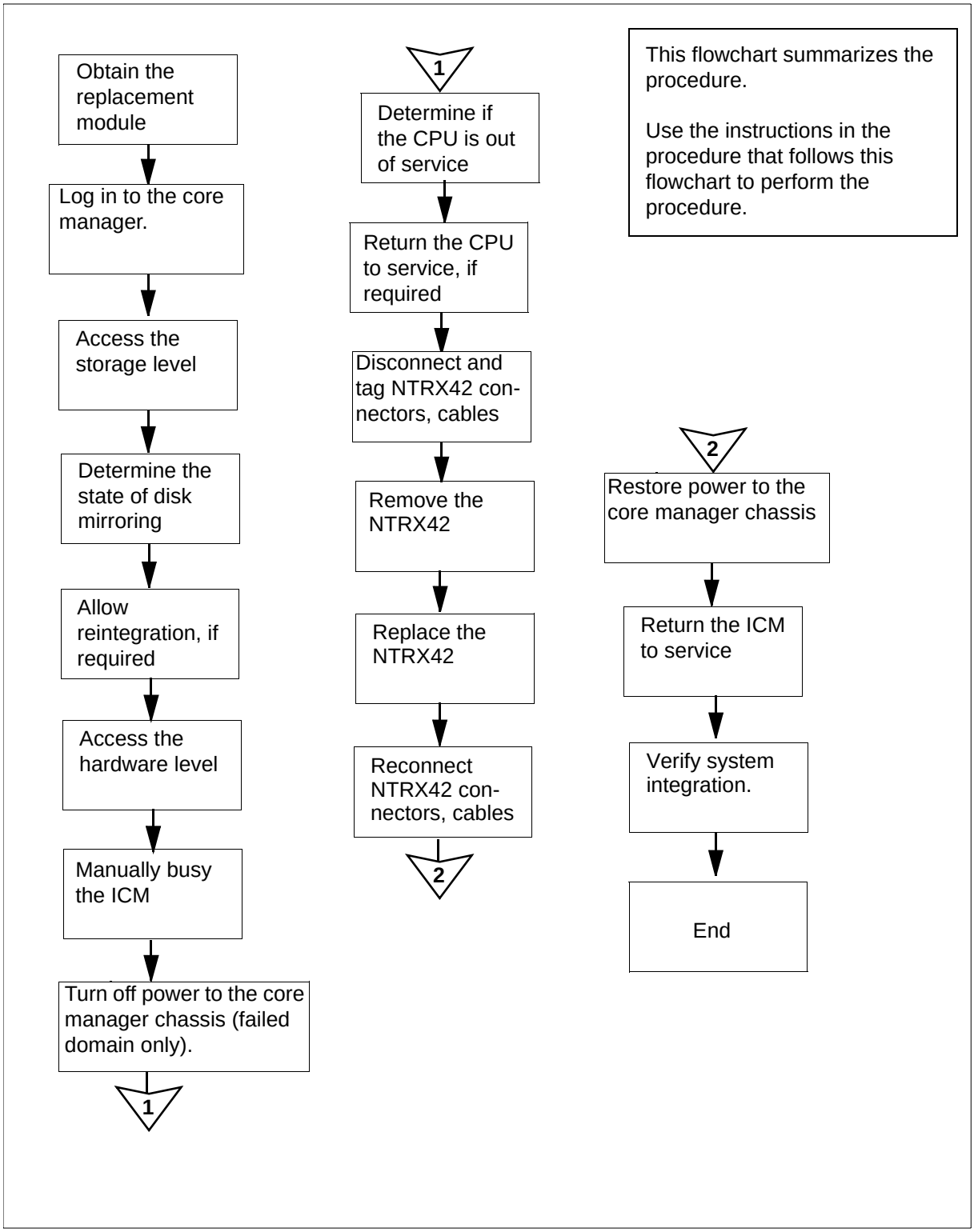
Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

Procedure

The following flowchart is a summary of the procedure. To replace the NTRX42 breaker module, use the instructions in the procedure that follows the flowchart.

Summary of replacing an NTRX42 breaker module



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

Replacing an NTRX42 breaker module

At the local or remote VT100 console

1 Proceed only if you have been directed to this card replacement procedure from a step in a maintenance procedure, are using the procedure for verifying or accepting cards, or have been directed to this procedure by your maintenance support group.

2 Obtain a replacement card. Verify that the replacement card has the same product equipment code (PEC), including suffix, as the card that is to be removed.

3 Log on to the CS 2000 Core Manager as a user authorized to perform fault-admin actions.

4 Query the SDM faults and status of all applications. Record the results for later verification:

```
querysdm flt
querysdm loads
```

5 Access the storage level of the SDM maintenance interface:

```
sdmmtc storage
```

Example response:

```
Volume Group   Status            Free(MB) / threshold
rootvg         Integrating (3%)   5232    /   400 !
datavg         Mirrored           16752   /   400
```

6 Verify the disk mirroring status for each volume group commissioned on the core manager.

If the status of disk mirroring indicates	Do
Integrating	step 7
Mirrored	step 8
Not Mirrored	Contact your next level of support before continuing with this procedure.

7

CAUTION
Potential loss of service
Do not continue this procedure while the disks are reintegrating. If you interrupt power to one ICM during the reintegration process, you will cause a reintegration failure that may require service-affecting manual recovery action.

The hard disks that provide mirrored storage for the system are reintegrating.

Wait until the reintegration process is complete before continuing this procedure. The reintegration process takes about 20 minutes for each Gbyte of data. The actual time required depends on the amount of data in the volume group, and the current processor load.

8 Access the hardware (Hw) level:

hw

9 Busy the ICM associated with the NTRX42 to be replaced. Use the following table to determine which ICM to busy.

ICM	Breaker
Domain 0 ICM in the main chassis	top left breaker
Domain 0 ICM in the I/O expansion chassis	bottom left breaker
Domain 1 ICM in the main chassis	top right breaker
Domain 1 ICM in the I/O expansion chassis	bottom right breaker

bsy <domain_no> icm

where

<domain_no>
is the domain number of the ICM (0 or 1)

Example response:

```
Hardware Bsy - Domain 0 Device ICM
This action will affect all devices in I/O
```

```
domain 0.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

Note: This syntax is valid for single chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

10 Confirm the busy command:

y

Note 1: When you busy the ICM in a domain, all subtending devices with the exception of the CPU (FAN, ETH, DSK1, DSK2, DSK3, DAT, and 512) in that domain are put in the CBsy state.

Note 2: For systems with an IO expansion chassis:

- the second ICM in the domain displays an F to indicate that ICM 2 is in a fault state.
- all subtending devices with the exception of the CPU (FAN, ETH, DSK1, DSK2, DSK3, DAT, and 512) in that domain are placed in CBsy State.

Example response:

```
Hardware Bsy : Domain 0 Device ICM - Command
initiated.
Please wait...

Hardware Bsy : Domain 0 Device ICM - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the interconnect module changes and all subtending devices changes to “M”. The out-of-service LED on the module is on (red).

At the front of the MSP

11 Determine the faulty circuit breaker on the MSP and switch both breakers on that circuit card to the OFF position. Safety tag the front of the circuit breaker.

12 An alarm may sound in the central office. If this occurs, silence the alarm from the DMS terminal:

SIL

At the back of the core manager

13

CAUTION
Potential service interruption
Ensure that you disconnect power to only the ICM you are replacing. If you disconnect power to the other ICM, the entire core manager shuts down.

Power down and then safety tag the corresponding main fuse in the PDC cabinet.

At the local or remote VT100 console

14 Determine if one CPU controller module has dropped out of service (indicated by an “F” (failed) under its header at the hardware menu level).

If	Do
one CPU is out of service	step 15
both CPUs are in service	step 16

15

CAUTION
Possible service degradation
If an ICM fails, the corresponding CPU controller module may be brought down by the system and must be returned to service manually.

Return the CPU controller module to service at the hardware (hw) menu level of the core manager maintenance interface.

```
rts <domain_no> CPU
```

where

<domain_no>
is the domain number (0 or 1) of the CPU controller module that you are returning to service

Example response:

```
Hardware RTS : Domain 0 Device CPU - Command
initiated.
Please wait...

Hardware RTS : Domain 0 Device CPU - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the CPU state changes to “I”, indicating that the CPUs are reintegrating. The reintegration process takes about 2 minutes to complete, after which the CPU status changes to in-service (indicated by a dot). The in-service LED on ICM 0 is on (green).

At the front panel of the cabinet

16

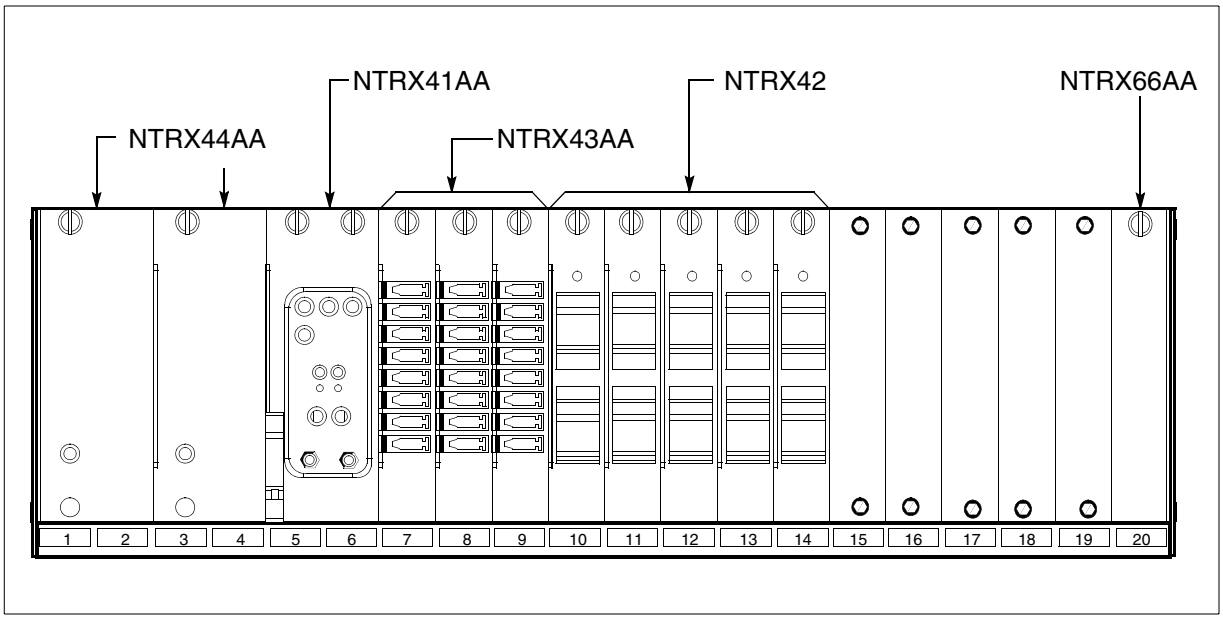
WARNING

Static electricity damage

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist.

17 Open the front cover of the MSP by pulling outward firmly at the finger holes provided and swing the cover down to the open position.



18 Use the breaker designation label to identify which cards are serviced by each circuit breaker (CB). For example, the label CB01-0/18-01 identifies circuit breaker 01 as controlling circuit card position 01 on shelf location 18 in bay 0. Many RX42 modules service two separate devices or units; both units must be powered down prior to removal of the associated RX42 circuit card.

19

A connector removal tool is available to facilitate removal of the AMP Faston receptacles from the power input and output connectors of the MSP modules. This tool comes in two lengths: P0746192 152 mm (6 in.) and P0747552 254 mm (10 in.). The shorter tool is used when access to the rear of the MSP is very limited.

This tool is approximately 2 mm (.090 in.) thick and 17 mm (.65 in.) wide, with a jaw-like cut-out at each end. The cut-out profile conforms to the shape of the Faston receptacle. The shorter tip of each profile is used to position the receptacle in the tool.

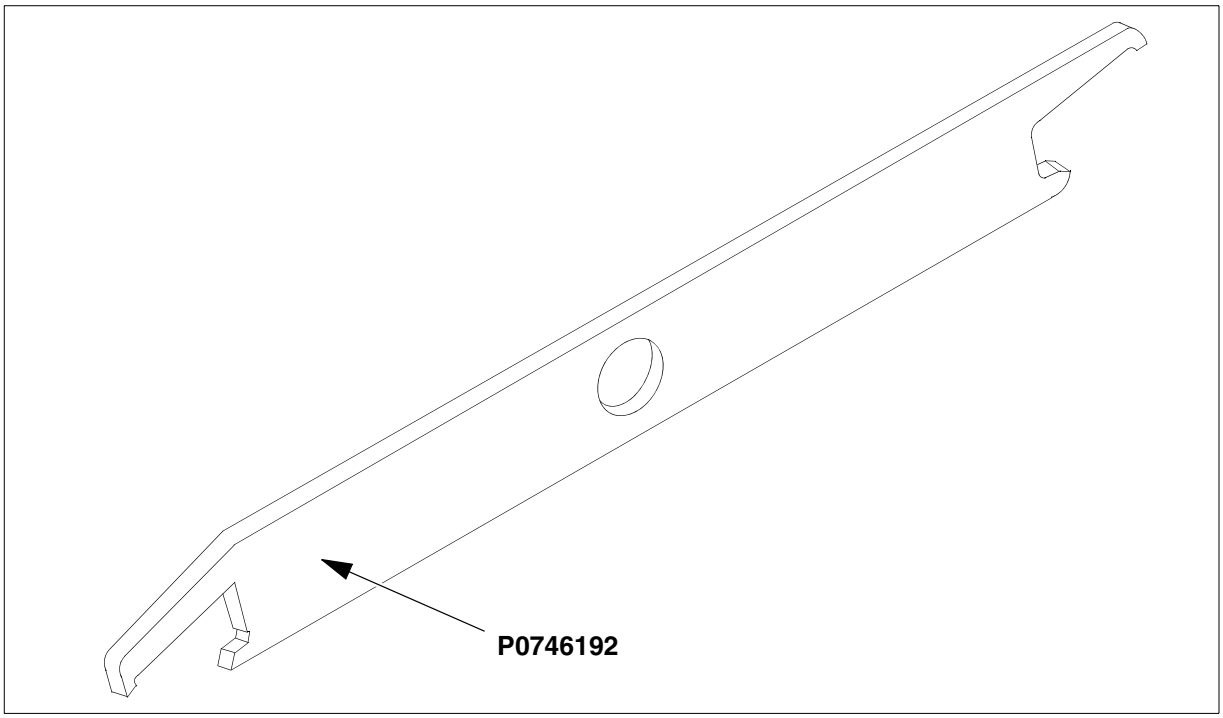
The first meeting point of the tool serves as the pivot point. By rotating the tool around this pivot point, the longer tip of the profile which has a hook on its end is engaged with the action-arm of the power connector. As the action-arm of the connector is depressed, the receptacle is disengaged from the connector tab. The receptacle is removed by pulling the tool with the receptacle trapped in its jaw, away from the connector. The

tool is disengaged from the receptacle by rotating the tool's hook off the action-arm of the receptacle.

Although the shape of the cut-out is the same on each end of the tool, the orientation of the profile is off by 15 degrees. This difference allows for the use of the tool at different angles, which may be required due to limited access to the connectors.

The following is an illustration of the connector removal tool.

Connector removal tool



20

DANGER
Risk of injury from high energy levels, static electricity damage
Wear a wrist strap connected to a wrist strap grounding point. This protects the equipment against damage caused by static electricity.

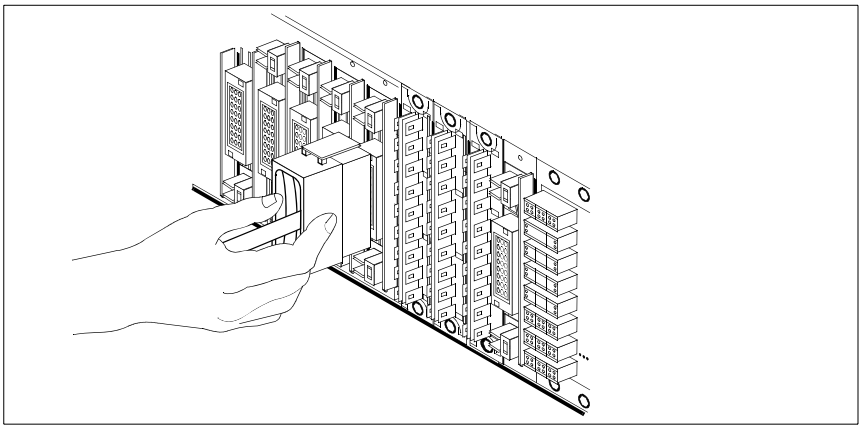
DANGER
Risk of injury from high energy levels, equipment damage
When removing or inserting a card, do not apply direct pressure to the components and do not force the cards into the slots.

DANGER
Risk of injury from high energy levels, voltage present
Do not insert metallic objects into the black connectors. Voltage is present and equipment damage could result.

Put on a wrist strap.

21 Swing the frame out and locate the NTRX42 circuit card. Ensure the card location by checking the slot number stamped into the chassis.

a Note wire color and location to facilitate reconnection.



b Safety tag the front of the circuit breaker to indicate maintenance activity.

c Using the connector removal tool, manually disconnect the power connectors to the circuit card. Working from the bottom of the MSP shelf to the top of the MSP shelf, manually disconnect and tag the smaller black power connectors located below the larger blue power connector. Manually disconnect and tag the large blue power connector. Disconnect and tag the smaller black power connectors located above the large blue power connector. Ensure you disconnect the black connectors before removing the circuit card.

d Although the connectors have voltage present on them, they are insulated. Secure the connectors to the power-connector bundle with a line-tie until it is time to reconnect them.

22 Disconnect and tag any jumper connectors and cables which may be present and set them aside for use on the replacement unit.

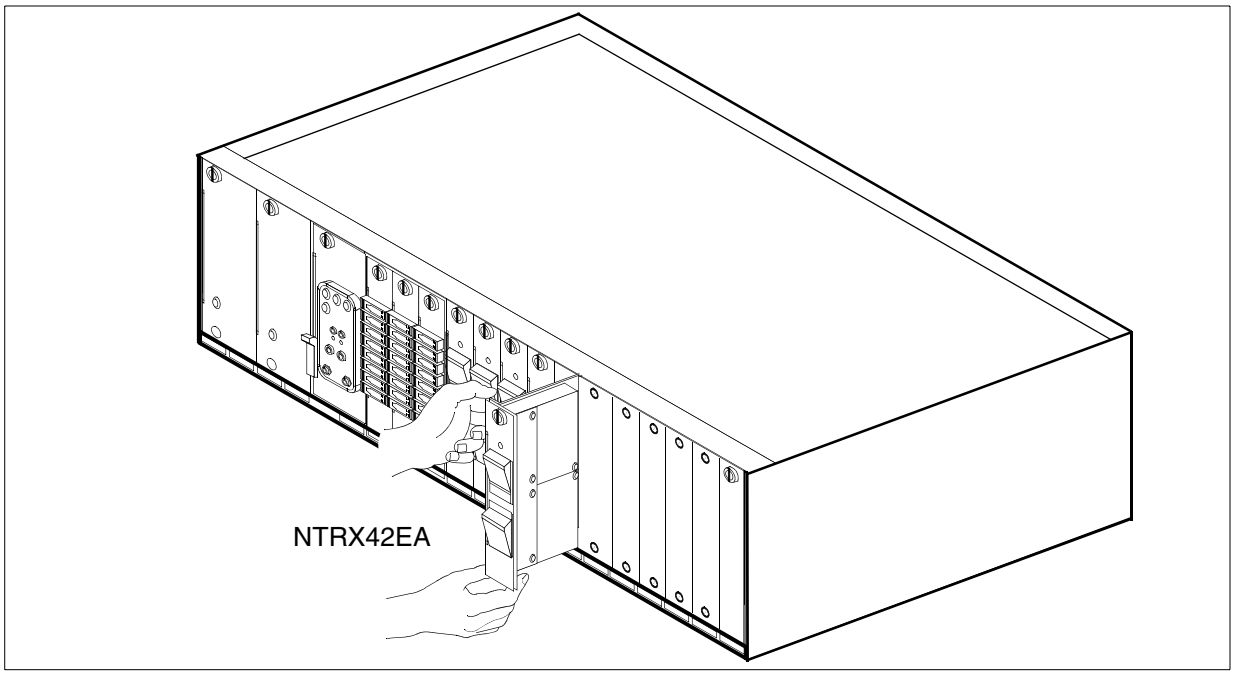
23

DANGER
Risk of injury from high energy levels, equipment damage
When removing or inserting a card, do not apply direct pressure to the components and do not force the cards into the slots.

Remove the faulty circuit card.

a Disengage the spring-loaded captive screw at the top of the circuit card.

b Grasping the top and bottom of unit, gently pull the circuit card towards you until it clears the shelf.



24 Ensure the replacement circuit card has the same PEC, including suffix, as the circuit card just removed.

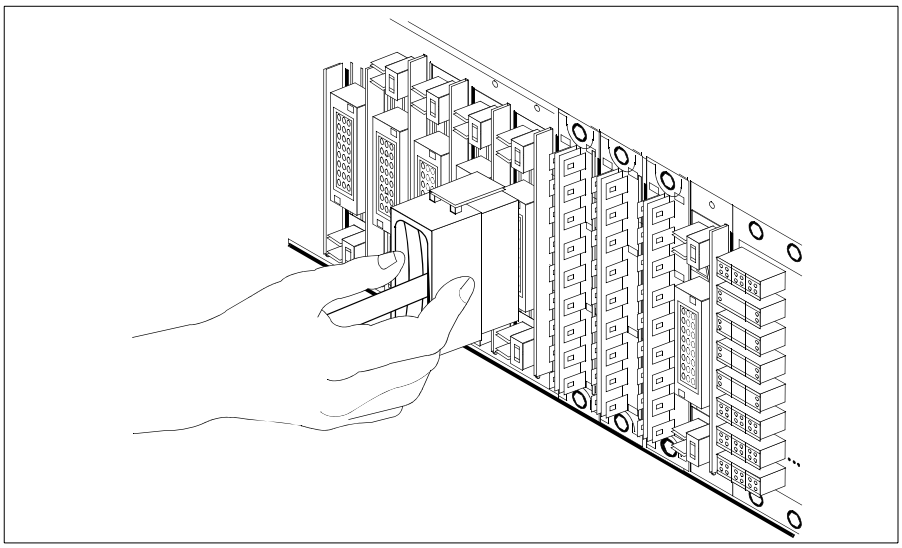
a Align the circuit card with the slots in the shelf and gently slide the circuit card into the shelf.

b Gently but firmly seat the circuit card.

c Tighten the captive screw at the top of the circuit card.

25 Locate the replaced circuit card and reattach the power connectors.

26 Replace any jumper connectors and cables removed in step 22. Reinsert the power connectors at the rear of the circuit card.



27 Apply appropriate label from spare parts on replacement NTRX42 circuit card.

28 Switch on associated power converter.

29 Reset the circuit breakers to ON (upward). If any card controlled by this breaker includes a reset switch, hold the RESET button downward while setting the circuit breaker to the ON position.

At the local or remote VT100 console

30 From the sdmmtc hw level return the ICM to service:

```
rts <domain_no> icm
```

where

<domain_no>
is the domain number of the ICM (0 or 1)

Note: This syntax is valid for single chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

Example response:

```
Hardware RTS : Domain 0 Device ICM - Command
initiated.
Please wait...

Hardware RTS : Domain 0 Device ICM - Command
complete.
```

31 Wait approximately five minutes for the interconnect modules to reintegrate. Check the LEDs on the ICM that you just finished returning to service.

If	Do
the ICM in-service LED is on (solid green), and the out-of-service LED is off	step 33
the ICM in-service LED is off, and the out-of-service LED is on (solid red or flashing red)	contact your next level of support
both LEDs on the CPU controller module are off	step 32

32 Reseat the ICM that you just finished returning to service, and repeat step 30.

33 You can determine the disk mirroring status for each volume group commissioned on the core manager by accessing the storage menu level of the core manager maintenance interface. Access the storage menu level:

`storage`

Example response:

```
Volume Group  Status              Free(MB)
  rootvg      Integrating (12%)    2252
  datavg      Integrating (5%)     1488
```

Note: The reintegration process takes several minutes to begin and takes approximately 20 minutes per Gigabyte to complete. The actual time required depends on the amount of data in the volume group, and the current processor load.

34 Remove safety tag from front of circuit breaker.

35 Close the front cover of the MSP. Swing the cover up to the closed position and lock the two cover latches.

36 Exit out of the SDMMTC interface.

`quit all`

37 Query the SDM faults and status of all applications by entering the following commands. Verify the results with the previous output from step 4. If the results differ, contact your next level of support.

`querysdm flt`

`querysdm loads`

38 You have completed this procedure.

Replacing CPU controller modules

Application

Use this procedure to replace the CPU controller modules, located at the front of the main chassis (slots 6 and 7, and slots 10 and 11) of a CS 2000 Core Manager.

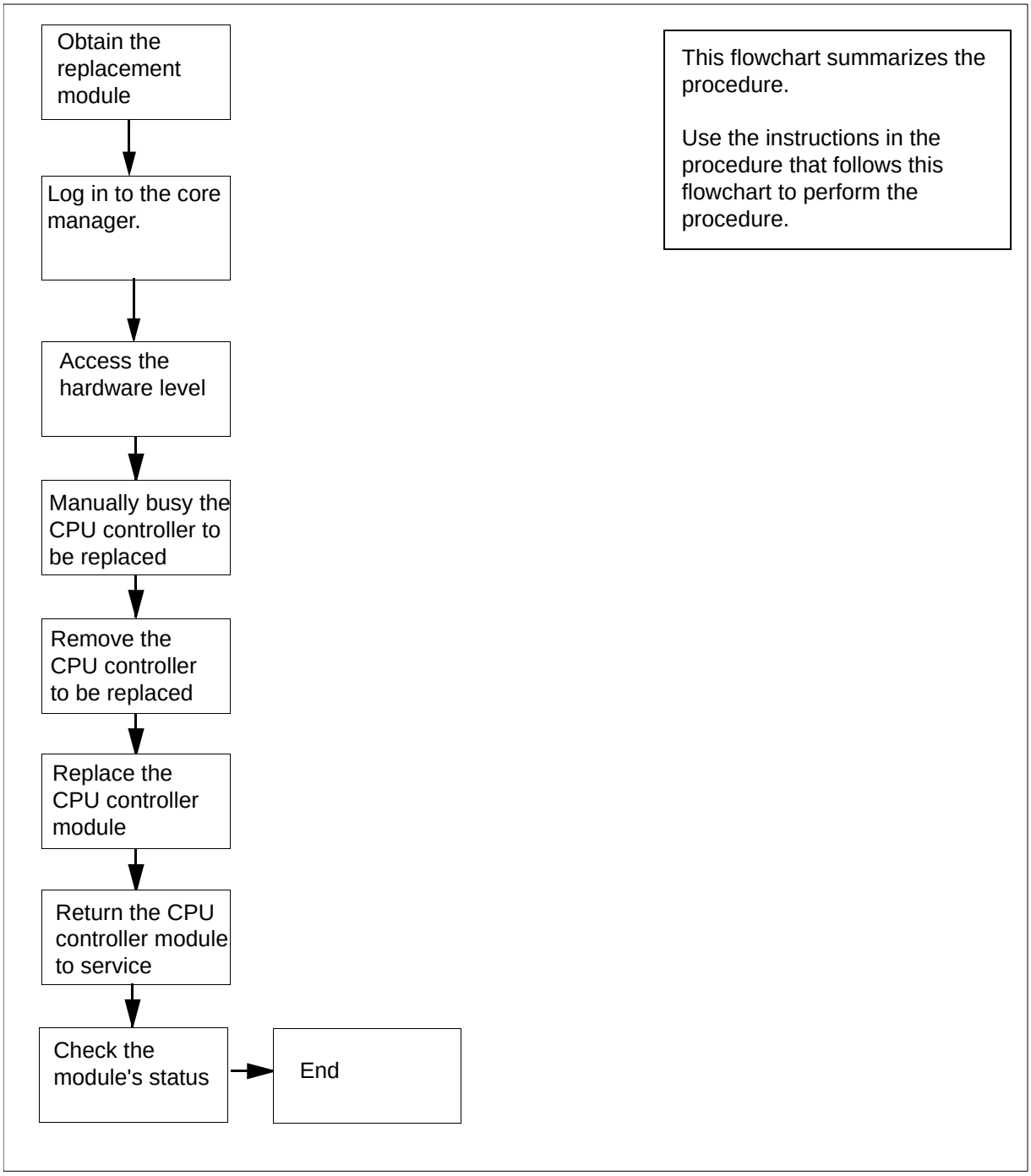
This procedure applies to any of the following CPU controller modules:

Nortel PEC	Name
NTRX50FK	CPU controller module with a PowerPC 604 processor and 128 MByte of DRAM
NTRX50FL	CPU controller module with a PowerPC 604 processor and 256 MByte of DRAM
NTRX50FM	CPU controller module with a PowerPC 604 processor and 512 MByte DRAM
NTRX50CF	CPU controller module with a PowerPC 604e processor and 128 MByte of DRAM
NTRX50CG	CPU controller module with a PowerPC 604e processor and 256 MByte of DRAM
NTRX50CH	CPU controller module with a PowerPC 604e processor and 512 MByte of DRAM
NTRX50NB	CPU controller module with a Arther750 processor and 512 MByte of DRAM

Action

The following flowchart is a summary of the procedure. To replace the CPU controller module, use the instructions in the procedure that follows the flowchart.

Summary of replacing a CPU controller module



Obtain a replacement CPU controller module

1 Obtain a replacement CPU controller module. Ensure that the replacement module has the same product engineering code

(PEC), including suffix, as the unit being removed. The PEC is printed on the module's top locking lever.

At the local or remote VT100 console

2 Log into the core manager as the root or maintenance user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the hardware (Hw) level:

```
> hw
```

5 Busy the CPU controller module you want to replace:

```
> bsy <domain_no> cpu
```

where

<domain_no>
is the domain number (0 or 1) of the CPU controller module that you are replacing

Note 1: The domain is

- 0 if the CPU controller module is in slots 6 and 7, or
- 1 if it is in slots 10 and 11 of the main chassis

Note 2: At the hardware menu level of the maintenance interface, the state of the CPU controller module changes to “M”. Allow approximately 2 minutes for the state to change.

At the front of the core manager

6

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

CAUTION
Potential service interruption
Remove only the CPU controller module that you busied in step 5. The in-service LED on this module is off, and the out-of-service LED is on (red). Do not remove the remaining, in-service module. The in-service LED on the in-service module is on (green), and the out-of-service LED is off. If you remove this module, the core manager shuts down and an automatic reboot occurs.

When a CPU controller module is pulled from the core manager, automatic message accounting (AMA) can go into backup, depending on the conditions:

- when an active CPU controller module is pulled, AMA goes into backup immediately at the CM level.

  When the CPU controller module is reinserted and manually returned to service, the module starts integrating. AMA does not go into backup.
- when an inactive CPU controller module is pulled from the core manager, AMA does not go into backup immediately.

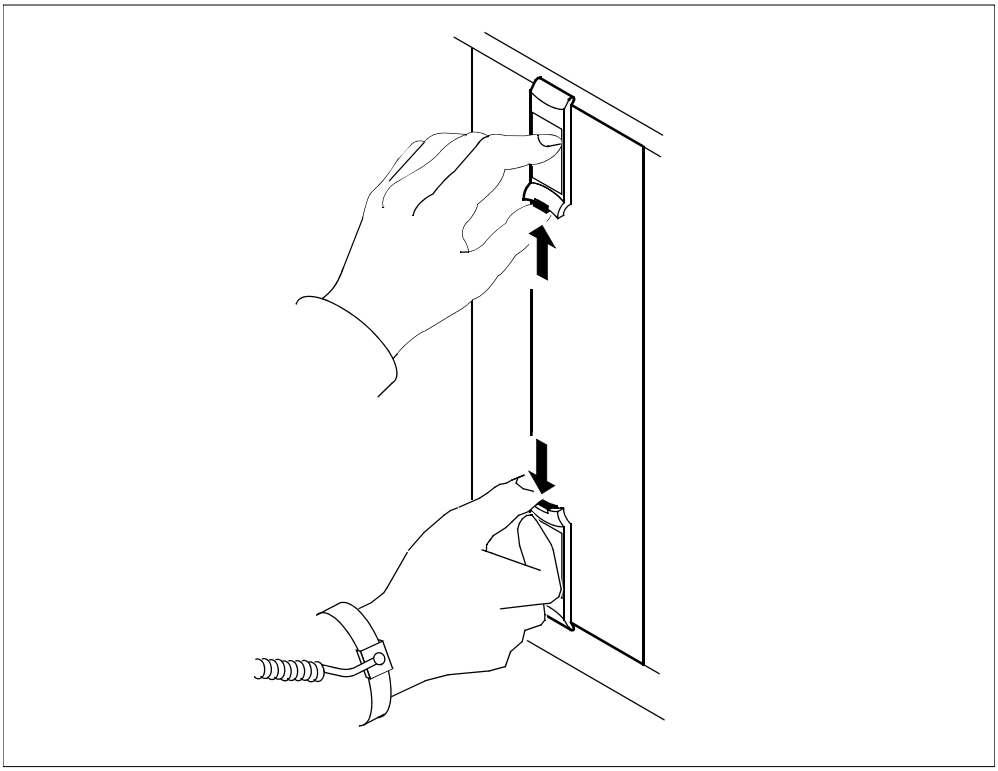
  However, when the module is inserted and starts reintegrating, AMA goes into backup.

Note: This behavior is normal. The reintegration time (approximately 1.5 minutes) is longer than the SuperNode Billing Application (SBA) tolerance to waiting for acknowledgement for storage of billing data.

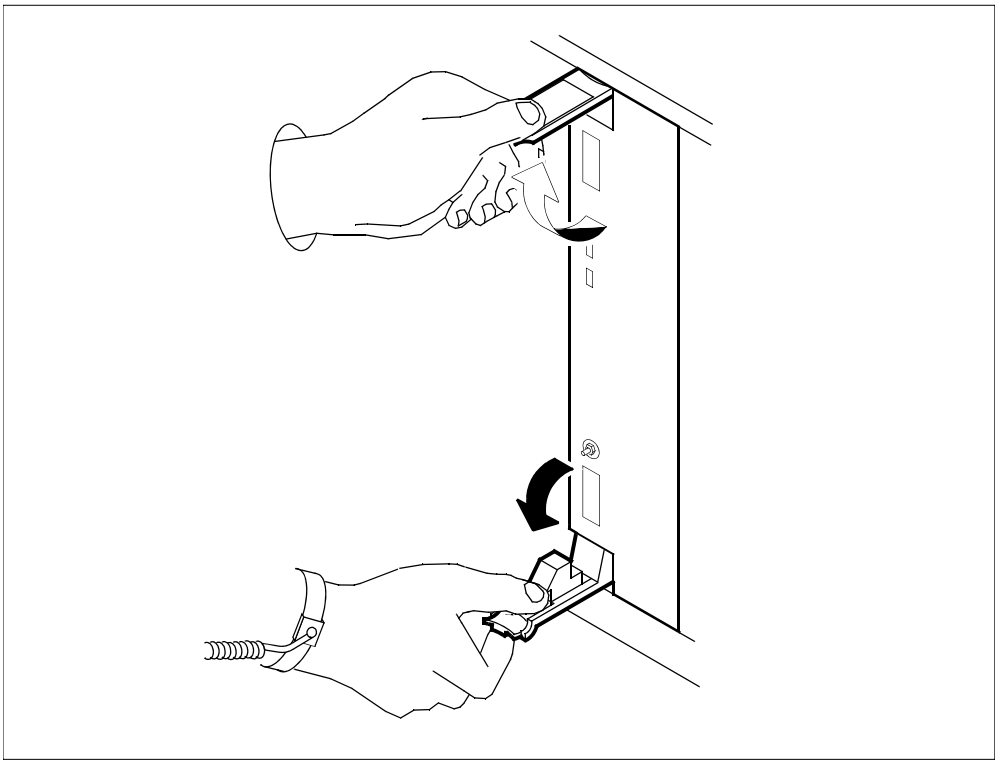
7 Undo the thumbscrews located on the top and the bottom of the CPU controller module.

Note: The thumbscrews are captive and cannot be removed from the module.

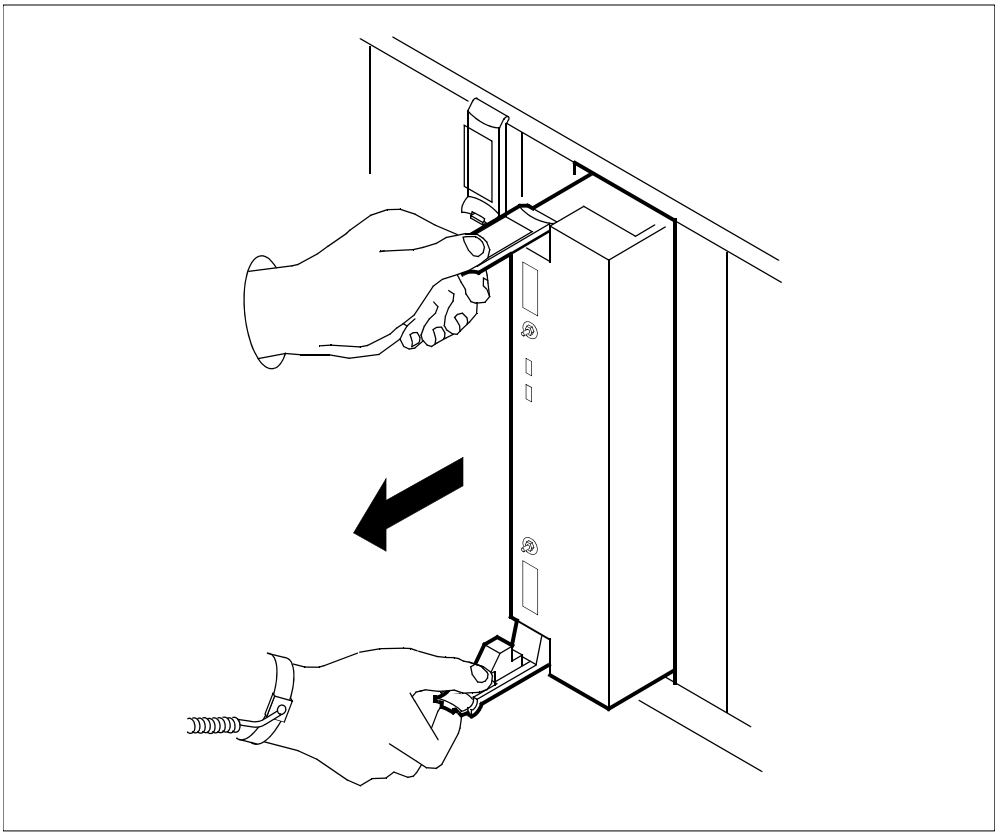
8 Depress the tips of the locking levers on the face of the CPU controller module.



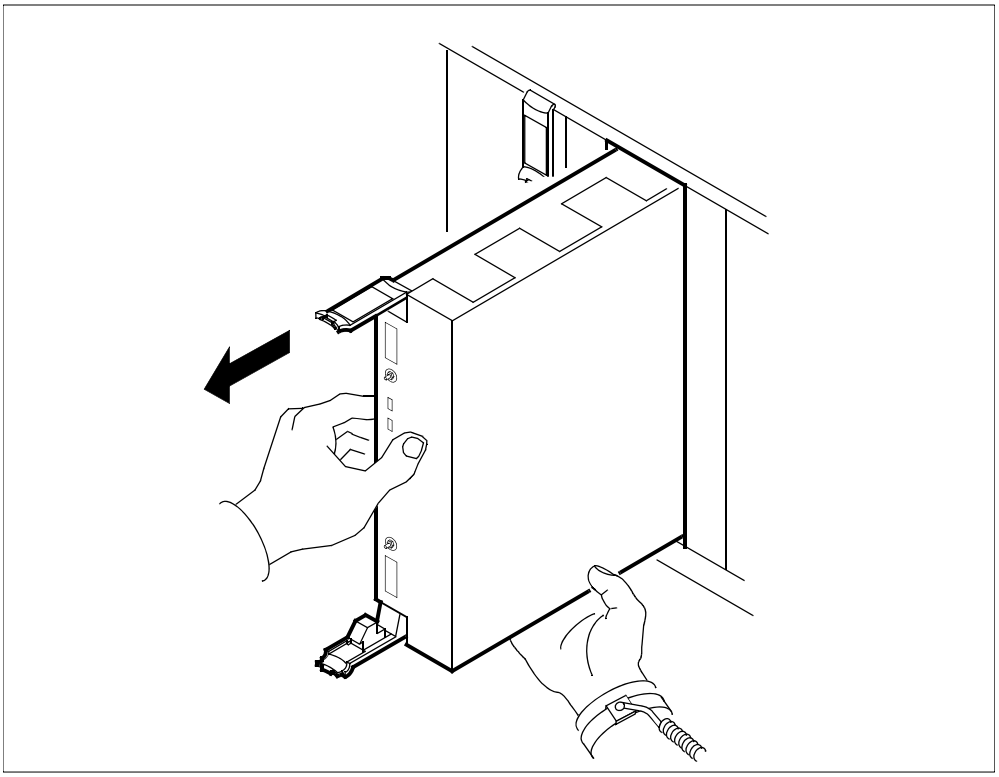
9 Open the locking levers on the face of the module by moving the levers outwards.



10 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 inches (5 cm) from the core manager shelf.



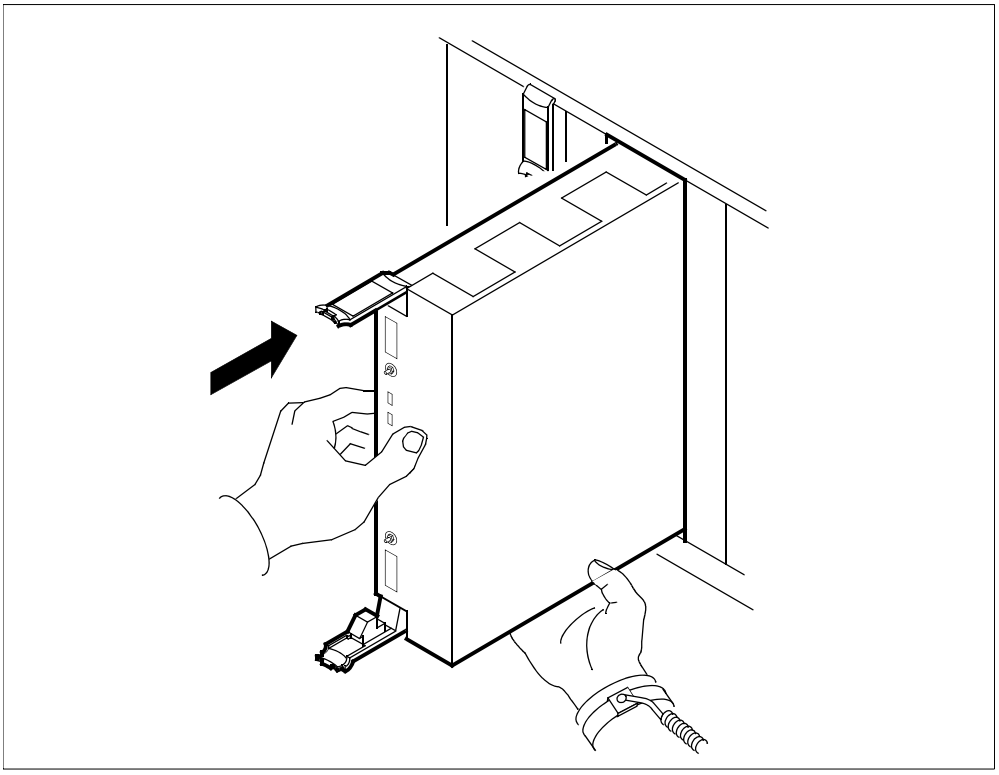
11 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



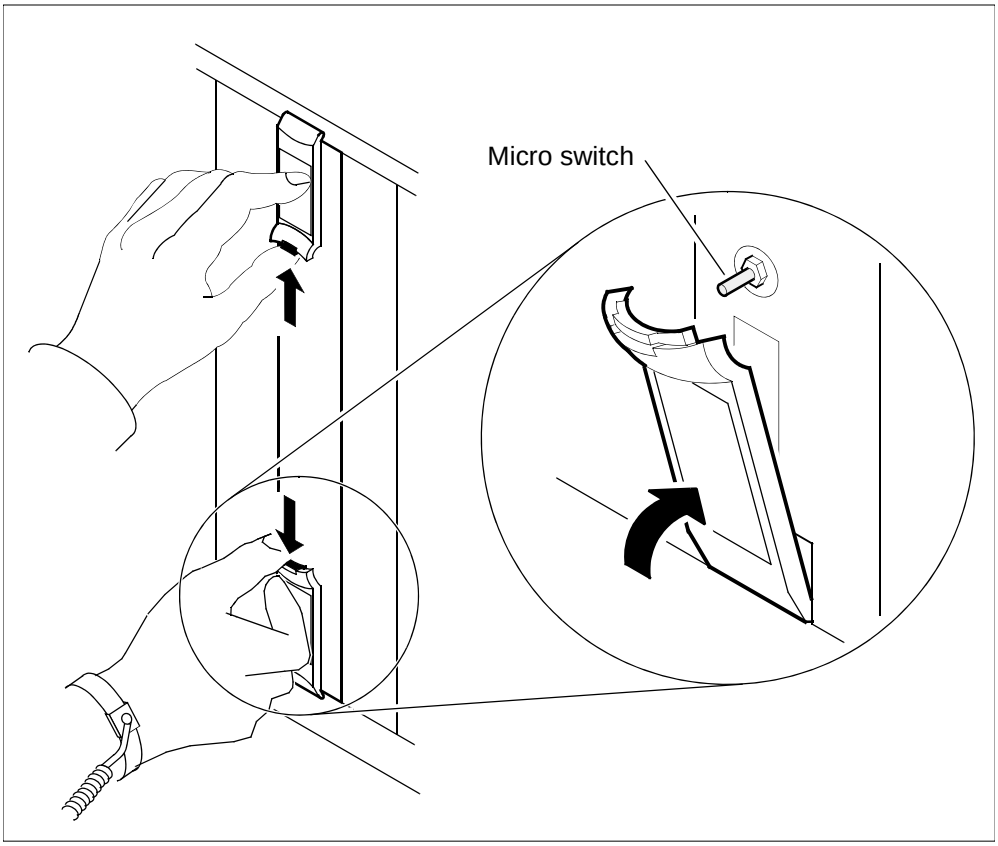
12 Place the module you have removed in an ESD protective container.

13 Insert the replacement module into the core manager shelf.

14 Gently slide the module into the shelf until it is fully inserted.



15 Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



16 Tighten the thumbscrews on the module.

When you insert the replacement CPU controller module, both LEDs on the module turn on and off briefly, indicating that you seated the module correctly, it is receiving power, and has passed its self tests.

At the local or remote VT100 console

17 Return the CPU controller module to service:

```
> rts <domain_no> cpu
```

where

<domain_no>
is the domain number of the CPU controller module that you replaced

Note 1: The domain is

- 0 if the CPU controller module is in slots 6 and 7, or
- 1 if it is in slots 10 and 11 of the main chassis

Note 2: At the hardware menu level of the maintenance interface, the CPU state changes to “I”, indicating that the CPUs are reintegrating. Following the reintegration process, the CPU status changes to in-service, indicated by a dot (.).

The in-service LED on the CPU controller module is on (green). Allow a minimum of 5 minutes for the CPU controller module to complete reintegration and return to service.

18 Determine the status of the controller module.

If the CPU controller module	Do
returns to service	you have completed this procedure
does not return to service	contact your next level of support

Replacing an I/O controller module

Application

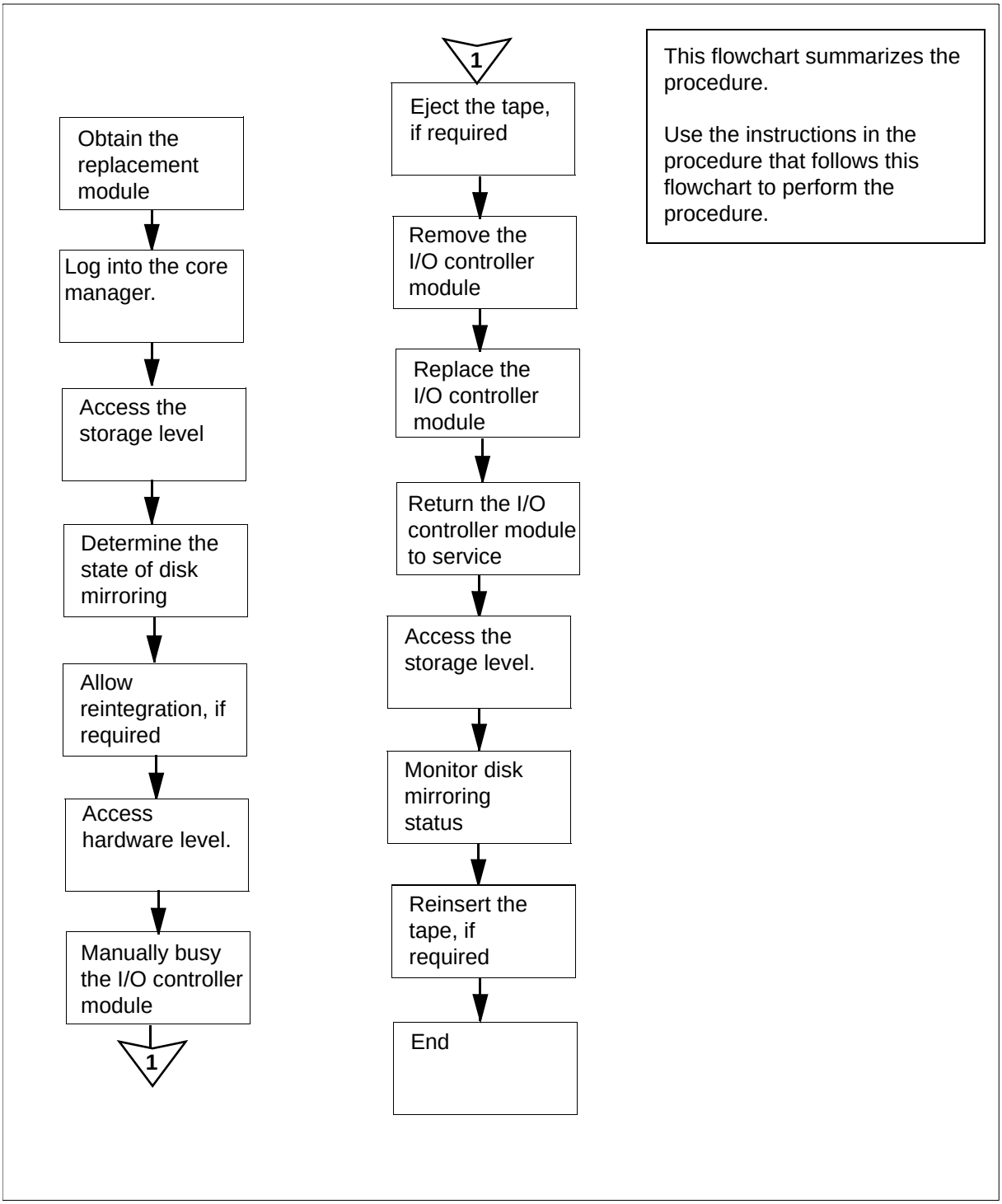
Use this procedure to replace an I/O controller module, located at the front of the main chassis (slots 2 and 3, and 13 and 14) or the I/O expansion chassis of a CS 2000 Core Manager. The slot number in the I/O expansion chassis is not restricted.

Nortel PEC	Name
NTRX50FQ	I/O controller module with 2-Gbyte disk drive and digital audio tape (DAT)
NTRX50FU	I/O controller module with two 2-Gbyte disk drives
NTRX50GN	I/O controller module with 4-Gbyte disk drive and digital audio tape (DAT)
NTRX50GP	I/O controller module with two 4-Gbyte disk drives
NTRX50NM	I/O controller module with 36-Gbyte disk drive and 12-Gbyte digital audio tape (DAT)
NTRX50NL	I/O controller module with two 36-Gbyte disk drives

Action

The following flowchart is a summary of the procedure. To replace the I/O controller module, use the instructions in the procedure that follows the flowchart.

Summary of replacing an I/O controller module



Replacing an I/O controller module

Obtain a replacement I/O controller module

1 Obtain a replacement I/O controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed on the module top locking lever.

At the local or remote VT100 console

2 Log into the core manager as the root or maintenance user.

3 Access the maintenance interface:

```
# sdmmtc
```

4 Access the storage level:

```
> storage
```

5 Determine the state of disk mirroring.

If disk mirroring is in the	Do
Integrating state	step 6
Mirrored or Not Mirrored state	step 7

6

CAUTION
Potential loss of service
Do not continue this procedure while the disks are reintegrating. If you remove an I/O controller module from service during the reintegration process, you will cause a reintegration failure which can require service-affecting manual recovery action.

The hard disks that provide mirrored storage for the system are reintegrating. Allow the reintegration process to complete before continuing this procedure. The reintegration process takes about 20 minute for each Gbyte. The actual time depends on the amount of data in the volume group, and the current processor load.

Note: When the disk drive in an I/O controller module (NTRX50GN is being reintegrated, the controller in-service green LED does not flash. Do not attempt to change state or remove any modules when the LED is flashing.

7 Access the hardware (Hw) level:

```
> hw
```

Note: If there is a tape in the tape drive, eject it now.

8 Busy the I/O controller module that you wish to replace:

```
> bsy <domain> dsk
```

where

<domain>
is the domain number (0 or 1) of the I/O controller module that you are replacing

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slots 2 and 3 or slots 4 and 5, of the main chassis
- 1 if the module is located in slots 13 and 14 or slots 15 and 16, of the main chassis
- 0 if the module is located in any two slots from 1 to 8 in the I/O expansion chassis
- 1 if the module is located in any two slots from 9 to 16 of the I/O expansion chassis

Note: The parameter “DSK” selects the disk on the I/O controller module. All other devices on the I/O controller module are busied automatically. (The example response shown is displayed when you busy the devices on the NTRX50FQ module.)

Example response:

```
Hardware Bsy - Domain 0 Device DSK
Busying DSK (0) will also busy ETH(0), DAT(0)

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

9 Confirm the Bsy command:

```
> y
```

Example response:

```
Hardware Bsy : Domain 0 Device DSK - Command
initiated.
Please wait...
```

When the Bsy command finishes, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware Bsy : Domain 0 Device DSK - Command
complete.
Request will make ent0 not fault tolerant. -
Command complete.
```

Note: At the hardware menu level of the RMI, the state of all devices on the I/O controller module changes to “M”.

At the front of the core manager

10

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

11

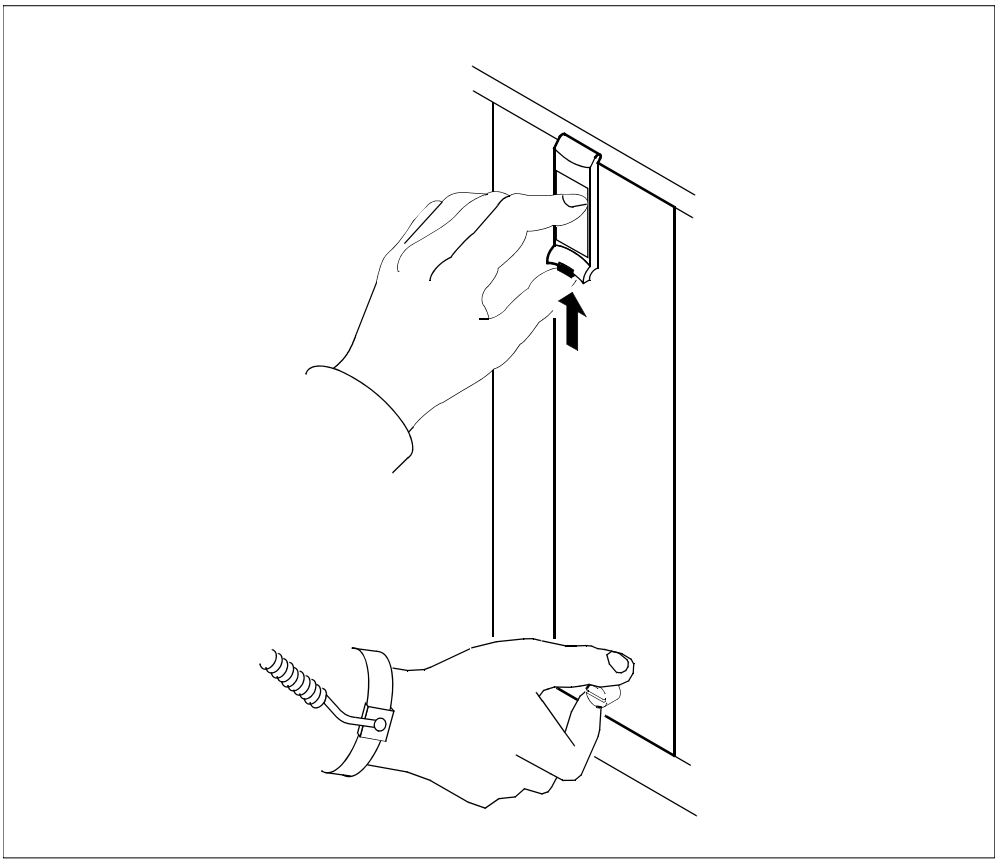
CAUTION
Potential service interruption
Remove only the I/O controller module that you busied in step 8. The in-service LED on this module is off, and the out-of-service LED is on (red).Do not remove the remaining, in-service module. The in-service LED on the in-service module is on (green), and the out-of-service LED is off.

CAUTION
Potential service interruption
I/O controller modules provide mirrored disk storage for the root or data volume groups. If you remove the in-service I/O controller module, you will cause a complete loss of service on the core manager. If you remove the in-service NTRX50FQ module, you will also cause an automatic reboot of the core manager.

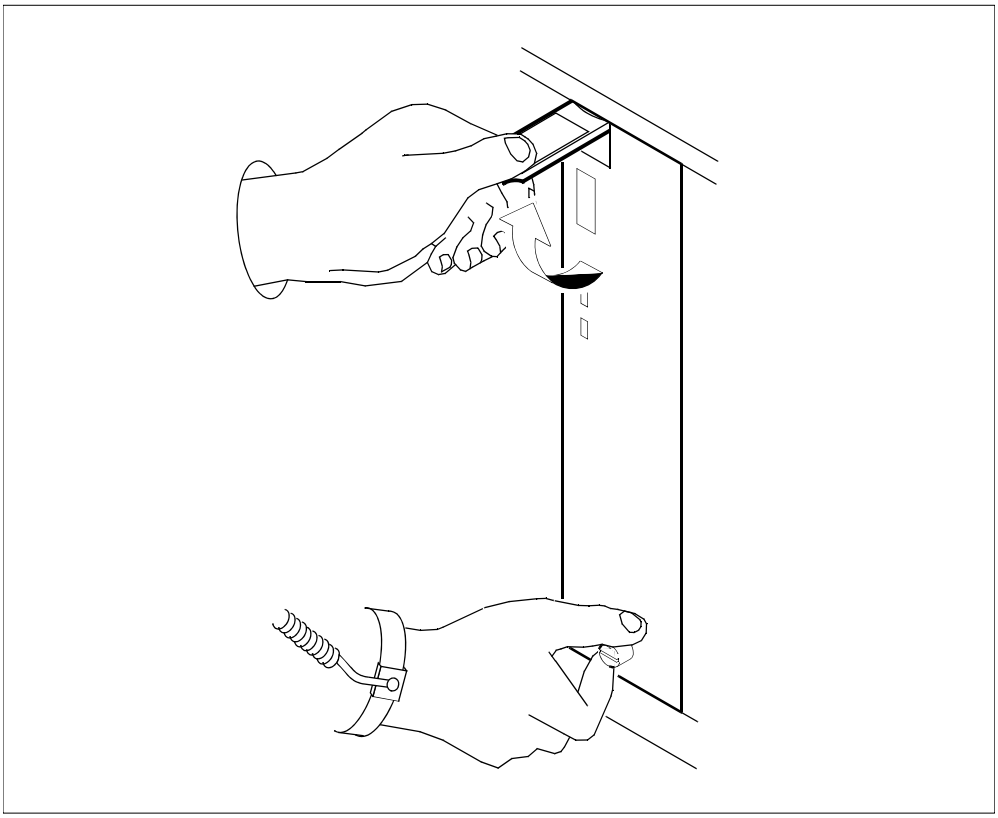
Undo the thumbscrews located on the top and the bottom of the I/O controller module.

Note: The thumbscrews are captive and cannot be removed from the module.

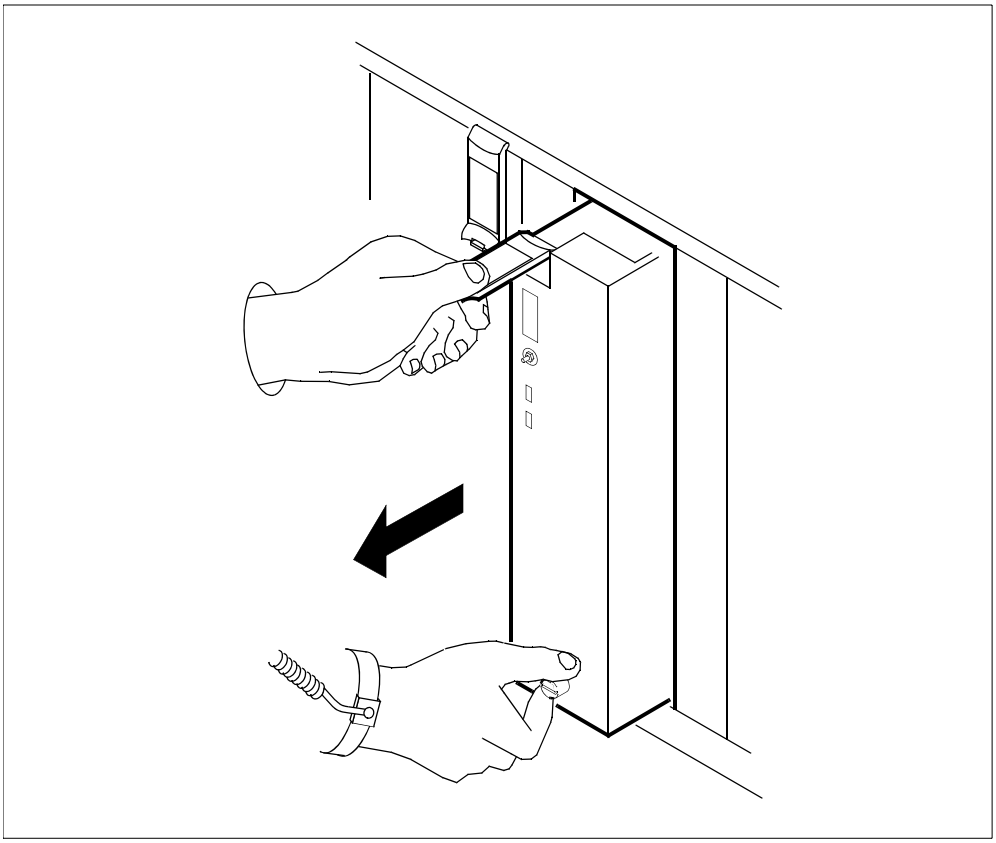
12 Depress the tip of the locking lever on the face of the I/O controller module.



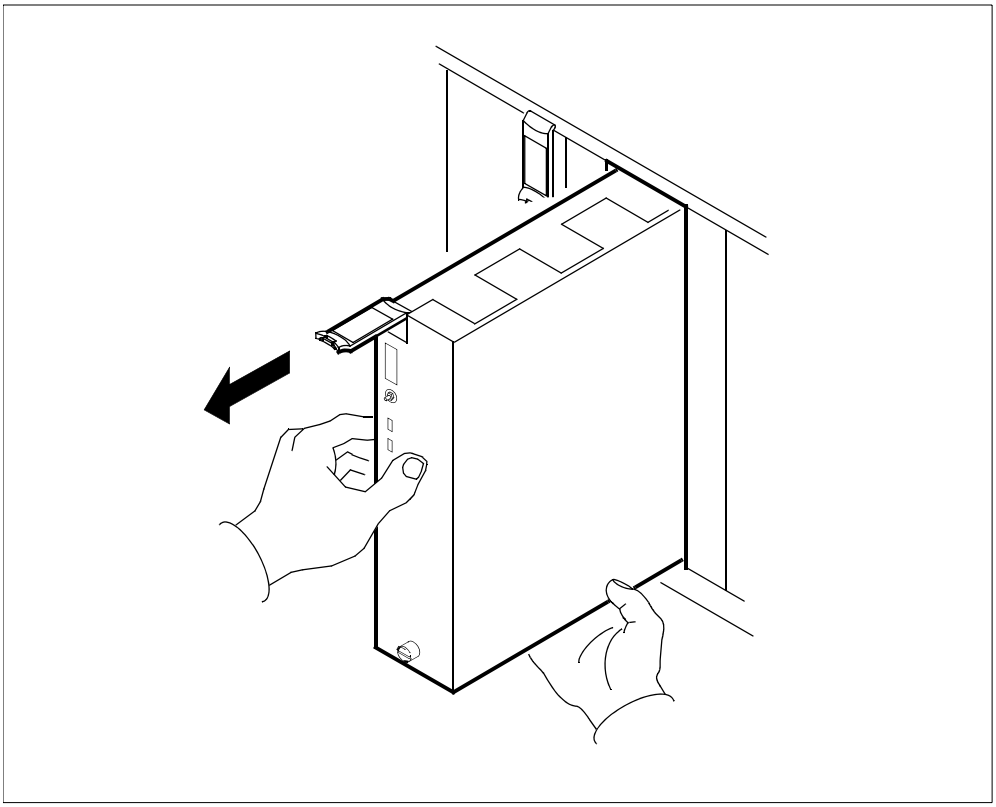
13 Open the locking lever on the face of the module by moving the lever outwards.



14 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 inches (5 cm) from the core manager shelf.



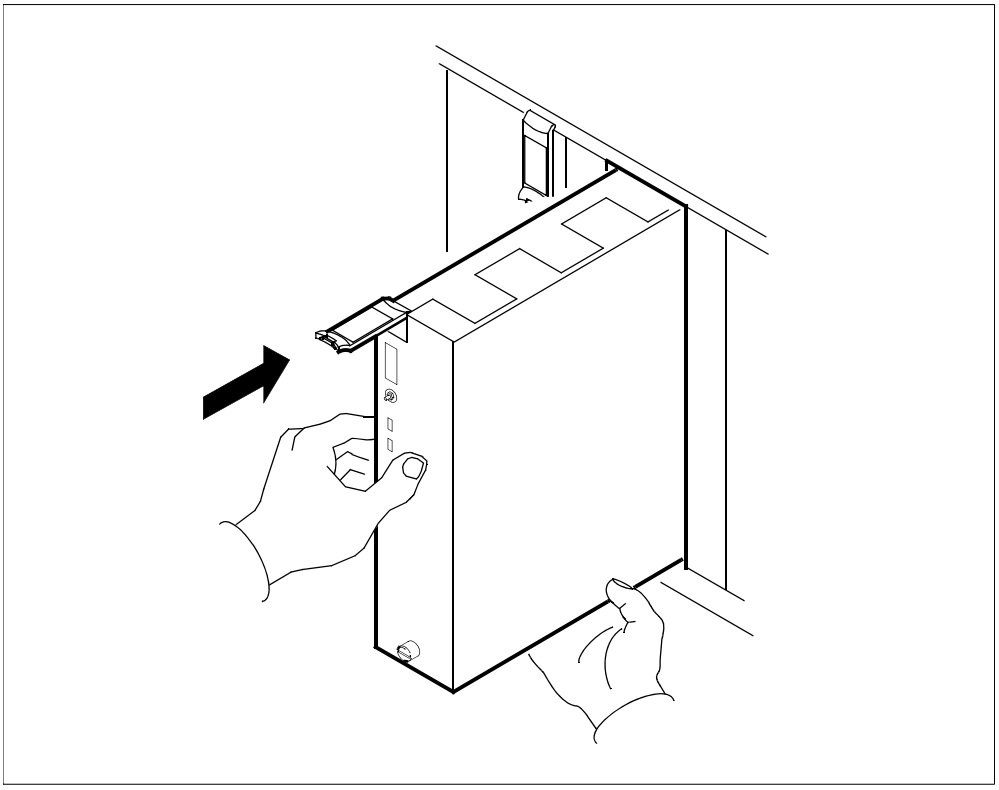
15 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



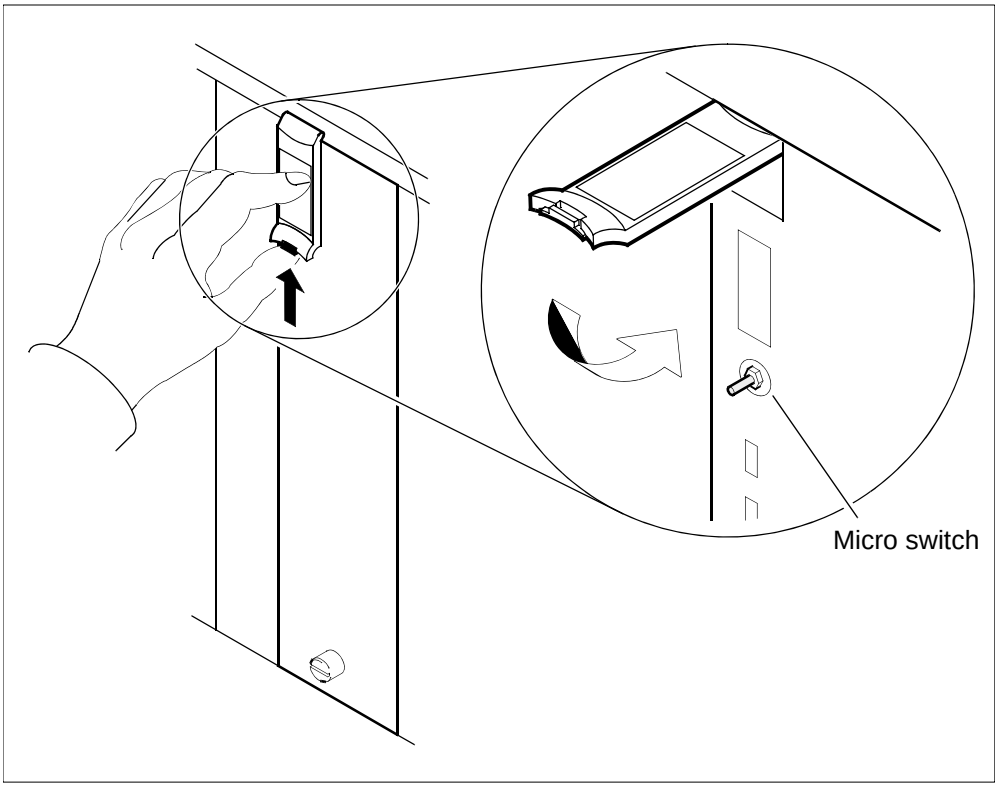
16 Place the module you have removed in an ESD protective container.

17 Insert the replacement module into the core manager shelf.

18 Gently slide the module into the shelf until it is fully inserted.



19 Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.



20 Tighten the thumbscrews on the module.

Note: When you insert the replacement I/O controller module, both its LEDs turn on and off briefly, indicating that the module is seated correctly, is receiving power, and has passed its self tests. The module's in-service LED then turns off, and its out-of-service LED turns on.

21 Return the I/O controller module to service:

```
> rts <domain> dsk
```

where

<domain>
is the domain number of the I/O controller module that you replaced (see step 8)

Example response:

```
Hardware RTS : Domain 0 Device DSK - Command
initiated.
Please wait...
```

When the RTS command finishes, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware RTS : Domain 0 Device DSK - Command
complete.
```

22 Access the storage level

```
> storage
```

23 Monitor the disk mirroring status. The mirroring status appears as Integrating, indicating that the hard disks that provide storage for the system are reintegrating. Allow the reintegration process to complete uninterrupted. This process requires about 20 minutes for each Gbyte. The actual time depends on the amount of data on your system, and the processor load at the time. When disk integration is complete, the disk mirroring status changes to Mirrored.

Note: During disk reintegration, the System-In-Service light on the upper fan tray in the main chassis flashes, and turns solid when disk reintegration is complete.

24 If you removed a DAT tape from the I/O controller module in step 10, reinsert it into the DAT drive.

25 You have completed this procedure.

Replacing the DS512 controller module

Purpose

Use this procedure to remove and replace a DS512 controller module.

Application

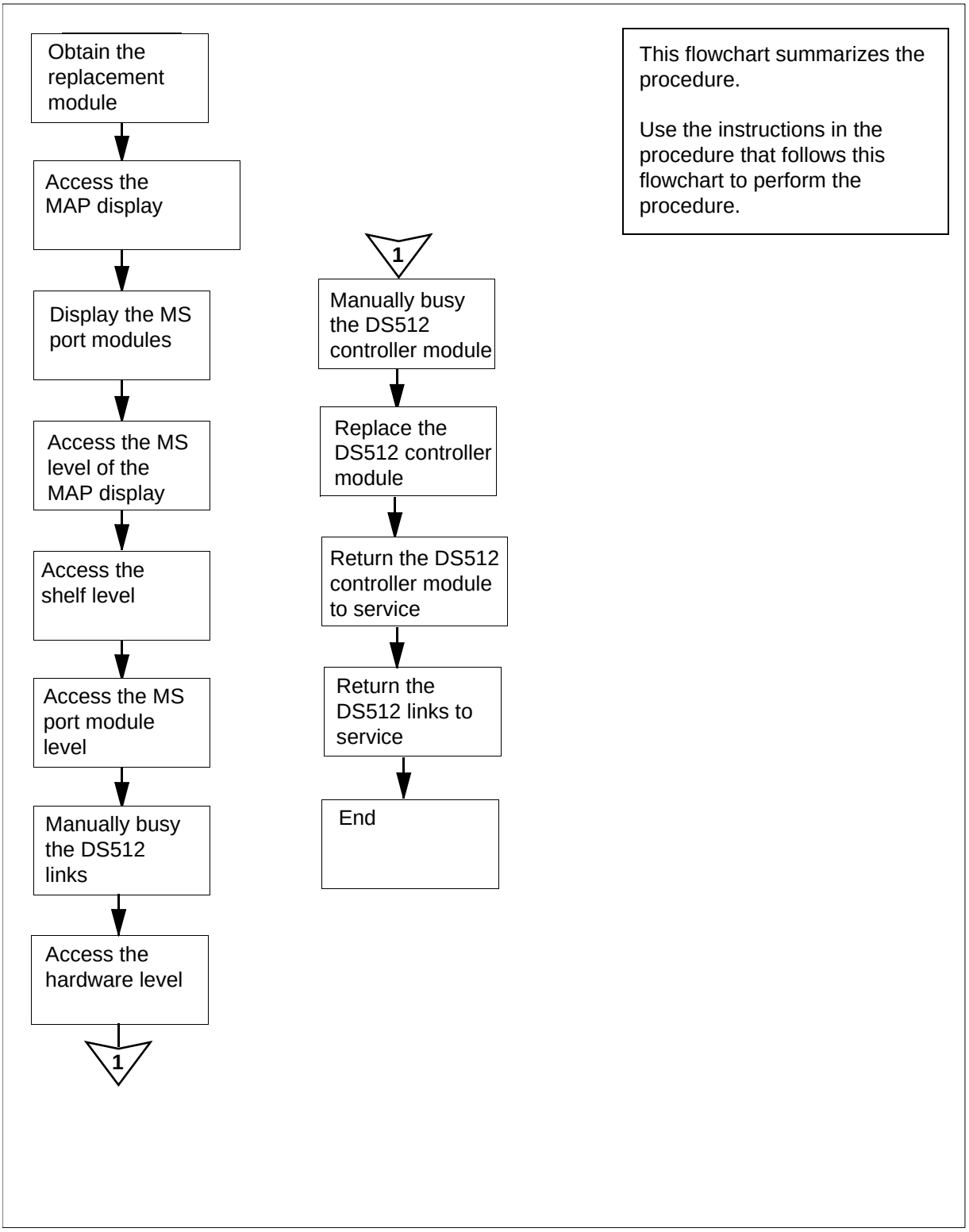
Use this procedure to replace the DS512 controller module, located at the front of the main chassis (slots 1 and 12) of the core manager.

Nortel PEC	Name
NTRX50GA	DS512 controller module
NTRX50GX	DS512 controller module

Action

The following flowchart is a summary of the procedure. To replace the DS512 controller module, use the instructions in the procedure that follows the flowchart.

Summary of replacing a DS512 controller module



Replacing a DS512 controller module

Obtain a replacement DS512 controller module

1 Obtain a replacement DS512 controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed on the top locking lever of the module.

At the MAP display

2 Access the SDM level:

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

3 Display the message (MS) port modules which provide the DS512 links to the core manager:

```
> trnsl
```

Example response:

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

Note: In the example response shown in step 3, the card number is 15.

4 Record the MS card number associated with the core manager DS512 links. The MS card number is the middle number shown in the parentheses.

5 Access the MS level:

```
> ms
```

6 Access the shelf level:

```
> shelf 0
```

7 Access the MS chain level that is associated with the core manager DS512 links:

```
> chain <card_no>
```

where

<cardno>
is the MS card number recorded in step 4

8 Busy the DS512 link between MS plane 0 and the core manager DS512 controller module you want to replace:

```
> bsy 0 link <link_number>
```

where

<link_number>
is the MS link number 0 or 1:

- 0 if the DS512 controller module is in slot 1 of domain 0, or
- 1 if the DS512 controller module is in slot 12 of domain 1

Example response:

```
Request to MAN BUSY MS: 0 shelf: 0 chain:19
link:  0 submitted.
Request to MAN BUSY MS: 0 shelf: 0 chain:19
link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane.

9 Busy the DS512 link between MS plane 1 and the core manager DS512 controller module you want to replace:

```
> bsy 1 link <link_number>
```

where

<link_number>
is the MS link number (0 if the DS512 controller module is in slot 1 of domain 0, or 1 if the DS512 controller module is in slot 12 of domain 1)

Example response:

```
Request to MAN BUSY MS: 1 shelf: 0 chain:19
link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 1 chain:19
link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane 1.

At the local or remote VT100 console

10 Log in to the core manager as the root or maint user.

11 Access the maintenance interface:

```
# sdmmtc
```

12 Access the hardware (Hw) level:

```
> hw
```

13 Busy the DS512 controller module:

> bsy <domain_no> 512

where

<domain_no>
is the domain number (0 or 1) of the DS512 controller module that you are replacing

Use the following list to determine the domain number. The domain number is:

- 0 if the module is located in slot 1 of the main chassis
- 1 if the module is located in slot 12 of the main chassis

Example response:

```
Hardware Bsy - Domain 0 Device 512

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

14 Confirm the Bsy command:

> y

Example response:

```
Hardware Bsy : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the Bsy command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware Bsy : Domain 0 Device 512 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the DS512 controller module changes to “M”.

At the front of the core manager

15

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic discharge grounding wrist strap.

16

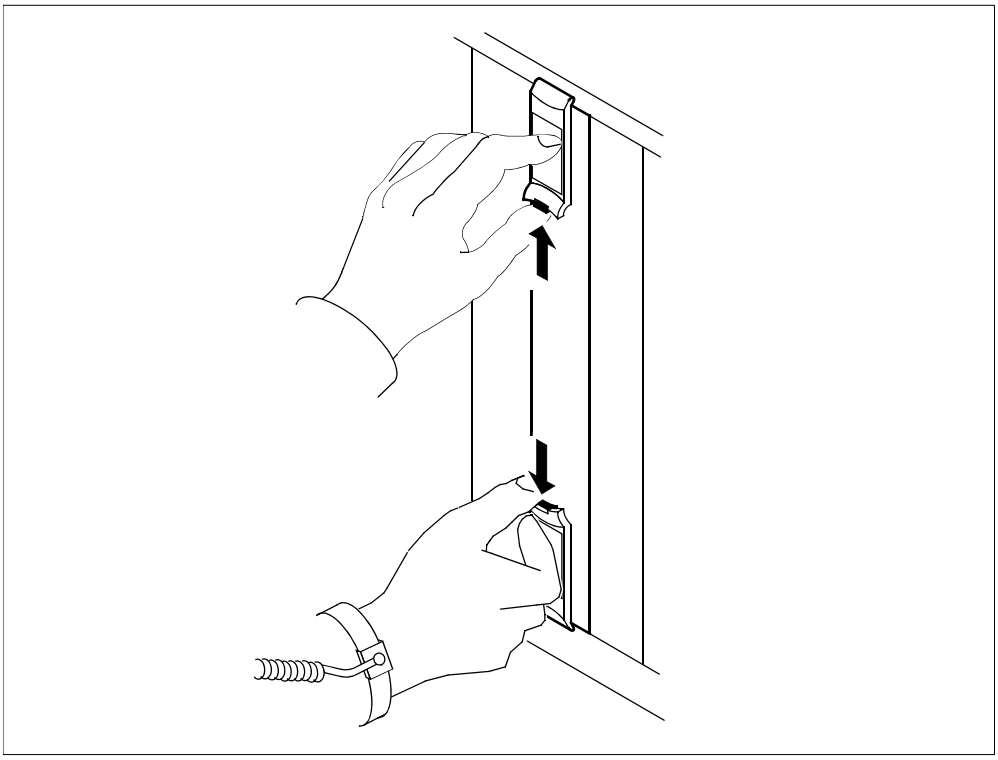
CAUTION
Potential service interruption
Unseat only the DS512 controller module that you busied in step 13, and not the corresponding DS512 controller module in the other I/O domain.

The in-service LED on the module busied in step 13 is off, and the out-of-service LED is on (red). If you remove the remaining in-service DS512 controller module, you will isolate the core manager from the computing module (CM).

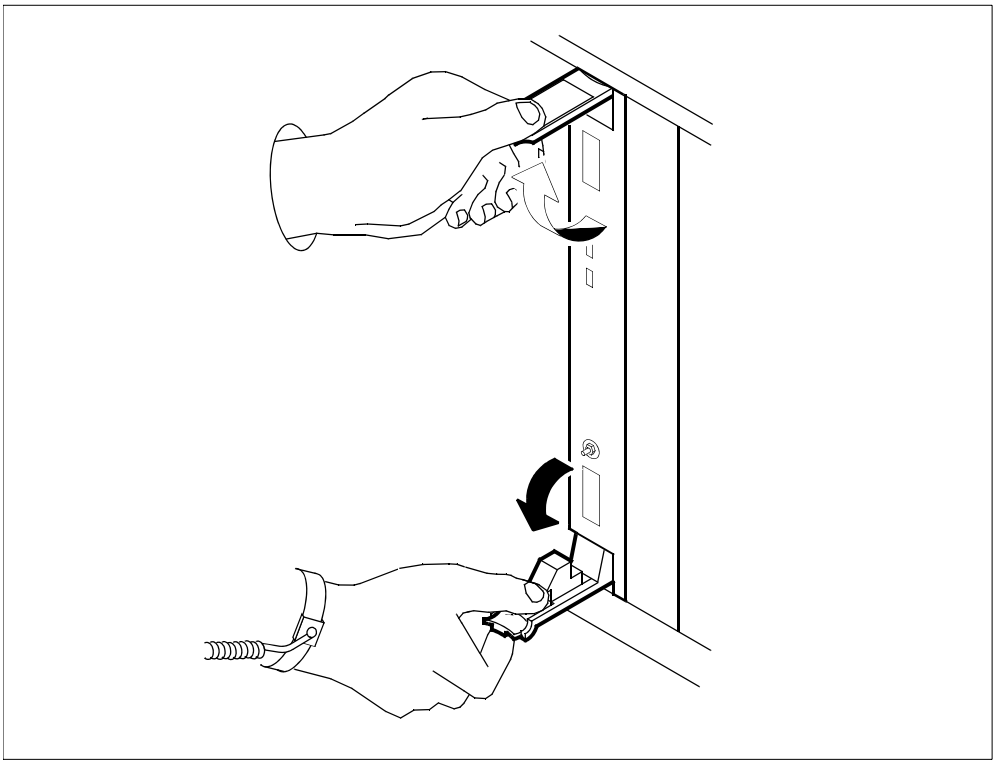
Undo the thumbscrews located on the top and the bottom of the DS512 controller module.

Note: The thumbscrews are captive and cannot be removed from the module.

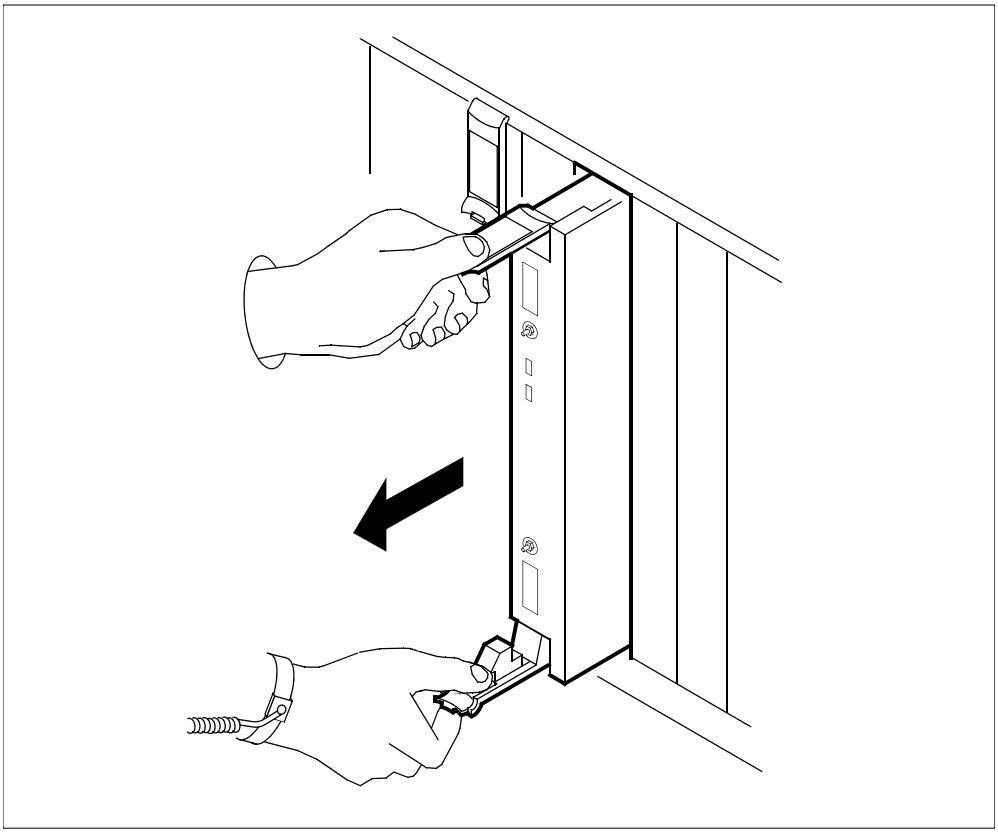
17 Depress the tips of the locking levers on the face of the DS512 controller module.



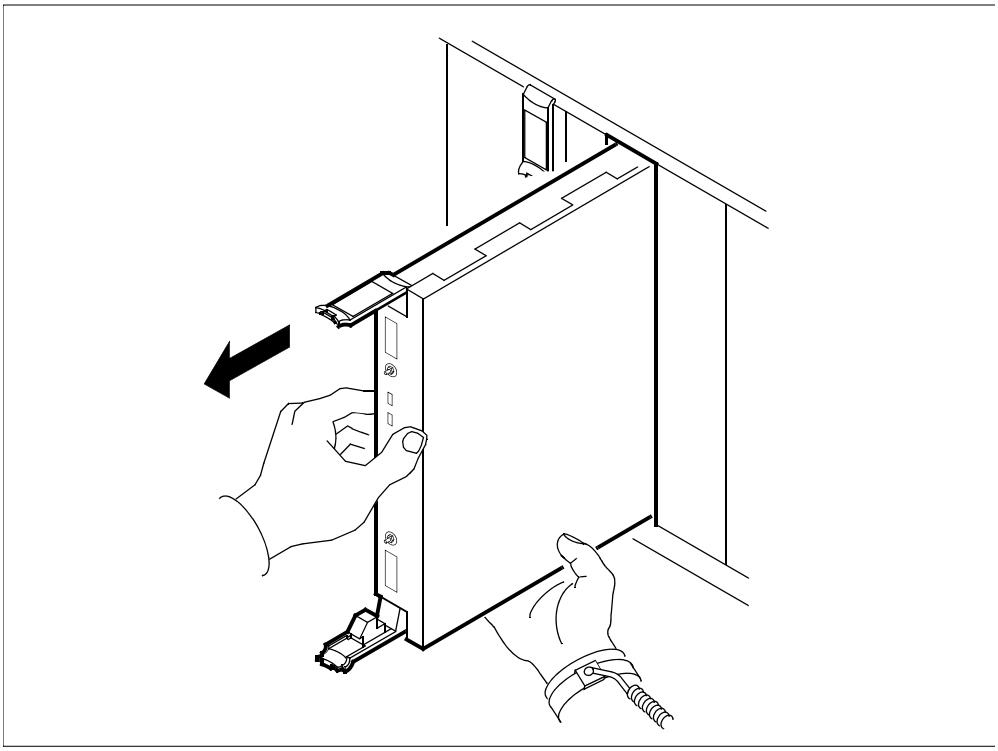
18 Open the locking levers on the face of the module by moving the levers outward.



19 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 inches (5 cm) from the core manager shelf.



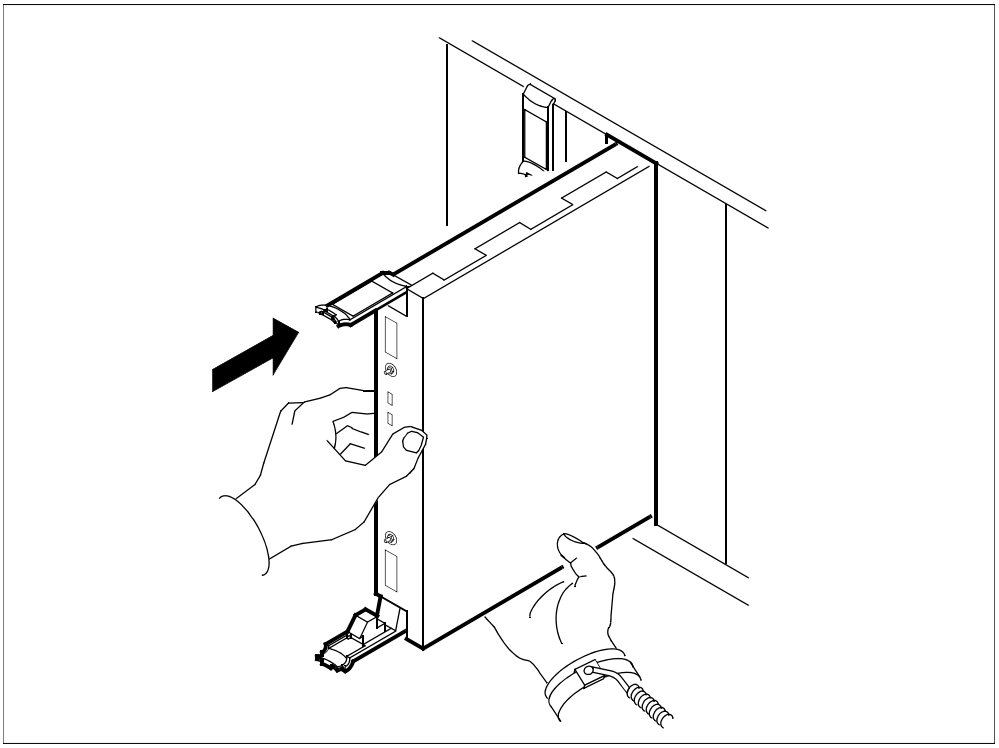
20 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



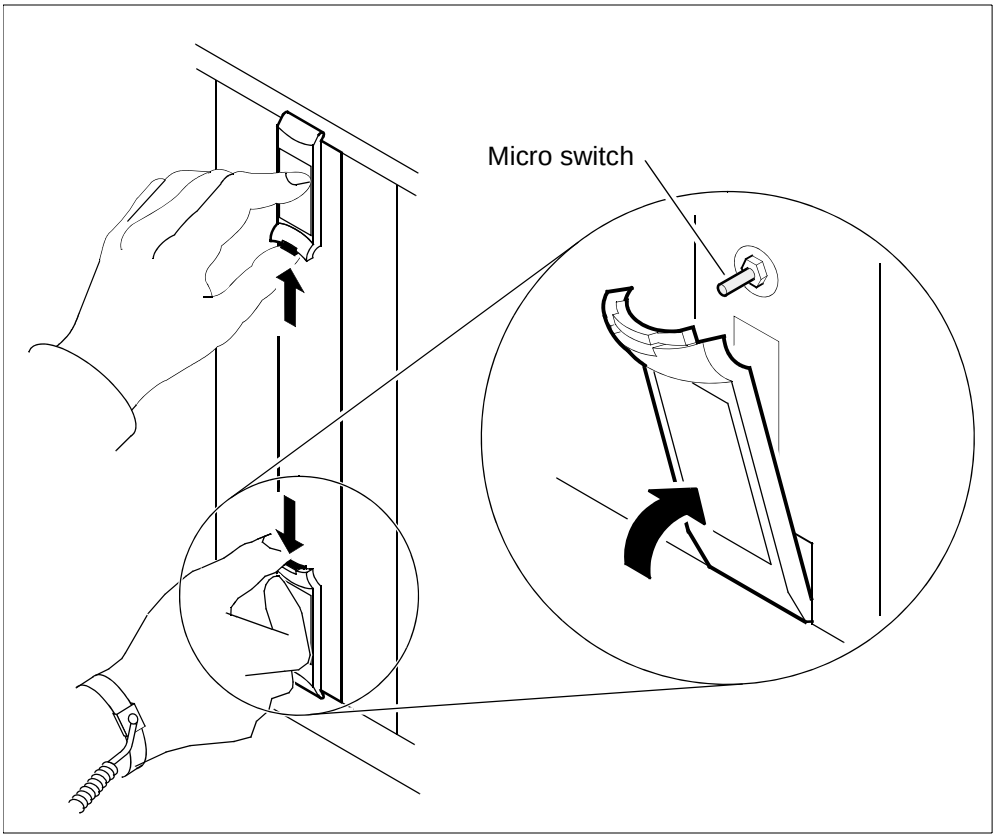
21 Place the module you have removed in an ESD protective container.

22 Insert the replacement module into the core manager shelf.

23 Gently slide the module into the shelf until it is fully inserted.



24 Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



25 Tighten the thumbscrews on the module.

At the local or remote VT100 console

26 Return the DS512 controller module to service:

```
> rts <domain_no> 512
```

where

<domain_no>
is the domain number (0 or 1) of the DS512 controller module you replaced.

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the RTS command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the DS512 controller module changes to a dot (.), indicating the module has returned to service. The in service LED on the DS512 controller module is on (green).

At the MAP display

27 At the MS chain level of the MAP display (accessed in step 7), return to service the DS512 link between MS plane 0 and the DS512 controller module that you replaced:

```
> rts 0 link <link_number>
```

where

<link_number>
is the MS link number:

- 0 if the DS512 controller module is in slot 1 of domain 0, or
- 1 if the DS512 controller module is in slot 12 of domain 1

Example response:

```
Request to RTS MS: 0 shelf: 0 chain:19 link:  0
submitted.
```

```
Request to RTS MS: 0 shelf: 0 chain:19 link: 0
passed.
```

Note: The state for the DS512 link changes to a dot (.) if the core manager DS512 link is in service. Otherwise, the state for DS512 link changes to a “P”.

28 At the MS chain level of the MAP (accessed in step 7), return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
> rts 1 link <link_number>
```

where

<link_number>
is the MS link number:

- 0 if the DS512 controller module is in slot 1 of domain 0, or
- 1 if the DS512 controller module is in slot 12 of domain 1)

Example response:

```
Request to RTS MS: 1 shelf: 0 chain:19 link:  1
submitted.
Request to RTS MS: 1 shelf: 0 chain:19 link: 1
passed.
```

Note: The state for the DS512 link changes to a dot (.) if the core manager DS512 link is in-service. Otherwise, the state for DS512 link changes to a “P”.

29 You have completed this procedure.

Replacing the DS512 personality module

Purpose

Use this procedure to replace a DS512 personality module.

Application

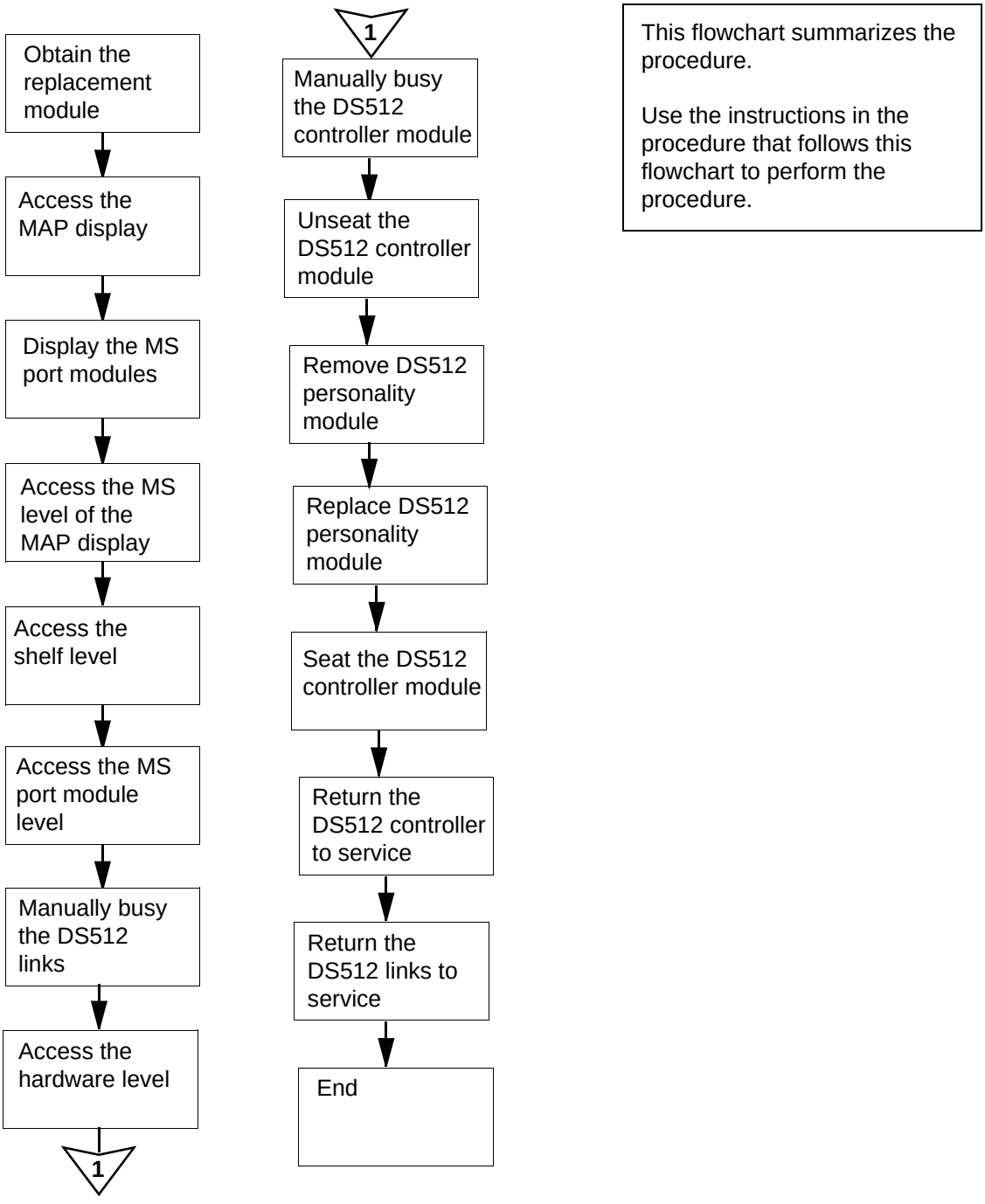
Use this procedure to replace the DS512 personality module, located at the rear of the main chassis (slots 1 and 12) of the core manager.

Nortel PEC	Name
NTRX50GH	DS512 personality module

Action

The following flowchart is a summary of the procedure. To replace the DS512 personality module, use the instructions in the procedure that follows the flowchart.

Summary of replacing a DS512 personality module



Replacing a DS512 personality module

Obtain a replacement DS512 personality module

1 Obtain a replacement DS512 personality module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is printed at the top of the module.

At the MAP display

2 Access the SDM level:

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

and pressing the Enter key.

3 Display the message (MS) port modules which provide the DS512 links to the core manager:

```
> trnsl
```

Example response:

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

4 Record the MS card number associated with the core manager DS512 links.

The MS card number is the middle number shown in the parentheses.

Note: In the example response shown in step 3, the card number is 15.

5 Access the MS level:

```
> ms
```

6 Access the shelf level:

```
> shelf 0
```

7 Access the MS chain level associated with the core manager DS512 links:

```
> chain <card_no>
```

where

<card_no>
is the MS card number recorded in step 4

8 Busy the DS512 link between MS plane 0 and the core manager DS512 personality module you wish to replace:

```
> bsy 0 link <link_number>
```

where

<link_number>
is the MS link number:

- 0 if the DS512 personality module is in slot 1 of domain 0, or
- 1 if the DS512 personality module is in slot 12 of domain 1

Example response:

```
Request to MAN BUSY MS: 0 shelf: 0 chain:19
link:  0 submitted.Request to MAN BUSY MS: 0
shelf: 0 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane.

9 Busy the DS512 link between MS plane 1 and the core manager DS512 personality module you want to replace:

```
> bsy 1 link <link_number>
```

where

<link_number>
is the MS link number:

- 0 if the DS512 personality module is in slot 1 of domain 0, or
- 1 if the DS512 personality module is in slot 12 of domain 1

Example response:

```
Request to MAN BUSY MS: 1 shelf: 0 chain:19
link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 1 chain:19
link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane 1.

At the local or remote VT100 console

10 Log in to the core manager as the root or maint user.

11 Access the maintenance interface:

```
# sdmmtc
```

12 Access the hardware (Hw) level:

```
> hw
```

13 Busy the DS512 controller module:

```
> bsy <domain_no> 512
```

where

<domain_no>
is the domain number (0 or 1) of the DS512 personality module that you are replacing.

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slot 1 of the main chassis
- 1 if the module is located in slot 12 of the main chassis

Example response:

```
Hardware Bsy - Domain 0 Device 512

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

14 Confirm the Bsy command:

```
> y
```

Example response:

```
Hardware Bsy : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the Bsy command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware Bsy : Domain 0 Device 512 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the DS512 controller module changes to “M”. The out-of-service LED on the module is on (red).

At the front of the core manager

15

WARNING
Static electricity damage
Wear an electrostatic (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on an electrostatic grounding wrist strap.

16

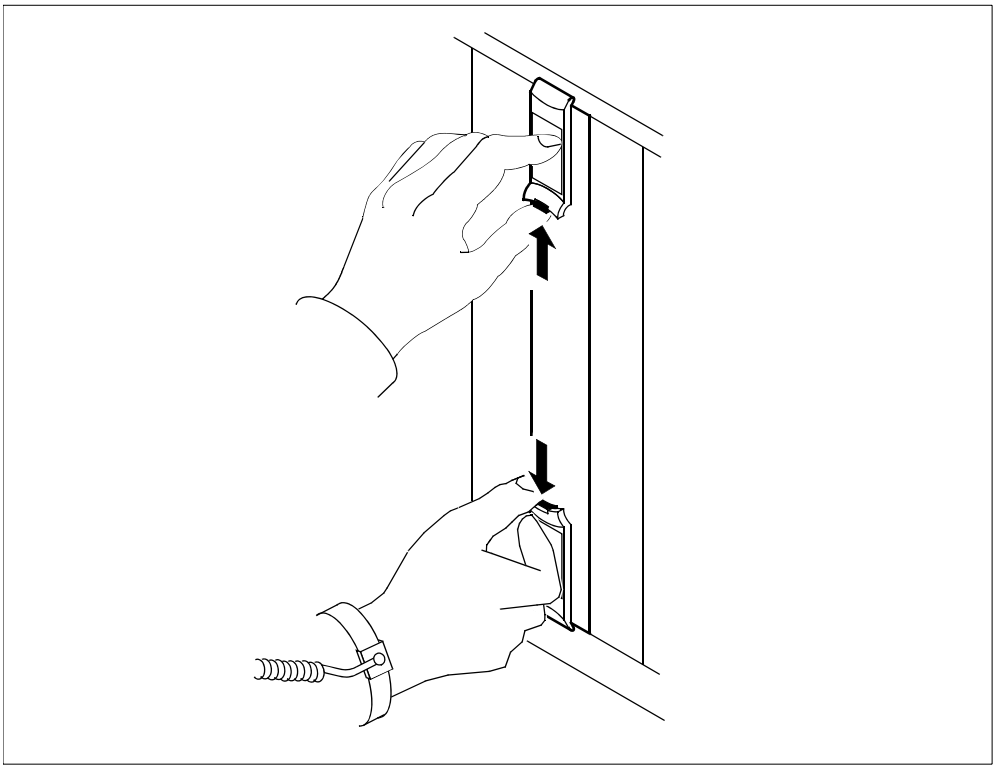
CAUTION
Potential service interruption
Unseat only the DS512 controller module that you busied in step 13, and not the corresponding DS512 controller module in the other domain. The in-service LED on the module busied in step 13 is off, and the out-of-service LED is on (red).

If you remove the remaining in-service dS512 controller module, you will isolate the core manager from the computing module (CM).

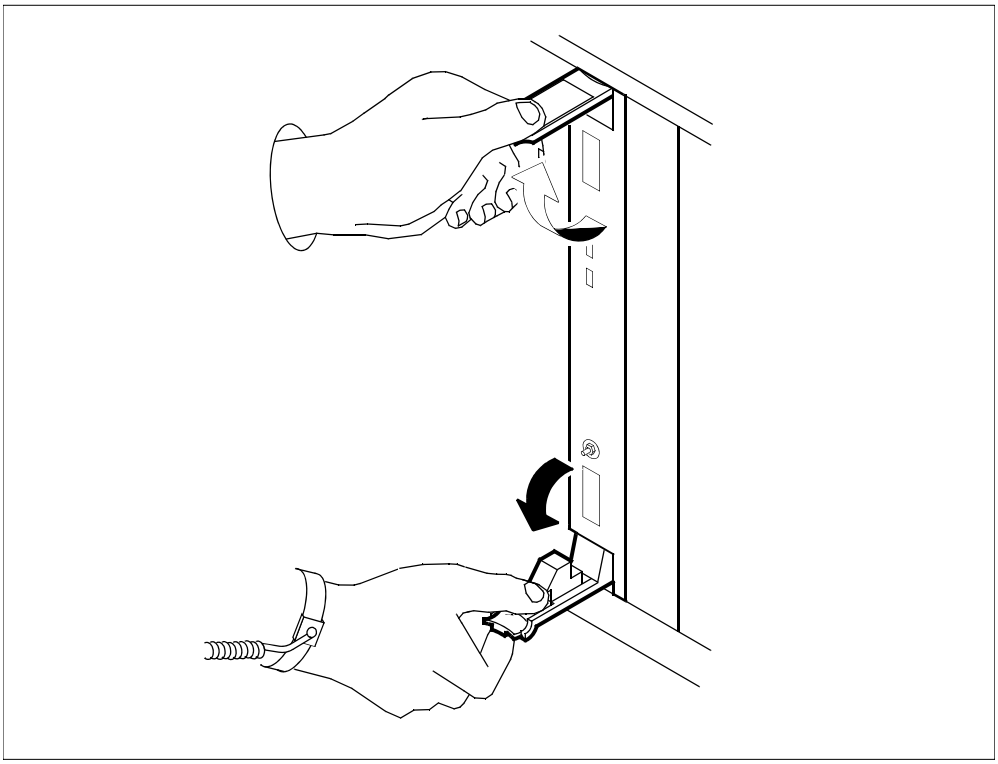
Undo the thumbscrews located on the top and bottom of the DS512 controller module associated with the DS512 personality module you wish to replace.

Note: The thumbscrews are captive and cannot be removed from the module.

17 Depress the tips of the locking levers on the face of the DS512 controller module.



18 Open the locking levers on the face of the DS512 controller module by moving the levers outwards.



At the back of the core manager

19 Loosen the two thumbscrews located at the top and the bottom of the DS512 personality module.

Note: The thumbscrews are captive and cannot be removed from the module.

20

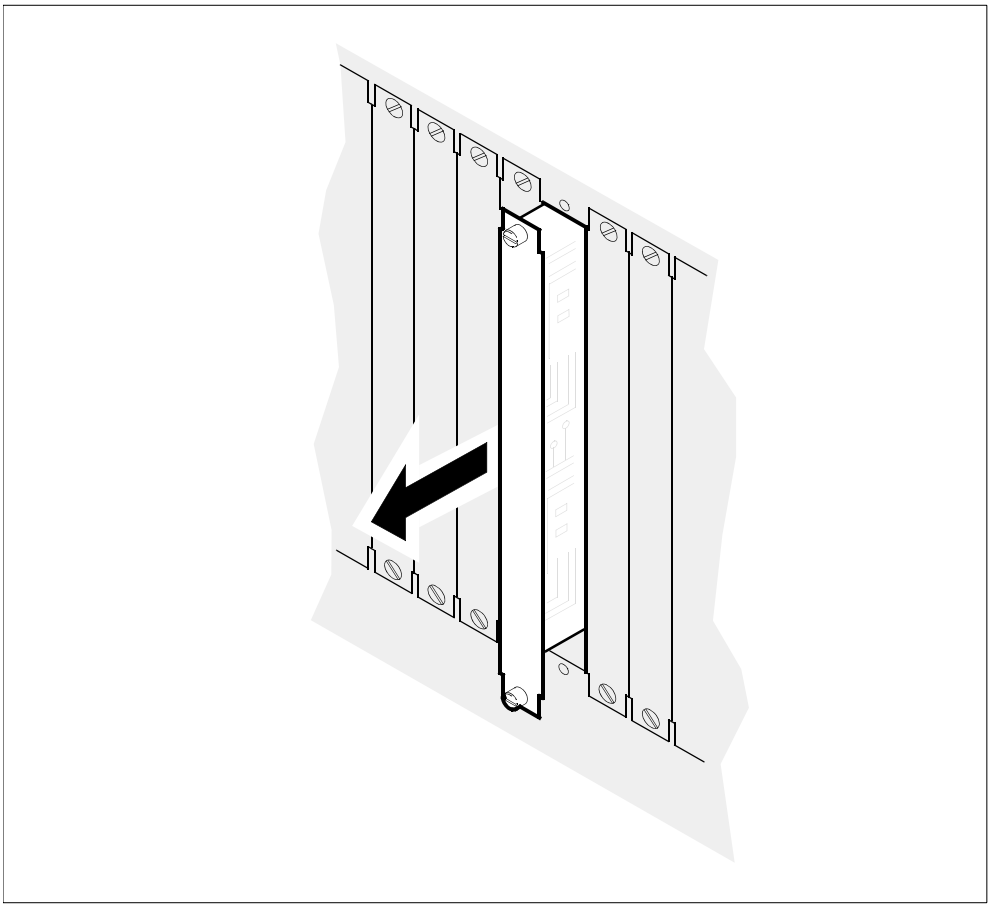
CAUTION

Disconnecting transmit and receive cables

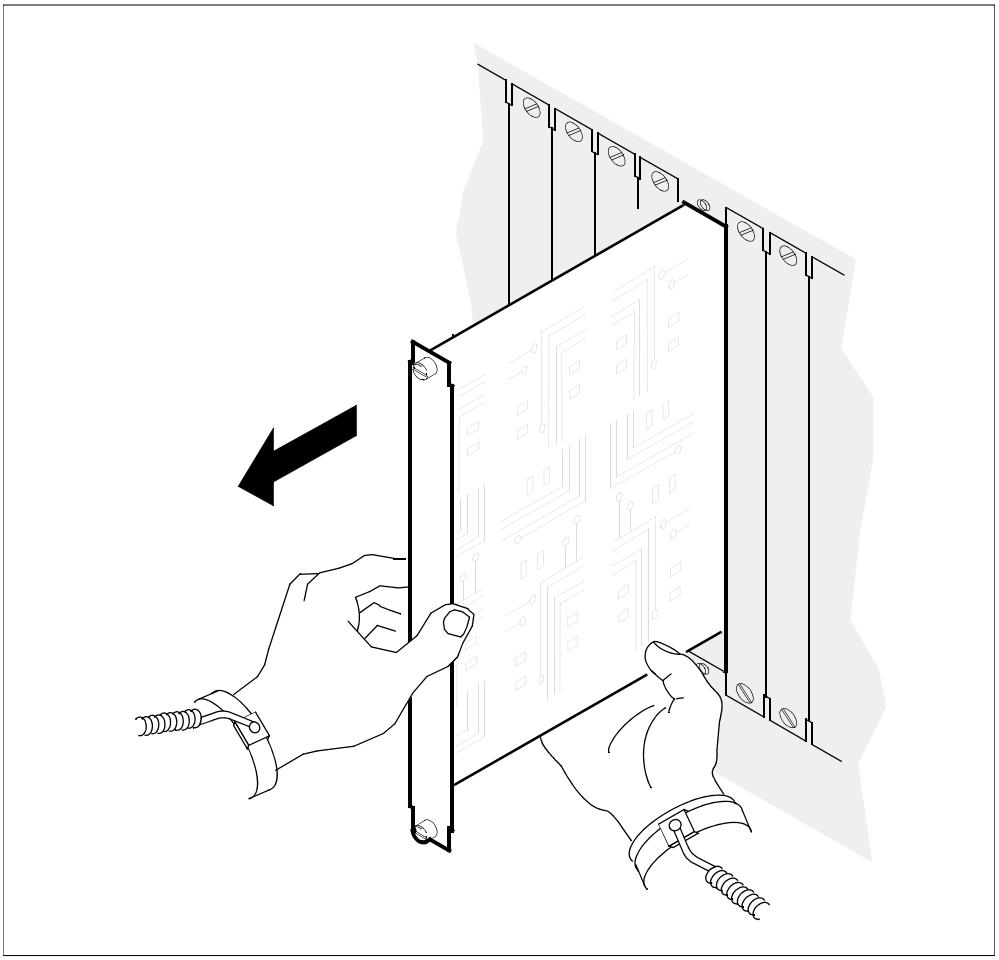
Do not mix the transmit and receive cables for each domain. Label these cables to ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Disconnect the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it 1/4 turn to the left.

21 While grasping the thumbscrews, gently pull the DS512 personality module toward you until it protrudes about 2 inches (5 cm) from the core manager shelf.



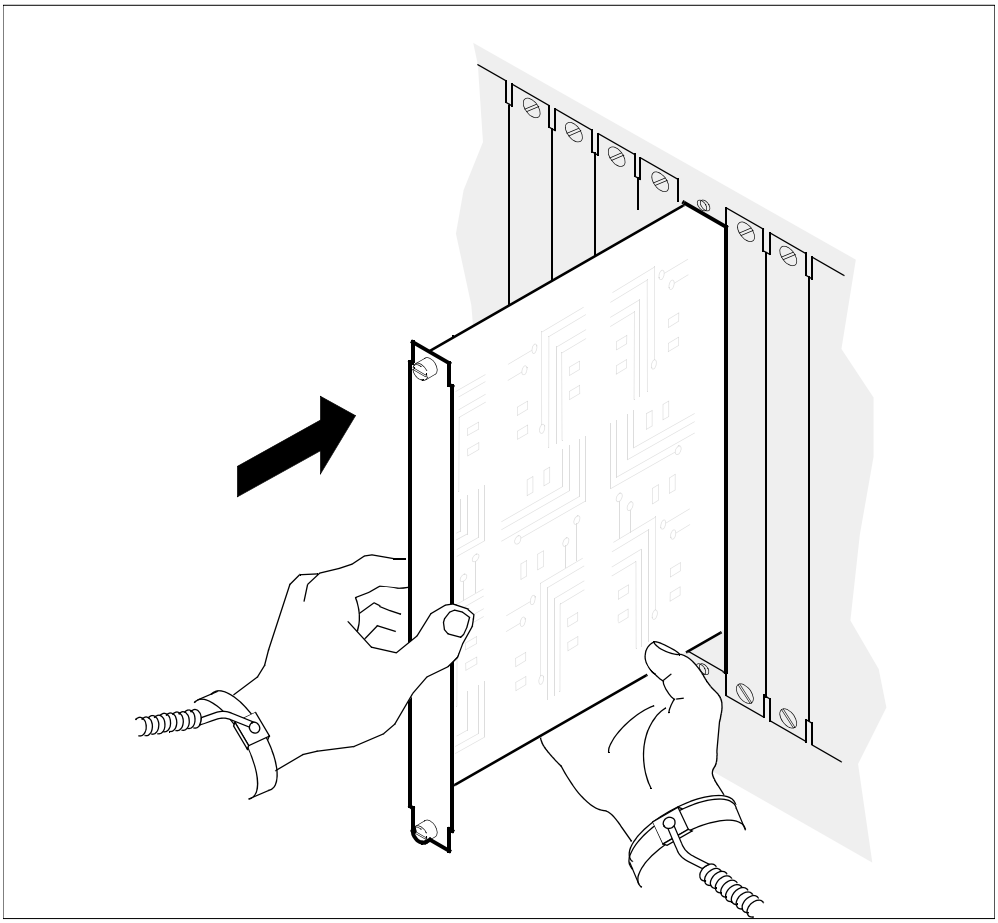
22 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the DS512 personality module toward you until it clears the shelf.



23 Place the DS512 personality module you have removed in an ESD protective container.

24 Insert the replacement DS512 personality module into the core manager shelf.

25 Gently slide the DS512 personality module into the shelf until it is fully inserted.



26 Tighten the thumbscrews at the top and the bottom of the DS512 personality module.

27

CAUTION

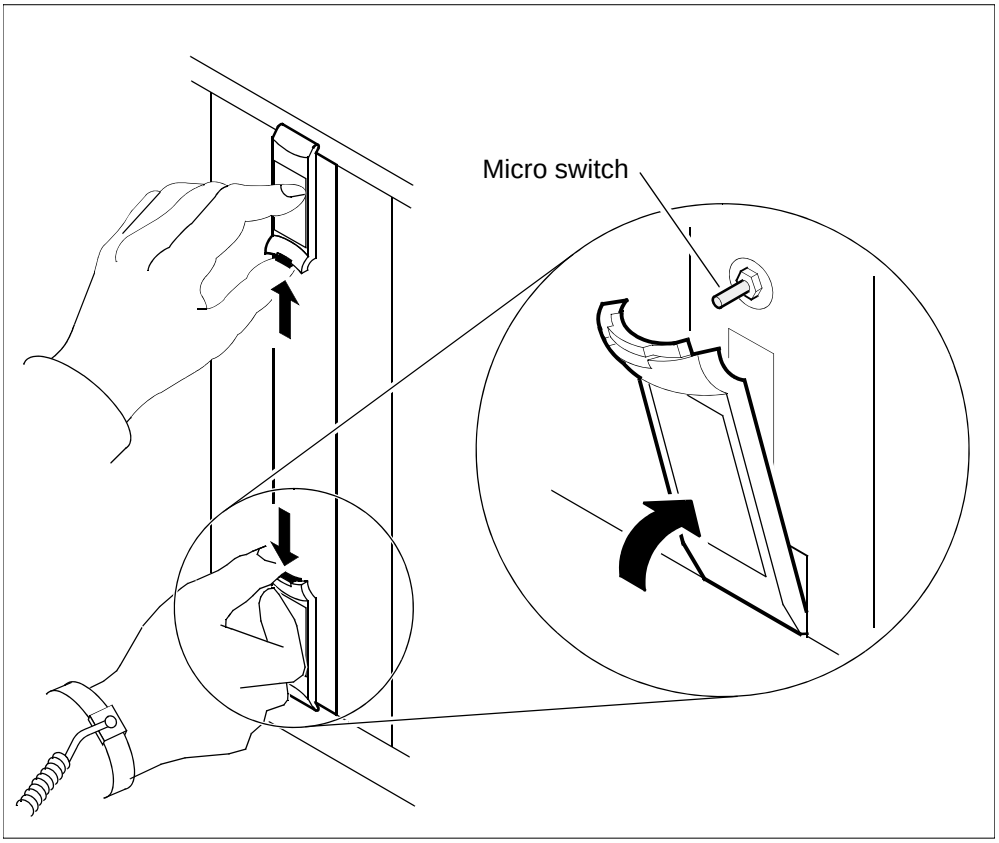
Reconnecting transmit and receive cables

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 the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it 1/4 turn to the right.

At the front of the core manager

28 Close the locking levers to secure the DS512 controller module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



29 Tighten the thumbscrews on the DS512 controller module.

At the local or remote VT100 console

30 Return the DS512 controller module to service:

```
> rts <domain_no> 512
```

where

<domain_no>
is the SDM domain number (0 or 1) of the DS512 controller module you replaced. (See step 13.)

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the RTS command is finished, the *Please wait...* message and the command confirmation disappear. The word *initiated* also changes to *submitted*, then *complete*.

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
complete.
```

Note: At the hardware menu level of the core manager maintenance interface, the state of the DS512 controller module changes to a dot (.), indicating the module has returned to service. The in-service LED on the DS512 controller module is on (green).

At the MAP display

31 At the MS chain level of the MAP (accessed in step 7), return to service the DS512 link between MS plane 0 and the DS512 personality module you replaced:

```
> rts 0 link <link_number>
```

where

<link_number>
is the MS link number:

- 0 if the DS512 personality module is in slot 1 of domain 0, or
- 1 if the DS512 personality module is in slot 12 of domain 1

Example response:

```
Request to RTS MS: 0 shelf: 0 chain:19 link:  0
submitted.
Request to RTS MS: 0 shelf: 0 chain:19 link: 0
passed.
```

Note: The state for the DS512 link changes to a dot (.) if the core manager DS512 link is in-service. Otherwise, the state for DS512 link changes to a “P”.

32 At the MS chain level of the MAP (accessed in step 7), return to service the DS512 link between MS plane 1 and the DS512 personality module you replaced:

```
> rts 1 link <link number>
```

where

link number
is the MS link number (0 if the DS512 personality module is in slot 1 of domain 0, or 1 if the DS512 personality module is in slot 12 of domain 1)

Example response:

```
Request to RTS MS: 1 shelf: 0 chain:19 link:  1
submitted.
Request to RTS MS: 1 shelf: 0 chain:19 link: 1
passed.
```

Note: The state for the DS512 link changes to a dot (.) if the core manager DS512 link is in-service. Otherwise, the state for DS512 link changes to a “P”.

33 You have completed this procedure.

Retrieving and viewing log records

Purpose

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

Application

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

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

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

Procedure

Retrieving and viewing logs

At a terminal or terminal session connected to the core manager

1 Log into the core manager.

2 Start the log query tool using the default settings:

logquery

Example response:

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

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

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


Command:
```

3 Access a list of available parameters and variables to view logs:

logquery -help

4 Enter the applicable command.

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

quit

6 You have completed this procedure.

Shutting down the master server

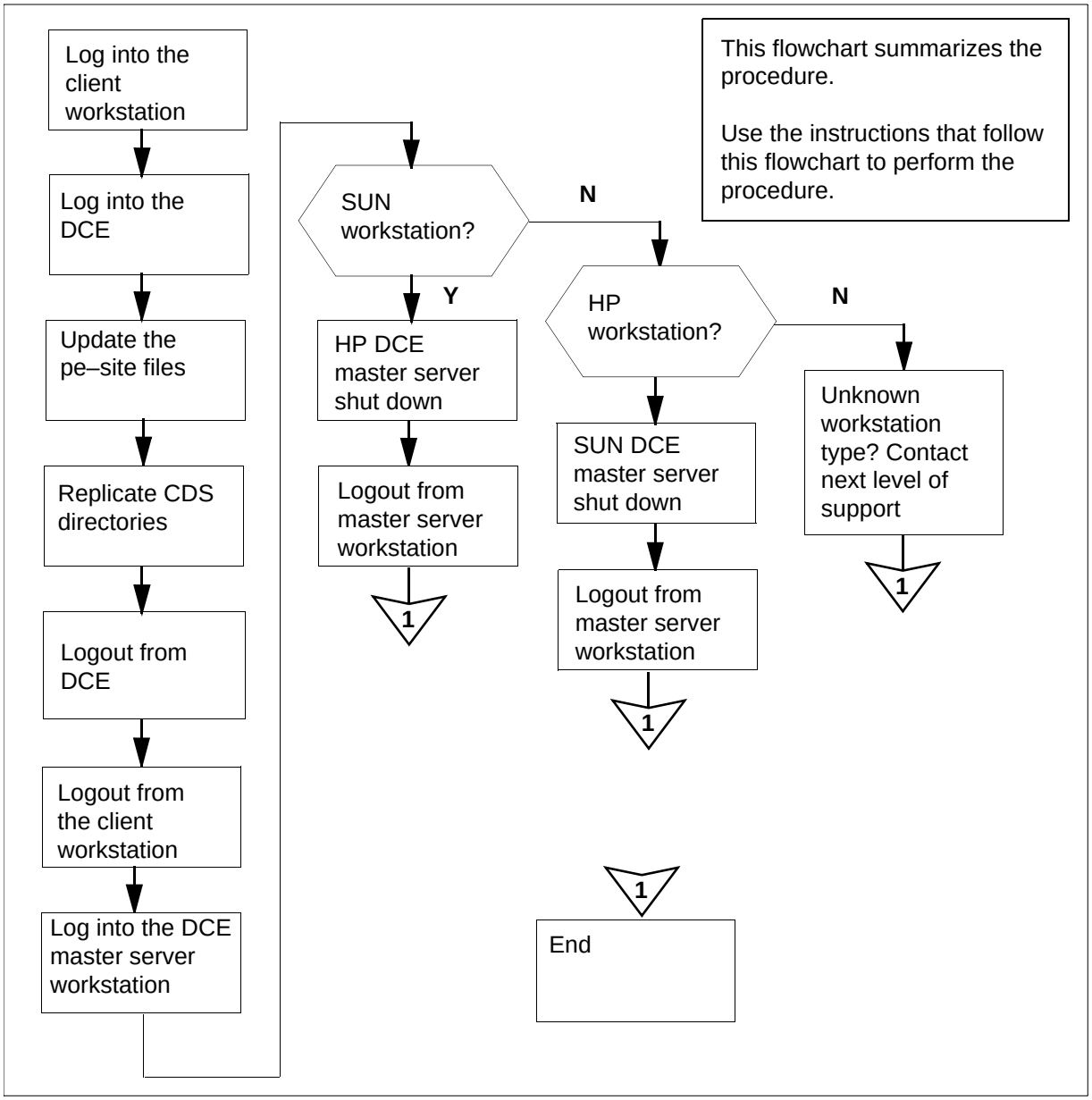
Purpose

Use this procedure when a master server malfunctions, or when you want to designate a different master server.

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure to perform the tasks.

Summary of shutting down the master server



Shutting down the master DCE server

ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator.

At the core manager client workstation

1 Log into the client workstation.

2 Log into DCE:

```
> dce_login <administrator_name>
```

where

<administrator_name>
is the userID of the administrator.

3 Enter the administrator password.

4 Access the /sdm/bin directory:

```
> cd /sdm/bin
```

5 Update the pe_site file:

```
> ./update_pe_site
```

Example response:

```
These are the registry servers currently running
in the cell:
“bmers38”
“bmerye6d” “master”
answer y for “Yes” will update all pe_site data
from above servers on each node within the cell.

Do you want to continue? [y]
```

6 Confirm you want to proceed:

```
> y
```

Example response:

```
host “bmers38” pe_site data is successfully
updated
host “bmers80” pe_site data is successfully
updated
host “bmersa00” pe_site data is successfully
updated
host “bmery7c8” pe_site data is successfully
updated

Security registry pe_site data update complete.
```

Note: If DCE is not running properly on a node, it does not work properly with the backup server. After you fix the DCE problem, on the machine redo step 5 and step 6.

7 Replicate CDS directories:

```
> ./replicate_cds_dirs
```

Example response:

```
The directories from master CDS
server/clearinghouse
“/.../sdmver.bnr.ca/bmerye6d_ch”
will be replicated to the following replicas;
       “/.../sdmver.bnr.ca/bmerha86_ch”
answer y for “Yes” will perform the replication.

Do you want to continue? [y]
```

8 Confirm you want to proceed:

```
> y
```

Example response:

```
Directory /.:/hosts has been replicated in
replica CDS bmerha86_ch
Directory /.:/subsy has been replicated in
replica CDS bmerha86_ch
Directory /.:/subsys/dce has been replicated in
replica CDS bmerha86_ch
Directory /.:/subsys/NT has been replicated in
replica CDS bmerha86_ch
CDS replica directory replicated completed
```

9 Log out from DCE:

```
> exit
```

10 Log out of the client workstation:

```
> exit
```

11 Log into the DCE master server workstation as the root user.

12 Determine the operating system:

```
> uname
```

Example response:

```
HP-UX
```

13 Determine the operating system.

If the O/S you are running is	Do
HP-UX	step 14, step 15, and step 19
SunOS	step 16, step 17, and step 19

If the O/S you are running is	Do
other	step 18

14 Follow the HP vendor's DCE configuration instructions to shut down the master server.

15 Log out of the master server workstation:

```
> exit
```

Go to step 19.

16 Follow the SUN vendor DCE configuration instructions to shut down the master server.

17 Log out of the master server workstation:

```
> exit
```

Go to step 19

18 For this type of operating system, contact your next level of support.

19 You have completed this procedure.

Starting the ETA server on the CS 2000 Core Manager

Purpose

Use this procedure to start an Enhanced Terminal Access (ETA) server.

Application

The ATA and ETA clients run on any remote workstation that is configured in the DCE cell. Along with the ETA server on the core manager, the ATA and ETA clients provide secure terminal access to the MAP/CI terminal and the SDM sessions.

ATA and ETA clients cannot access the ETA server until the ETA server is installed.

Prerequisites

Before you begin this procedure, you must complete the installation procedures described in “Installing the ETA application server software on the CS 2000 Core Manager” in the CS 2000 Core ManagerConfiguration Management document.

Action

Starting the ETA server on the core manager

At the local or remote VT100 console

1 Log into the core manager as the maint user.

2 Access the maintenance interface:

```
maint: sdmmtc
```

3 Access the application (Appl) level:

```
> appl
```

4 The application menu lists the software packages installed on the core manager. Locate the Enhanced Terminal Access application. The version number is the same as the one displayed when the software was installed.

Example of the application menu level:

```
# Application                  State
1 Table Access Service         InSv
2 Operation Measurements       ISTb
3 Log Delivery Service         InSv
4 Enhanced Terminal Access     OffL
```

5 If Enhanced Terminal Access is not InSv, as shown in step 4, then busy it:

```
> bsy <ETA_no>
```

where

<ETA_no>
is the number next to the ETA application.

6 Start the ETA application:

```
> rts <ETA_no>
```

where

<ETA_no>
is the number next to the ETA application.

Note: The state of Enhanced Terminal Access (ETA) shown at the application level must be InSv. The ETA application is dependent on the DCE service on the core manager. If DCE is not in service, then ETA is off-line.

7 You have completed this procedure.

Troubleshooting DCE

Purpose

Use these DCE troubleshooting procedures for solving operational DCE administration problems. Information is provided that defines the cause of the problem, and offers solutions. These procedures must be used by qualified DCE administrators only.

Prerequisites

CAUTION
Risk of inoperable DCE applications
IBM DCE Version 3.1 has changed and no longer provides the executables for the NTP and NULL time providers that are required to configure the time source for the DCE machines. IBM DCE version 2.0 did contain the NTP and NULL time executables.

Proper operation of the DCE cell requires that these time-provider executables are running on the DCE server machines. IBM does provide "sample" .c files that can be compiled into executables. These executables must then be added to the system and configured in a way that ensures they are always running. The details of this process are not fully explained in the IBM documentation.

Core manager applications requiring DCE do not successfully configure into a 3.1 cell without the dts_ntp_provider or dts_null_provider binaries present. In their absence, DCE applications are inoperable.

You can contract with Nortel Global Professional services to install and configure the DCE cell, providing the proper configuration for the required time-provider executables.

Applications

In the following sections, each problem is assigned a number that references its category. For example, the first problem pertaining to DCE Security Service is numbered SEC001.

The problems are grouped into four problem categories as follows:

1. DCE Security Service (SEC) problems
2. DCE Cell Directory Service (CDS) problems

3. DCE Distributed Time Service (DTS) problems
4. miscellaneous (MISC) problems

The events related to DCE are recorded in a suite of standard log files. The log files are as follows:

- /opt/dcelocal/var/svc/error.log

  records the events which indicate an unexpected error occurred
- /opt/dcelocal/var/svc/fatal.log.

  records the events which indicate an unrecoverable error occurred
- /opt/dcelocal/var/svc/warning.log

  records the events which indicate an error that was corrected automatically

DCE Security Service (SEC) Problems

The following paragraphs describe symptoms, possible causes and solutions for DCE security service problems.

SEC001: Failure of dce_login on HP

Symptom:
On HP, dce_login fails with the following message:

```
Password Validation Failure - Registry object not
found (dce/sec)
```

Possible causes:
The DCE security register does not recognize your DCE principal name, or some of the DCE daemons on the DCE server are down.

Solution:
Perform dce_login with valid DCE account name, or start the DCE server daemons, and perform dce_login.

SEC002: Failure of dce_login on SUN

Symptom:
On SUN, dce_login fails with the following message.

```
User Identification Failure - Registry object not
found (dce/sec)
```

Possible cause:
The DCE security register does not recognize your DCE principal name, or some of the DCE daemons on the DCE server are down.

Solution:
Perform dce_login with valid DCE principal name, or start the DCE server daemons, and perform dce_login.

SEC003: Failure of dce_login on HP or SUN

Symptom:
On HP or SUN, dce_login fails with the following message.

```
Password Validation Failure - Invalid password
(dce/sec)
```

Possible cause:
The DCE security register does not recognize the user name, or password.

Solution:
Perform dce_login with valid DCE principal name and password.

SEC004: Failure of dce_login on core manager

Symptom:
On the core manager, dce_login fails with the following message.

```
You entered an invalid principal name or password
```

Possible cause:
The DCE security register does not recognize the password.

Solution:
Perform dce_login with valid DCE principal name and password

SEC005: Failure of dce_login on HP or SUN

Symptom:
On HP, or core manager, dce_login fails with the following message.

```
Clock skew too great (dce/krb)
```

On SUN, dce_login fails with the following message (the message appears in the opt/dcelocal/var/svc/error.log file):

```
Clock skew too great to authenticate (dce/rpc)
```

Possible Cause:
There is a time skew between the machine on which you are trying to login to, and the security server.

Solution:
Use the date -u command on the local machine, and each of the security server machines. The date -u command gives the time on each machine in UTC. This command eliminates possible time zone differences between the different machines. Using the values given by the date -u command, adjust the local machine time to match the security server time.

SEC006: Failure of dce_login on HP or SUN

Symptom:
On HP, or core manager, dce_login fails with the following message.

```
Credentials cache I/O operation failed XXX (dce/krb)
```

On SUN, dce_login fails with the following message.

```
Unable to set context: internal error in sec_login
(dce/sec)
```

Possible cause:
The dce_login command was not able to store the credentials received from the security server. The dce_login command attempts to store these credentials in a file /opt/dcelocal/var/security/creds. The

- disk partition can be full
- directory can be unwritable

If on SUN, you can run dce_login under truss as follows:

truss -f dce login

This identifies the system call that is failing, and the associated errno value.

Solution:
There are two solutions as follows:

- ensure there is enough disk space
- make the /opt/dcelocal/var/security/creds directory world-writable

SEC007: Lost the cell_admin password

Symptom:
Lost the cell_admin password

Solution:
Use locksmith mode of secd to restore the cell_admin account. Locksmith mode is only available to root on the master security server.

Stop the master security server. Restart the server with the following command:

```
> secd - locksmith fooBar -lockpw
```

This command results in the following actions:

- you are prompted for a password for account fooBar (FooBar is the locksmith account)
- secd restarts normally but does not drop into the background
- locksmith mode configures the fooBar account as valid.
- fooBar is configured for access to conduct all processes, despite the ACLs.

Continue with the following steps:

1. Open another window on the master security machine.
2. Login to DCE as fooBar (specifying the secd password).
3. Complete your necessary actions.
4. Reset the cell_admin password or set the account-validity flags back to VALID.
5. Kill the secd process.
6. Restart secd normally, and verify functionality.
7. Delete the fooBar account.

Note 1: The locksmith mode cannot repair damage caused by deletion of crucial security principals or accounts.

Note 2: The locksmith user only has control over the master security server.

SEC008: DCE startup script hangs

Symptom:
During an attempt to start DCE on SUN, the DCE startup script hangs when it tries to activate the secval service. The following message appears:

```
waiting for dced to create string bindings
```

Note: secval represents the security validation service running on a host as part of dced service. This security validation service maintains the security credentials of the host machine.

Possible Cause:
The secval part of dced is trying to log into DCE as hosts/*hostname*/self. The startup script is waiting for the “self” login to complete. If the message “waiting for dced to create string bindings” appears more than three times, the DCE startup script is hung.

Solution:
Perform the following steps to determine the cause of the problem:.

- Verify that at least one security server is operational. Secd is not starting if the message “waiting for dced to create string bindings” appears on a security server machine.
  - Search in the /opt/dcelocal/var/security directory for a log file or a core-dump file from secd.
- Verify that dced, which is started before secd, is operational.
  - if it is not operational, search the /opt/dcelocal/var/dced directory for a log file or a core-dump file from dced.

If the security servers are operational, and the message “waiting for dced to create string bindings” appears on a client workstation, stop the DCE startup script using control-C. Enter the following command:

```
dce_login hosts/<hostname>/self -k /krb5/v4srvtab
```

where

<hostname>
is the name of the local workstation.

You must be logged in as root to enter this command. Replace the value “hostname” with the hostname for your local client workstation. The dce_login command attempts to login as hosts/*hostname*/self using the keytab /krb5/v5srvtab of the client workstation. If dce_login

- is successful, the secval starts. Stop and restart the DCE.
- fails, then go to the SEC002: Failure of dce_login on SUN on page 233 section of this document to get more information.

SEC009: Failure of “dcecp keytab” commands

Symptom:
Dcecp keytab commands fail with the following message:

```
Requested protection level is not supported.
```

Possible cause:
The command is attempting to use DCE packet-privacy encryption. The

packet-privacy encryption relies on DES and is not available in international versions of DCE.

Solution:
Complete the following steps:

- add the “-noprivacy” argument to the keytab command
- restart dced daemon with the -c option

DCE Cell Directory Service (CDS) Problems

The following paragraphs describe symptoms, possible causes and solutions for DCE cell directory service problems.

CDS001: DCE startup script hangs with two cdsadv processes running

Symptom:
On the core manager, the rc.dce process hangs with two cdsadv processes running

Possible cause:
There should be one cdsadv process per host system, and one cdsclerk process per UNIX user who uses DCE.There are three possible causes of this problem:

- the cache file on disk is corrupted because the system crashed when a previous cdsadv process was writing to it
- the cdsadv process underwent “kill -9” while it was saving to disk
- /etc/hosts file contains a faulty line: <IP address to LAN>sdm

Solution:
If the system crashed when a process was writing to it, or the process underwent “kill -9” while it was saving to disk, do the following:

1. Suspend DCE monitor.
2. Stop cdsadv process.
3. Change the directory using command:

   ```
   cd /opt/dcelocal/var/adm/directory/cds
   ```

4. Rename or remove cds-cache.000<some #>and cds_cache.version.
5. Run dce.clean.
6. Re-activate DCE monitor.

If the /etc/hosts file contains a faulty line, do the following:

1. Suspend DCE monitor.
2. Stop the cdsadv process.
3. Remove the faulty line in /etc/hosts file.
4. Ensure that the host name is correct.
5. Run dce.clean.
6. Re-activate DCE monitor.

CDS002: Failure of cdsadv or cdsclerk

Symptom:
On SUN, cdsadv or cdsclerk fails to start. The following message appears.

```
No space left on device.
```

Both cdsadv and cdsclerk use the same CDS cache. The cache is stored on disk /opt/dcelocal/var/adm/directory/cds/cds_cache.nnn. The cache is also kept in memory.

In memory, the cache is accessed through the UNIX inter-process communication (IPC) facility. IPC has three features which are shared memory, semaphores and messages. DCE uses shared memory, and semaphores. DCE does not use messages.

Read the man page for *ipcs* for more information. All of the processes use the following IP resources:

- one 500 KB shared memory segment
- one semaphore set which consists of two semaphores

Possible cause:
The problem can occur because your system IPC resources are used up. It is possible that the semaphores have not been unlocked by other software. Also, the kernel parameters can be configured for too small a value to accommodate the heavy usage of IPC resources.

Solution:
Use the `ipcs` command to examine the IPC resources.

Use the `iperm` command to eliminate the old, unused shared memory and semaphores.

There are several kernel parameters that affect various aspects of IPC resources. These parameters can be left at default values, or they can be set in /etc/system.

Use the `/etc/sysdef` command to check kernel parameters and modify the “etc/system” file to increase IPC limits. A change to “etc/system” requires reboot to take effect.

Review and adjust the following parameters:

Parameter Name	Default (Maximum)	Meaning
seminfo_semmni	10	number of semaphore IDS
seminfo_semmap	10	entries in the free-semaphore-block map
seminfo_semmns	60	number of semaphores
seminfo_semmnu	30	number of processes using SEM_UNDO feature
seminfo_semmsl	25	number of semaphores per ID
shminfo_shmmni	100	number of shared memory IDs

Note: Seminfo_semmap must be set to the same value as seminfo_semmni.

Add the following lines to the /etc/system file:

- set semsys:seminfo_semmns=100
- set semsys:seminfo_semmnu=50
- set semsys:seminfo_semmsl=50

Then reboot the system.

These settings are not definitive. You must understand the IPC needs of the software that runs on your system, and set your kernel parameters accordingly.

DCE Distributed Time Service (DTS) Problems

The following paragraphs describe symptoms, possible causes and solutions for DCE distributed time service problems.

DTS001: Too few dts servers

Possible Cause:
DTS is configured by default to require three time servers. Now, only the DTS server is running within this DCE cell. This problem can be a result of the following reasons:

- some DTS servers are down
- more DTS servers need to be configured
- the default value of the minservers attribute setting of 3 may not be appropriate for your cell

If the DTS servers are down, bring them up.

Configure more DTS servers if required.

If the default value of the minservers attribute is not appropriate for your cell, then reset the value using the following command:

```
dcecp -c dts modify -minservers 1
```

This change is effective until dtsd is stopped. The command must be reissued each time dtsd is restarted.

DTS002: Undetermined drift

Symptom:
DCE is ISTb on the core manager. The log indicates the following message.

```
DTS Clock not synchronized, undetermined drift.
```

Possible Cause:
The following reasons may be causing the problem:

- The lan-profile name of the core manager is not correct.
- The number of dts servers in the DCE cell is less than the value of the minservers attribute of dts. This may be caused by a dead DTS server.

Solution:
Either one of the following solutions is recommended.

1. If the lan-profile name is not correct, then re-commission DCE with the correct LAN profile.

   OR

1. If the number of dts servers is less than the value of the minservers attribute, change the default value of minservers attribute.

2 Change minservers value to less or equal the number of good dts servers currently configured in the cell. You may also be able to bring up a dead DTS server.

DTS003: Failed to retrieve remote server

Symptom:
One of the following messages appears in one of the DCE log files:

- `Can't get remote server's principal name`
- `Failed to retrieve server binding from the namespace`

Possible cause:
The messages above usually indicate that one of the DTS profiles is inaccurate. The dtsd daemon on the local machine is attempting to connect to a remote DTS server. The server is not responding, or the local machine LAN profile is missing or empty.

Solution:
Refer to the solutions offered for problem numbers DTS001: Too few dts servers on page 241 and DTS002: Undetermined drift on page 241.

DTS004: Failure of dtsd

Symptom:
On a SUN workstation, the dtsd daemon does not start. The following message appears.

```
No space left on device
```

Possible cause:
The dtsd daemon cannot allocate its shared memory segment, or semaphores. DTS uses a shared memory segment of size 88 bytes. The key is normally 1. The DTS creates two semaphore sets with the keys normally (shared memory key + 1) and (shared memory key + 2).

The file /opt/dcelocal/var/adm/time/dts_shared_memory_id records the shared memory ID on disk. The DTS shared memory segment is used to hold a block of DTS control data.

Solution:
Other application software, including Oracle and NIS+, also use IPC. Refer to problem number CDS002: Failure of cdsadv or cdsclerk on page 239 for more information on configuring your IPC resources.

DTS005: DCE configuration fails

Symptom:
On core manager, DCE configuration fails with the following message.

```
Configuring DTS Clerk (dts_cl)...Cannot start
/opt/dcelocal/bindtsd
```

Possible cause:
The /var/locks directory was accidentally deleted by a power failure.

The DCE configuration failure caused by the absence of the /var/locks directory causes the DCE dtsd to perform a core dump. The core dump in turn creates a DCE error log in the /opt/dcelocal/var/svc directory. The error log gives a report as follows:

Example
1998-10-13-10:35:43:411-05:00I-----dtsd ERROR dts events logevent_v_ultrix.c 43
2 0x2002722c DCE error: Time service already running on this node (dce / dts)

This report is false as there is no DTS daemon running under these circumstances.

Solution:
Create a /var/locks directory with world-writable permission, and restart the DTS daemon.

DTS006: DCE configuration on the core manager failed on *start DTS daemon*

Symptom:
After the hot removal or insertion on the core manager, the DCE configuration fails on *start DTS daemon* with the following error message.

```
Configuring DTS Clerk (dts_cl...
Cannot start /opt/dcelocal/bin/dtsd
```

Possible cause:
The /var/locks directory is missing.

Solution:
Create a /var/locks directory with world-writable permission, and restart the DTS daemon.

DTS007: DCE clock drift

Symptom:
The *dcecp -c clock show* displays a suffix "-----"

Possible cause:
The DCE clock has an undetermined drift.

Solution:
Enter the following command on a local machine.

 # dcecp -c clock synch

If this command does not remove the drift in about 15 min., check the dts servers for the same drift problem. If the dts servers have the same problem, synchronize the dts servers, and run the above command again. You have to synchronize the time starting with the global server, then the local server, and then the client workstation.

See also DTS002: Undetermined drift on page 241.

Miscellaneous (MISC) Problems

The following paragraphs describe symptoms, possible causes and solutions for miscellaneous problems.

MISC001: Failure of "dcecp hostdata" commands

Symptom:
On HP, core manager, or SUN, dcecp -c hostdata catalog command failed with following message.

```
Communication failure.
```

Possible cause:
The problem may be occurring because the node has multiple IP addresses. DCE does not know which IP address to communicate with.

Solution: Set the environment variable depending on whether you are on core manager, HP or SUN:

1. On core manager, set RPC_UNSUPPORTED_NETIFS to exclude those unsupported IP addresses. Do this before configuring and starting DCE.
2. On HP or SUN, set RPC_SUPPORTED_NETADDRS to include only the supported IP address. Do this before configuring and starting DCE.

MISC002: Name service unavailable

Symptom:
The DCE based application fails. The following error messages may appear.

- `Communication failure`
- `Name service unavailable`

Possible cause:
The DCE daemons are not running on your host. If you are running client-server applications such as ETA, check that the DCE daemons are running on both the client, and the server hosts.

Solution:
Stop, and restart all DCE daemons on all hosts. On DCE client hosts, dced and cdsadv daemons must be running. You may also see one or more cdsclerk and dtsd daemons. On DCE servers, the dced and dtsd daemons can be running. You can see the secd and cdsd daemons depending on the role of the machine.

If you are unsure which DCE daemons run on a specific machine, check the DCE configuration file. Check the processes running on your workstation to make sure that the daemons listed in the configuration file are running on the workstation. The DCE configuration files to check are as follows:

- on the SUN, check the file /opt/dcelocal/etc/setup_state:
  - — if the file has a line that says *startup_dced*, the workstation must be running the dced daemon.
  - — check the processes running on the workstation to confirm that the dced daemon is running.
  - — check the processes on the workstation for every daemon listed in the file with the prefix, *startup_*

Note: Although the DCE configuration file lists the secval daemon (see line that says startup_secval), the secval daemon

does not show up as a process running on the workstation. The secval daemon is part of the dced daemon.

- on the HP, check the file /etc/rc.config.d/dce:
  - if a HP-UX 10.20 operating system, the file is in the current configuration flags section.
  - if the file has a line that says *DCED=1*, the dced daemon is running on the workstation
  - the file has a line that says *SECD=0*, the secd daemon is not running on the workstation.
- on the core manager, check the file /opt/dcelocal/etc/rc/dce:
  - if the file ends with a line that says *daemonrunning $DCELOCAL/bin/dced*, then the dced daemon is running on the workstation.
  - if you find a line such as *#daemonrunning $DCELOCAL/bin/secd*, then the secd daemon is not running on the workstation

MISC003: Port 135 problem

Symptom:
On SUN, the DCE startup script hangs when it attempts to start dced. The message “Waiting for TCP port 135 to clear” appears. The startup script can hang also when at attempt is made to start DCE on the core manager. The message “port 135 is busy” appears.

Port 135 is a port that dced uses. There are two reasons why the startup script may hang:

- DCE was stopped and immediately restarted. The operating system waits three minutes before marking TCP port 135 available for use again.
- another process is using port 135

Solution:
If DCE was immediately stopped and restarted, the DCE startup script hangs for a few minutes. TCP port 135 is then available again.

There must not be any other process using port 135.

Note: llbd can be using port 135. If the llbd (NCS Local Location Broker Daemon) is running, you must prevent lldb from starting. The NCS llbd was developed before dced. Dced is able to emulate lldb if you have older NCS RPC software that depends on llbd.

MISC004: Unknown interface

Symptom:
dcecp keytab, host, hostdata, or server commands fail on SUN. The message “Unknown interface” appears.

Possible cause:
Several dcecp commands are disabled by default in DCE for SUN. This is for security purposes.

Solution:
Re-enable the dcecp commands by running dced with the -x argument.

> ***Note:*** Not all dcecp host and server subcommands are available in the current release of DCE on SUN, even with dced -x. See the release notes for details.

MISC005: Time skew too great

Symptom:
DCE programs indicate “Time skew too great.”

Possible Cause:
An RPC has failed because of a time skew between this machine and a DCE server. Any DCE programs that depend on DCE security fails if the clock skew is greater than five minutes.

Solution:
Check the time-of-day clock on the machine where the message appeared. Also, check the server it was coonected to and all of the security servers.

Use the *date -u* command on the local machine, and each of the security server machines. The *date -u* command gives the time on each machine in UTC. This command eliminates possible time zone differences between the different machines. Using the values given by the *date -u* command, adjust the local machine time to match the security server time.

MISC006: Cannot use *unconfig* option to unconfigure master server

Symptom:
Cannot use *unconfig* option in the dce_config tool on the HP to unconfigure the master server.

Possible Cause:
Unknown. It is possibly a design intent built into the HP.

Solution:
Use DCM, the SAM-based tool, to unconfigure the master server, or reconfigure the entire cell.

MISC007: Cannot start DCE daemons using dce_config tool on the HP

Symptom:
When you stop the daemons and start them again to configure the DCE, the following error message appears.

```
KRB5CCNAME environment variable set.  Possibly in an
invalid dec_login shell, exit before starting DCE.
```

Possible Cause:
Invalid dce_login shell.

Solution:
Log in to the machine as the root user, and use the dce_config tool to start the daemons.

MISC008: dce_config tool on the HP fails to start DCE daemons

Symptom:
While trying to start the daemons using the dce_config tool, the following error message appears.

```
Could not get current time using inetd socket
connection.
```

Possible Cause:
The dce_config tool on the HP tries to synchronize the time with another host, usually the master server. If the master server is on a PC, the above error message appears because the PC does not have inetd.

Solution:
Modify the /etc/dce_config_env file on the HP machine to turn the check_time option off. Replace the check_time option {checktime:=y} with {checktime:=n}.

MISC009: On HP or SUN DCE server, DCE logs can fill up the /opt/dcelocal/var directory

Symptom:
The /opt/dcelocal/var directory reaches its maximum size when the DCE server runs for a long period of time.

Possible Cause:
By default, DCE writes the following logs to the /op/dcelocal/var directory until the directory is full.

Solution:
Monitor the following log files periodically:

- /opt/dcelocal/var/svc/fatal.log
- /opt/dcelocal/var/svc/error.log
- /opt/dcelocal/var/svc/warning.log

Modify the /opt/dcelocal/var/svc/routing file to circulate the log records. Indicate a maximum size for the files. When the file reaches its maximum size, the system replaces the oldest records with the newer records within the log file.

For example, split up a DCE log into seven sub log-files. Set the maximum number of lines for each sub log-file to 1000 lines. When the file reaches the 1001st record, the system replaces the oldest record in the file with the new record.

Example
FATAL:FILE.7.1000:/opt/dcelocal/var/svc/fatal.log
ERROR:FIL.7.1000:/opt/dcelocal/var/svc/error.log
WARNING:FILE.7.1000:/opt/dcelocal/var/svc/warning.log

MISC010: File /etc/dce/rc.dce is empty

Symptom:
When using the sdmconfig program to configure DCE, the following error message appears.

```
Configuring CDS Clerk (cds_cl)...
Cannot add definition of cache server to
/etc/dce/rc.dce
declaration of CACHE_SRV was not found
```

The core manager shows the status of DCE as *Uneq* when the sdmconfig process shows that the DCE configuration has passed.

Possible cause:
The /etc/dce/rc.dce file has faults.

Solution:
Make sure that the /etc/dce/rc.dce file is complete. If the file size is less than 15 Kilobytes, or if the size is 0 Kilobytes, the rc.dce file is not complete.

To recover the rc.dce file, copy an rc.dce file from another core manager with the same operating system.

After you have recovered the rc.dce file, create a soft link from /etc/rc.dce to /etc/dce/rc.dce. Then reconfigure the DCE in the core manager. Refer to the procedure “Configuring the core manager in a DCE cell” in the core manager Configuration Management document.

Troubleshooting log delivery problems

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 CS 2000 Core ManagerConfiguration Management document.

No logs being received at a Log Delivery client

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

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

Refer to procedure “Modifying a log device using logroute” in the CS 2000 Core ManagerConfiguration Management document.

Logs not formatted properly

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

- at the Device menu, verify that the correct log format has been commissioned for the device (STD, SCC2, STD_OLD, SCC2_OLD)
- at the Global Parameters menu, check that the parameters for start and end of line, and start and end of log, are set correctly.

For more information, refer to procedure “Modifying a log device using logroute” in the CS 2000 Core ManagerConfiguration Management document.

Log devices on the computing module are full

If a CS 2000 Core Manager 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.

An example log is shown below:

```
SNM0 SDM *SDM303 NOV19 23:01:15 9897 TBL SDM Base Maintenance
    Package: SDM_BASE.logs
    Process: start_sdmlaq
    Trouble condition asserted
    Reason: No available CM log devices
```

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.

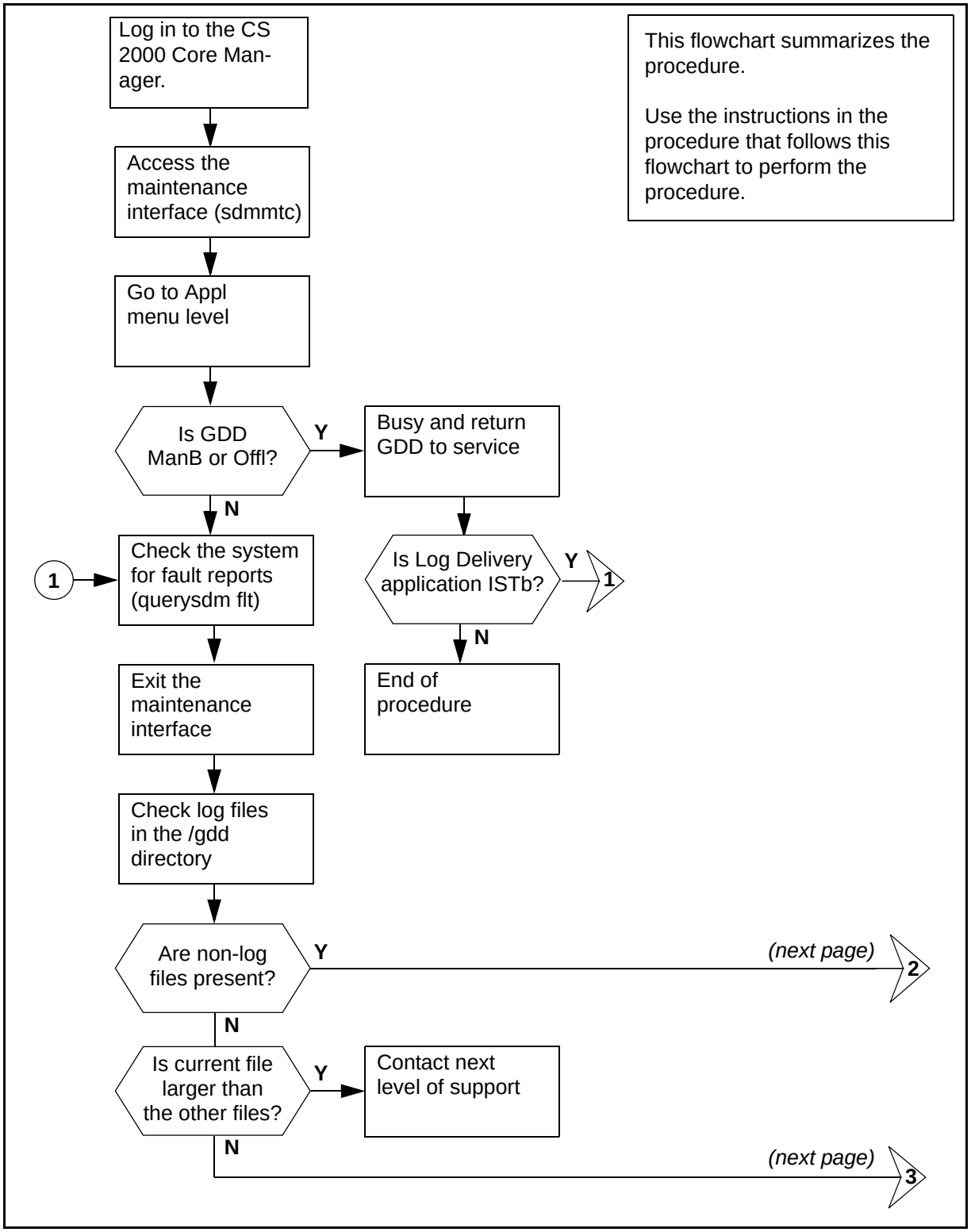
Interval

Perform this procedure when the state of the log delivery application in the Apply menu level of the CS 2000 Core Manager maintenance interface is ISTb.

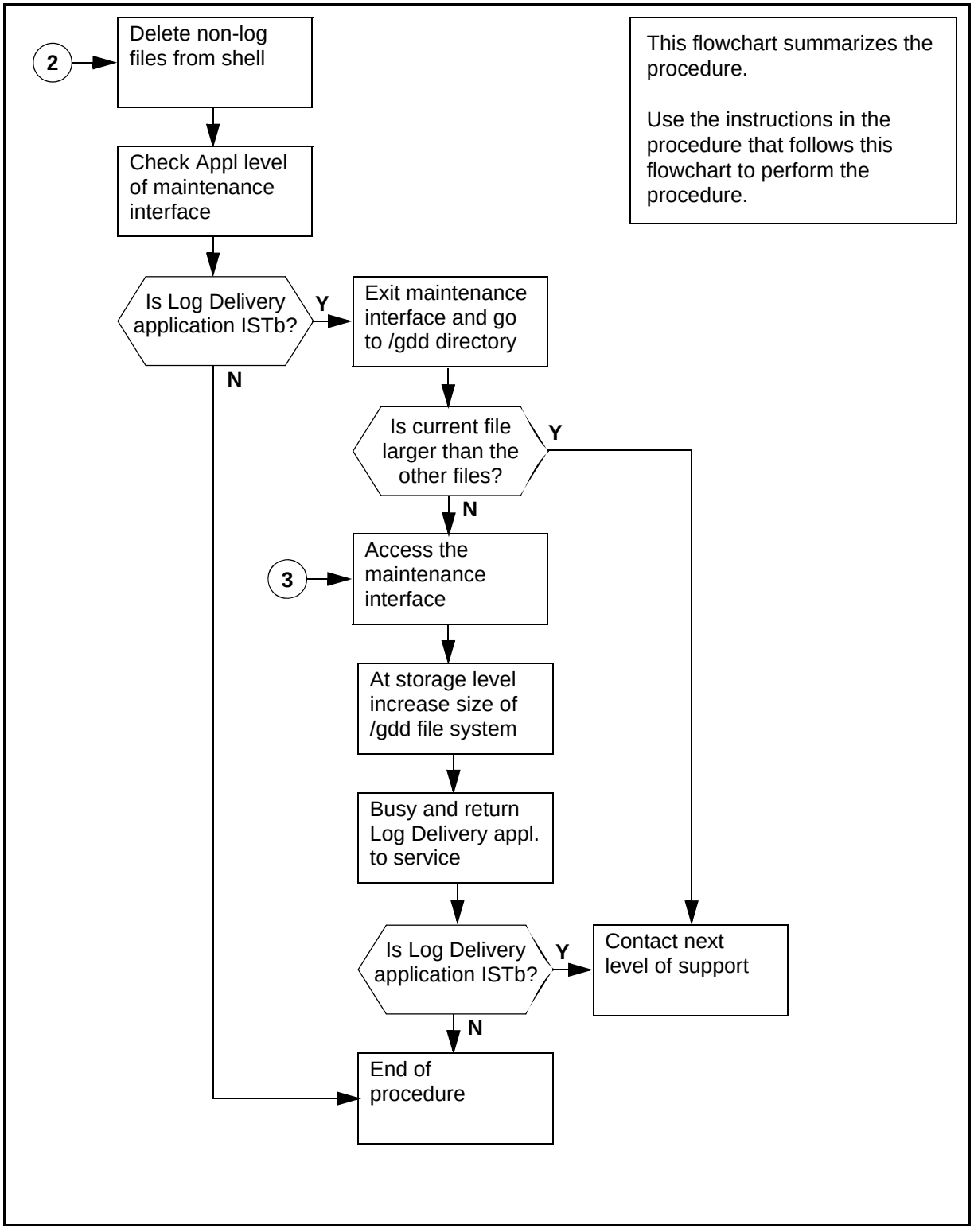
Action

The flowchart that follows provides a summary of this procedure. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Summary of troubleshooting the Log Delivery application when its node state is ISTb *(page 1 of 2)*



Summary of troubleshooting the Log Delivery application when its node state is ISTb *(page 2 of 2)*



Troubleshooting the log delivery application when its state is ISTb

At the local or remote VT100 console

1 Log into the CS 2000 Core Manager as the root user.

2 Access the maintenance interface:

```
# sdmmtc
```

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 CS 2000 Core Manager for any faults:

```
> querysdm 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 22

7 Exit the maintenance interface:

```
> quit all
```

8 Access the /gdd directory:

```
# cd /gdd
```

Note: You must be a root user of the CS 2000 Core Manager 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:

```
# sdmmtc
```

13 Access the application level (Appl):

```
> appl
```

14 Determine if the state of the log delivery application is ISTb. Wait at least one minute 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 /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 Return to the maintenance interface:

```
# sdmmtc
```

20 Access the storage level:

```
> storage
```

21 Increase the size of the /gdd file system:

```
> change lv /gdd <Mbytes>
```

where

<Mbytes>
is the number of megabytes you want to increase the current size of the /gdd file system

Note: Configure the size of the /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

22 Busy the Log Delivery application:

`> bsy <fileset_number>`

where

<fileset_number>
is the number next to the GDD application

23 Return the Log Delivery application to service:

`> rts <fileset_number>`

where

<fileset_number>
is the number next to the GDD application

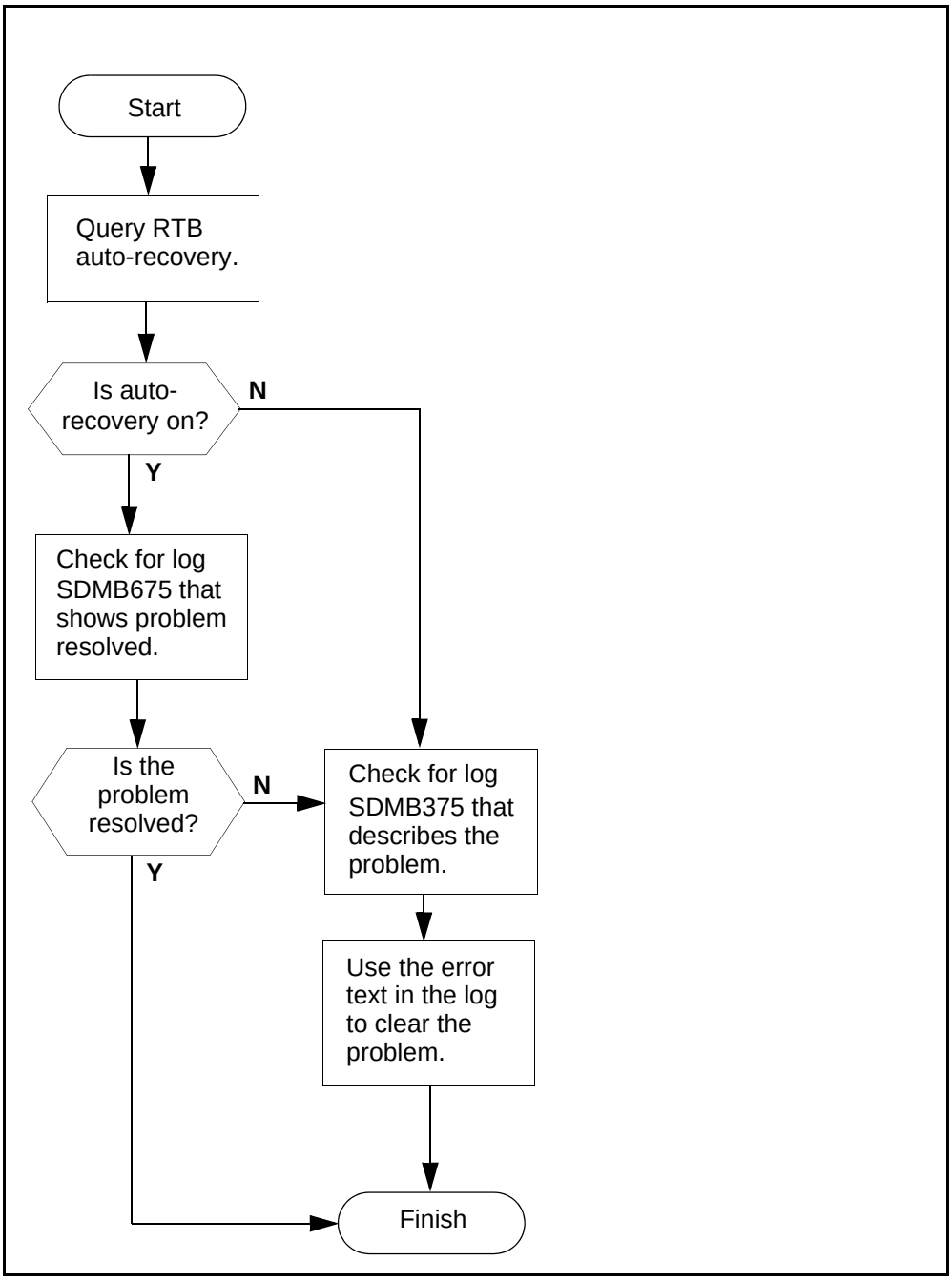
24 Determine if the state of the log delivery application is still ISTb. Wait at least one minute for the ISTb state to change to InSv.

If the Log Delivery application	Do
remains ISTb	contact your next level of support
goes InSv	you have completed this procedure

25 You have completed this procedure.

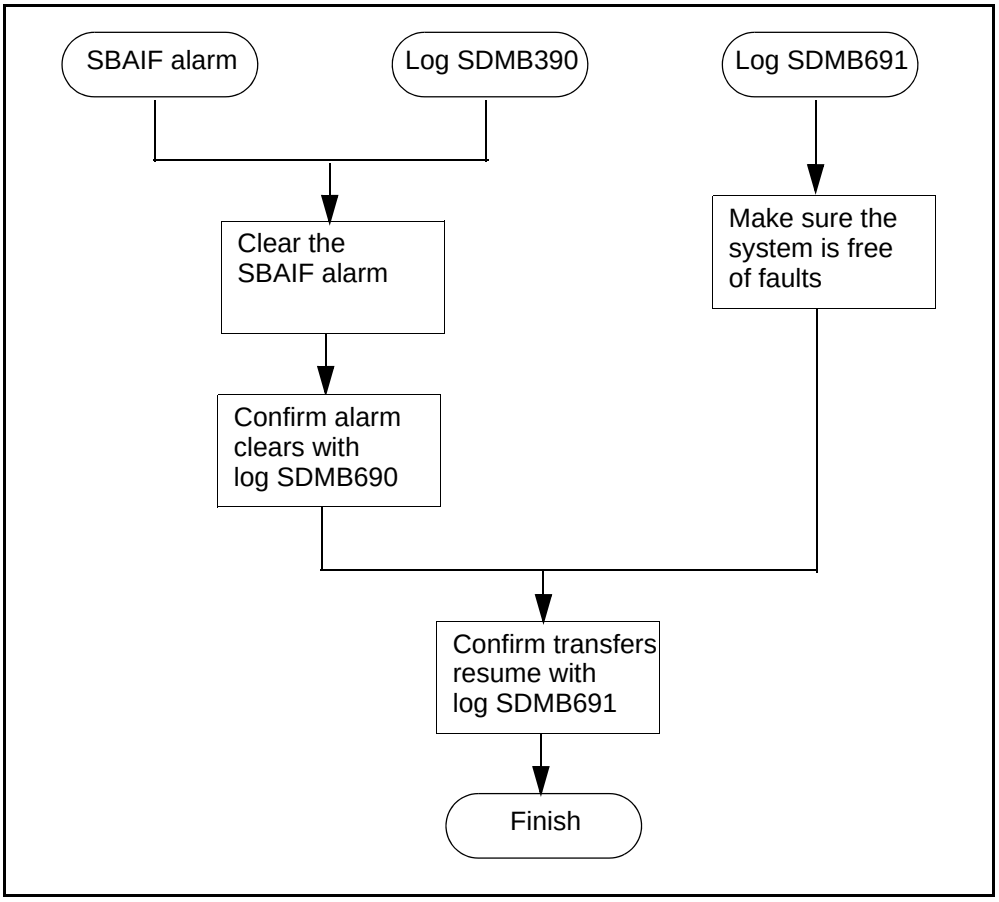
Troubleshooting RTB problems

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



Troubleshooting problems with scheduled billing file transfers

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



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

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

Viewing the dcemonitor status file

Purpose

Use this procedure to view the dcemonitor status file.

Application

The core manager detects common DCE failure conditions, reports them to the core manager node control facility, and automatically takes the appropriate recovery action to clear the problem.

The status of DCE, reported by dcemonitor, is displayed under the LAN connectivity menu level of the core manager remote maintenance interface (RMI).

This automatic DCE maintenance is performed by the dcemonitor script. The dcemonitor script is a Tool Command Language (TCL) program that is continuously executed by a DCE control program (dcecp) running in the core manager platform. Dcemonitor writes its current status, problems found, and the recovery action to a file that is regularly rewritten. By viewing the contents of the status file, you can determine what caused the DCE state change.

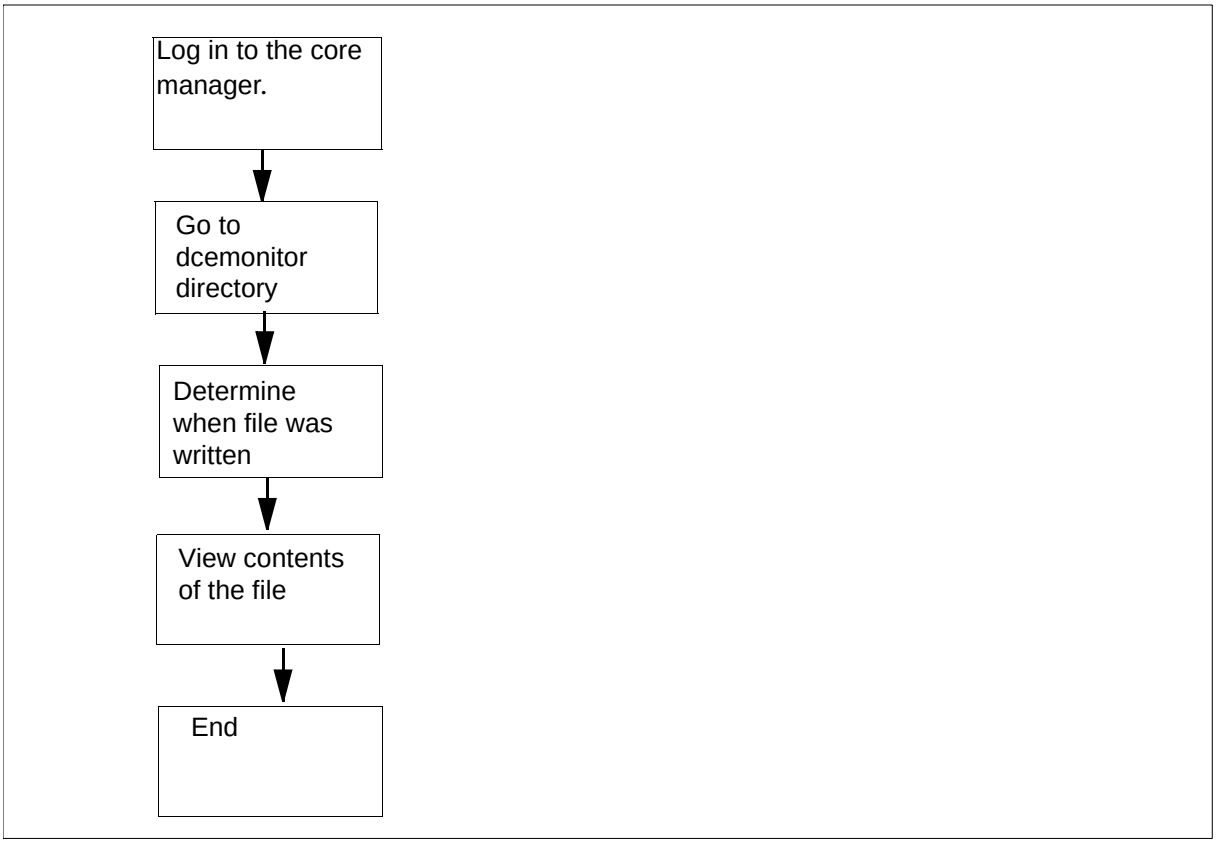
Use this procedure when dcemonitor cannot fix the problem, and manual intervention is necessary. Problems requiring manual intervention include:

- the server identifies a mismatch resulting from a change to the switch Common Language Location Identifier (CLLI)
- the core manager hostname is changed
- the core manager has been restored from a backup tape

Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure to perform the tasks.

Summary of viewing the dcemonitor status file



Viewing the dcemonitor status file

ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator.

At the local VT100 console or remote client workstation

1. Log in to the core manager as the root user.
2. Access the dcemonitor data directory:
   ```
   # cd /sdm/configdata/dce
   ```
3. Determine when the file was last written:
   ```
   # ls -l dce_mon_status
   ```
4. View the contents of the status file:
   ```
   # cat dce_mon_status
   ```
5. You have completed this procedure.

Troubleshooting AFT alarms

Purpose

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

Application

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

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

Indication

At the 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 generated 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.

Procedure

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

Clearing critical alarms

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

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

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

Clearing major alarms

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

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

Procedure

Use the following procedure to clear an AFT alarm manually.

Clearing an AFT alarm manually

At the core manager

1 Access the BILLMTC level:

```
billmtc
```

2 Access the Application (APPL) level:

```
appl
```

3 Access the Automatic File Transfer (AFT) level:

```
aft
```

4 Clear the alarm:

```
alarm cancel <session_name>
```

where:

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

Example response:

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

5 To cancel the alarms, enter:

yes

Example response:

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

6 You have completed this procedure.

Deleting a tuple from automaticFileTransferTable

CAUTION

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

At the core manager

1 Access the BILLMTC level:

billmtc

2 Access the APPL level:

appl

3 Access the AFT level:

aft

4 Access the AFTCONFIG level:

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.

Clearing a system audit alarm

Purpose

Use this procedure to clear a system audit alarm.

Indication

The “SDM System Audit Status” under the system (SYS) level of the core manager maintenance interface has a status of “fail”:

- the SYS level header displays ISTb (in-service trouble), and
- the “SDM” header displays ISTb

When the failure is major, an M is displayed under the SYS and SDM headers.

Meaning

One or more of the system audit checks reported a failure.

Impact

One or more failures exist on the system, which can prevent successful completion of an upgrade.

Action

View the system audit report to determine the failures and take the necessary action. Refer to Viewing the system audit report and taking corrective action on page 29 in this document. Once you have corrected the failures, clear the system audit alarm using the steps that follow.

> ***Note:*** If you choose not to correct the failures, you can still clear the system audit alarm. However, the alarm re-appears on the next execution of the system audit.

Refer to “System audit overview” in the CS 2000 Core Manager Basics document for more information on the system audit.

At the core manager

1 Log in to the core manager.

2 Access the system level:

```
# sdmmtc sys
```

3 Clear the system audit alarm:

```
> audit clear
```

4 When prompted, confirm the command:

> y

5 You have completed this procedure.

Clearing a critical APPL alarm

Application

Use this procedure to clear an APPL SDM critical MAP 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 an SDM critical alarm.

Meaning

An SDM 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 core manager is out of service, all core manager applications are unavailable.

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 processed.

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

Action

Clearing critical APPL alarm

At the MAP display

1 Access the SDM level of the MAP display:

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

Example response:

```
SDM   SysB(NA)    Links_OOS: 4
```

2 Determine the state of the core manager.

If the state is	Do
SysB (NA)	step 4
SysB/ the core manager is not responding	step 3
SysB/core manager online upgrade in progress but not responding	contact your next level of support
SysB	step 68

3 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 four links are out of service	step 11

4 Determine the MS hardware that provides the DS512 links to the core manager:

```
> trnsl
```

Note: The CM has designated the core manager as system busy (SysB) because all four message switch (MS) ports that provide the DS512 links to the core manager are unavailable. The core manager can still be operational, but it is unable to communicate with the computing module (CM).

Example response:

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

5 Record the MS port card number that is associated with the core manager DS512 links.

Note: In the example response shown in step 4, the port card number is 15.

6 Access the MS level of the MAP display:

```
> ms
```

7 Access the shelf level:

```
> shelf 0
```

8 Access the MS port card level that is associated with the core manager DS512 links:

```
> card <cardno>
```

where

<cardno>
is the MS card number noted in step 5.

9 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.

10 You have completed this part of the procedure.

11 Access the EXT level of the MAP display:

```
> ext
```

12 List all major EXT alarms:

```
> list maj
```

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

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

If a core manager-related FSP alarm is	Do
present	step 14
not present	step 16

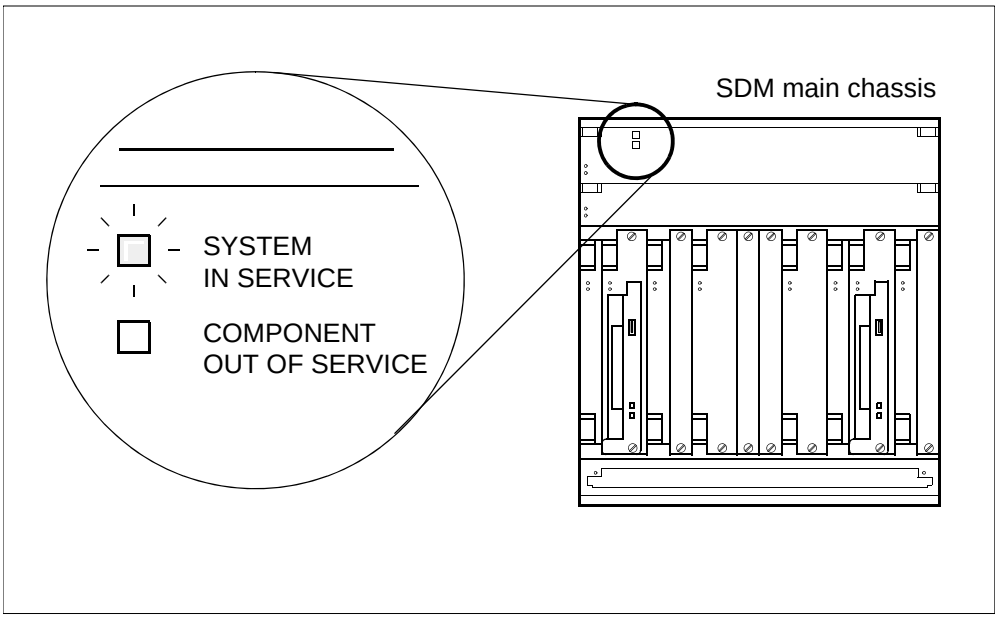
Note: An EXT FSP major alarm triggered by the core manager indicates that one or both -48V dc power inputs to the core manager have failed, or that the core manager has shut down because of thermal failure (overheating).

14 Clear the EXT FSP alarm using the procedure Clearing an EXT FSP major alarm on page 334 in this document.

15 You have completed this part of the procedure.

At the front of the core manager

16 At the front of the core manager, determine if the System in Service light is on (green).



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:

- system software has crashed.
- the system is booting, or the attempt to boot has failed.
- the system cannot boot because both CPUs or both I/O controller modules containing the root volume group (rootvg) are out of service.
- the system has been manually shut down.

If the in-service light is	Do
on	step 44
off	step 17

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

If the system was	Do
manually shut down	step 21

If the system was	Do
not manually shut down	step 18

18 Ensure that the local console is connected to SP0 of the CPU personality module using the designated cable. Ensure that the console is operational and correctly configured for VT100 operation.

At the local VT100 console

19 Log into the core manager as the root user.

20 Determine if the system is booting.

If the system is	Do
booting	step 22
not booting, or the boot has failed	step 21

At the front of the MSP

21 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. Proceed according to the chassis in your system.

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

At the local VT100 console

22 Monitor the boot process. The boot process takes at least 5 minutes.

If the boot process	Do
does not start	step 23
starts, but does not complete (returns to the FX-Bug prompt)	step 35

If the boot process	Do
completes normally, and the login prompt is displayed	step 33

At the front of the core manager

23 Physically verify that the CPU controller modules (NTRX50CF,CG,CH,FK, FL, or FM) are present in the main chassis (slots 6 and 7, and 10 and 11).

24 Determine if either CPU controller module was accidentally unseated or removed. (This situation occurs if one CPU controller module was in manual busy or system busy state, and the remaining in-service CPU controller module was removed in error.)

If	Do
both CPU controller modules are present	step 29
a CPU controller module was removed or unseated	step 25

25

WARNING
Static electricity damage
Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Reinsert the CPU controller module that was removed in error.

At the local VT100 console

26 Determine whether the system has begun to boot.

If the system is	Do
booting	step 28
not booting, or the boot has failed	step 27

At the front of the MSP

27 Cycle power to the core manager by turning the MSP breakers off and on. The MSP breakers supply power to the core manager. Proceed according to the chassis in your system.

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

At the local VT100 console

28 Monitor the boot process. The boot process takes at least 5 minutes.

If the boot process	Do
does not start	step 29
starts, but does not complete (returns to the FX-Bug prompt)	step 35
completes normally, and the login prompt is displayed	step 33

At the front of the core manager

29

WARNING
Static electricity damage
Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Put on the ESD grounding wrist strap.

30 Verify that each CPU controller module is seated correctly and passes self tests by unseating, and then reseating it. Ensure that both CPU controller modules are seated firmly and the latches are closed snugly.

When a CPU controller module is reseated and its latches closed, both LEDs on the CPU controller module turn on solid for

a brief period, indicating that the module is powered up, fully seated, and has passed its self tests.

If	Do
one CPU controller module fails its self tests	step 31
both CPU controller modules fail their self tests	contact your next level of support
both CPU controller modules pass their self tests	step 32

31 Replace the CPU that failed its self tests.

Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the top locking lever of the module. Refer to the appropriate core manager hardware replacement procedures.

At the local VT100 console

32 Monitor the boot process.

If the boot process	Do
does not start	contact your next level of support
starts, but does not complete (returns to the FX-Bug prompt)	step 35
completes normally, and the login prompt is displayed	step 33

33 Access the maintenance interface:

```
# sdmmtc
```

Note: Monitor the alarm banner at the top level of the SDM maintenance interface. Wait at least 10 minutes for the core manager to recover (until all items on the alarm banner display a dot).

34 Go to step 43.

At the front of the core manager

35 Physically verify that the I/O controller modules that provide root volume group (rootvg) storage for the system, are present in the main chassis (slots 2 and 3, and 13 and 14).

Determine if either I/O controller module was accidentally unseated or removed. (This situation can occur if one I/O controller module was in manual-busy or system-busy state, and the remaining in-service I/O controller module was removed in error.)

If	Do
both I/O controller modules are present	step 38
an I/O controller module was removed or unseated	step 36

36 Reinsert the I/O controller module that was removed in error.

37 Go to step 39.

38 Unseat and reseat both I/O controller modules in slots 2 and 3, and slots 13 and 14. Ensure that they are seated firmly and that the latches are closed snugly.

At the front of the MSP

39 Cycle power to the core manager by turning the MSP breakers off and on. The MSP breakers supply power to the core manager. Proceed according to the chassis in your system.

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

At the local VT100 console

40 Monitor the boot process at the local VT100 console.

If the boot process	Do
does not start	step 41
completes normally, and the login prompt is displayed	step 43

41 Perform a system software reinstall using the procedure "Performing a full restore of the software load from S-tape" in the CS 2000 Core Manager Security and Administration document. Ensure that you reboot the system as indicated in that procedure.

42 Monitor the boot process.

If the boot process	Do
starts, but does not complete (returns to the FX-Bug prompt)	contact your next level of support
completes normally, and the login prompt is displayed	step 43

43 Complete the remainder of the procedure "Performing a full restore of the software from S-tape" in the CS 2000 Core Manager Security and Administration document.

At the local or remote VT100 console

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

45 Access the maintenance interface:

```
# sdmmtc
```

46 Access the maintenance (Mtc) level:

```
> mtc
```

47 Access the connectivity (Con) level:

```
> con
```

Example response:

```
Heartbeat status:                SysB
IP address synchronization:        .

DS512 Link States:
I/O domain 0, port 0:            Closed
I/O domain 0, port 1:            Closed
I/O domain 1, port 0:            Closed
I/O domain 1, port 1:             Open
```

48 Continue according to state of the DS512 links.

If	Do
all four links are failed	step 55

If	Do
any of the links are closed	step 49

49 Note the I/O domain number and port number of each closed link.

At the back of the core manager

50 Physically inspect the fiber link connections to the core manager DS512 personality modules.

If the fibre links	Do
require reconnecting or replacement	step 51
appear undamaged, and are correctly connected	step 53

51

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 DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the right.

At the local VT100 console

52 Monitor the link status at the connectivity (Con) level.

If	Do
any of the links are closed	step 53
all four links are open	you have completed this procedure
two links are open, and two links are failed	step 55

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

At the MAP display

53 At the MAP display, determine the MS hardware that provides the DS512 links to the core manager:

```
> trnsl
```

Example response:

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

54 Record the MS port card number associated with the system-busy DS512 links identified in step 52.

Note: In the example response shown in step 53, the port card number is 15.

At the local VT100 console

55 Access the hardware (Hw) menu level of the SDM maintenance interface:

```
>hw
```

56 Check the status of the DS512 controller modules, indicated under the *512* header.

If	Do
either of the DS512 controller modules are manually busy (indicated by an M)	step 57
both DS512 controller modules have failed (indicated by an F)	step 60
one DS512 controller module failed, and the other is in service (indicated by a dot)	step 59
both DS512 controller modules are in service	contact your next level of support

57 Determine from office records or other personnel why one or both DS512 controller modules are manually busy. When permissible, return each manual-busy DS512 controller module to service:

```
> rts <domain_no> 512
```

where

<domain_no>
is the domain number (0 or 1).

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message, and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
submitted.
```

58 Check that the system displays a dot for the status of the DS512 controller modules indicated under the *512* header.

If	Do
both DS512 modules are in service (indicated by a dot)	you have completed this procedure
only one DS512 module is in service	contact your next level of support

59 Return the failed DS512 controller module to service using the procedure Clearing a minor or major APPL SDM alarm on page 286.

If you	Do
cannot return the DS512 module to service	contact your next level of support
can return the DS512 module to service	you have completed this procedure

At the front of the core manager

60 Physically verify that the two DS512 controller modules (NTRX50GA, front slots 1 and 12) are present in the main chassis.

61 Determine if either of these modules were accidentally unseated or removed. (This scenario may have occurred if one DS512 controller module was in manual-busy or system-busy state, and the remaining in-service DS512 controller module was removed in error.)

Note: If both LEDs on the DS512 controller module are off, the module is not seated correctly.

If	Do
both DS512 modules are present	step 66
one DS512 controller module was removed or unseated	step 62

62 Reinsert the DS512 controller module that was removed or unseated in error. Ensure that the module is seated firmly and that the latches are closed snugly.

At the local VT100 console

63 Return the DS512 controller module to service:

```
> rts <domain_no> 512
```

where

<domain_no>
is the domain number (0 or 1).

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message, and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command
submitted.
```

64 Check the status of the DS512 controller modules, indicated under the *512* heading.

If	Do
both DS512 modules have failed (indicated by an F)	step 66
one DS512 controller module is in service, and one has failed	step 65

65 Return the system-busy DS512 controller module to service using the procedure Clearing a minor or major APPL SDM alarm on page 286.

If you	Do
cannot return the DS512 module to service	contact your next level of support
can return the DS512 module to service	you have completed this procedure

At the front of the core manager

66 Replace the failed DS512 controller module at the front of the core manager using the procedure Replacing the DS512 personality module on page 209.

Note: You can determine if a DS512 controller module is faulty by viewing the component out-of-service LED and the system in service LED. If the module is faulty, the component out-of-service LED is on (red), and the system in service LED (green) is off.

67 Go to step 68.

At the MAP display

68 The core manager state SysB at the MAP display with no additional qualifier (NA or / not responding) indicates that the core manager is communicating successfully with the CM. However, all core manager applications have failed, or another internal core manager problem exists. Manually busy the core manager:

```
> bsy
```

Example response:

```
SDM Bsy initiated.
SDM Bsy completed.
```

69 Return the core manager to service:

```
> rts
```

Example response:

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

If the core manager	Do
recovers	you have completed this procedure
does not recover	step 70

70 Busy the core manager at the MAPCI;MTC;APPL;SDM level:.

```
> bsy
```

71 Reboot the core manager:

```
> rebootsdm
```

Note: Wait for the */Reboot SDM in progress* message to disappear from the screen before you continue with the procedure.

72 Return the core manager to service:

> RTS

If the SysB state	Do
returns	contact your next level of support
does not return	you have completed this procedure

Clearing a minor or major APPL SDM alarm

Purpose

Use this procedure to clear an APPL SDM minor or major 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. This appearance indicates an SDM minor or major alarm. If the alarm is major, the letter M also appears below SDM.

Meaning

An SDM minor or major alarm indicates that the core manager is in manual-busy (ManB) or in-service trouble (ISTb) state.

Application

If the core manager state at the MAP display is ManB, the core manager was set to that state by the MAP command.

If the core manager state at the MAP display is ISTb, the computing module (CM) is receiving ISTb status from the core manager. One or more of the following conditions exist:

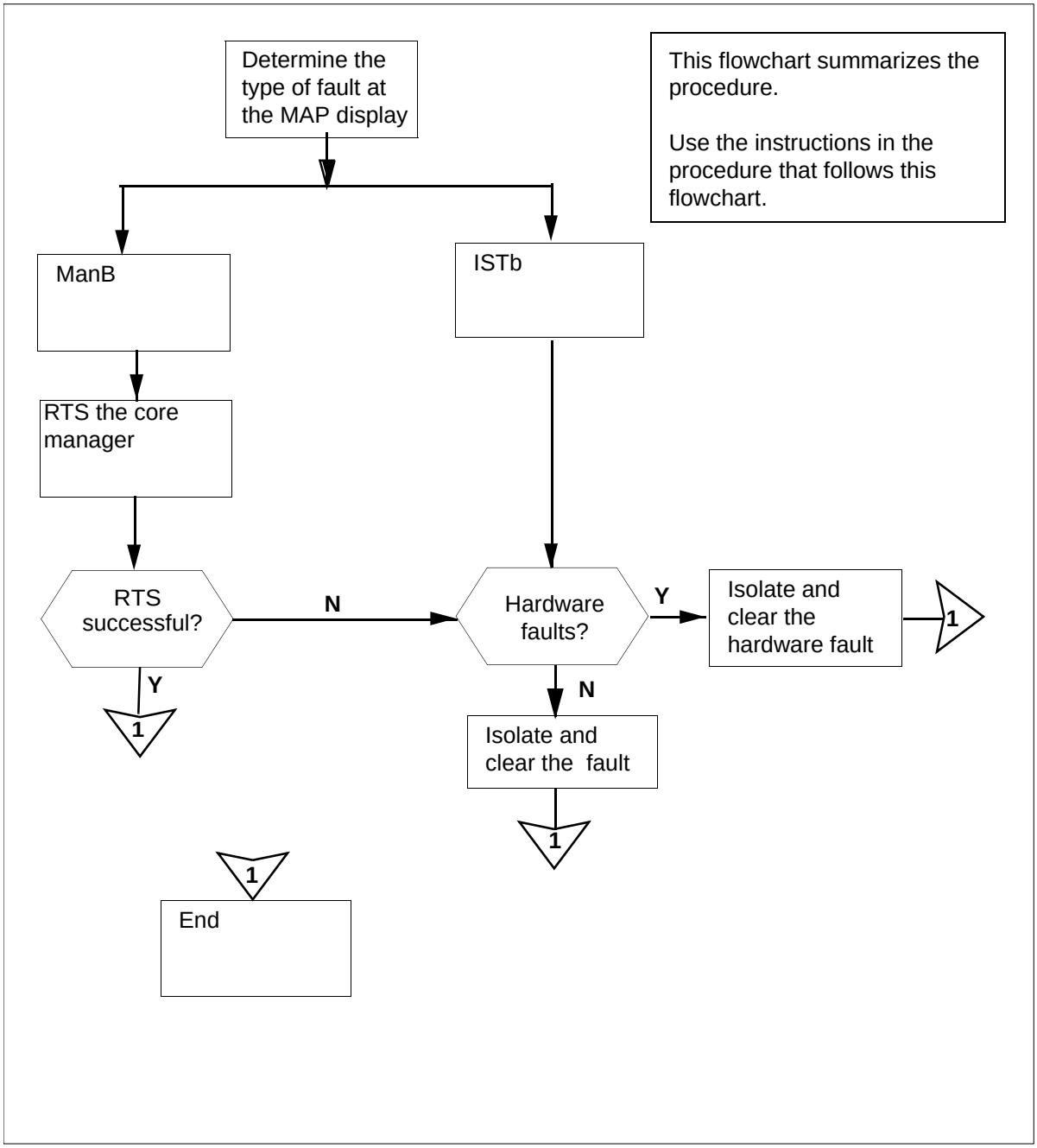
- one or more core manager applications have failed, but at least one application has not failed
- a system software resource has exceeded its alarm threshold
- the core manager cannot communicate with one or more defined nodes on the local area network (LAN) of the operating company
- the Distributed Computing Environment (DCE) is not in service
- a core manager application is reporting an in-service trouble condition
- a hardware device failure has been reported.
- disk mirroring is in progress or has failed.
- there is an Internet protocol (IP) mismatch between the CM and the core manager

Note: If all core manager applications fail, the core manager node state is system busy (SysB). The system generates an APPL SDM critical or APPL SysB critical alarm.

Action

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

Summary of clearing a minor or major APPL SDM alarm



Clearing a minor or major APPL SDM alarm

At the MAP display

1 Access the SDM level at the MAP display:

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

Example response:

```
SDM 0 ISTb LINKS_OOS: .
```

2 Check the node state of the core manager at the MAP display.

If the state is	Do
ManB	step 3
ISTb	step 4

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

```
> rts
```

Example response:

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

If the core manager	Do
returns to service	you have completed this procedure
does not return to service	step 4

4 Obtain fault status information from the core manager:

```
> querysdm flt
```

Example Response:

```
* SDM300 Connection has been lost
   Type: LAN
   Host Name: noc
   Fri Jan 22 11:12:58 1999

* SDM317 DCE problem detected
   Reason: DTS Clock not synchronized,
undetermined drift
   Fri Jan 22 15:56:40 1999

* SDM303
   Package: SDM_BASE.tasl
   Process: taslddm
   Trouble condition asserted
   Reason: tasltm: Data Dictionary not
available
   Fri Jan 22 15:56:43 1999

* SDM303
   Package: SDM_BASE.omsl
   Process: omslomm
   Trouble condition asserted
   Reason: OMM-CMMGMT Link Down
   Fri Jan 22 15:56:25 1999

* SDM303
   Package: SDM_SURV.excrep
   Process: hug
   Trouble condition asserted
   Reason: OM service NOT available
   Fri Jan 22 15:56:26 1999
```

5 Use the following table to determine the type of fault indicated by the response. Note the log type for use in later steps.

Fault type	log number	Description
Connection	SDM300	Connection has been lost Type: CM <reason> Connection has been lost Type: LAN Host Name: <hostname>
Logical volume	SDM301	Logical volume(s) not mirrored Volume group name: <vgn> Status: <status>
Exceeded resource threshold	SDM302	Resource threshold exceeded Type: CPU Current Value/Threshold: <n><n> Resource threshold exceeded Type: Swap space Current Value/Threshold: <n><n> Resource threshold exceeded Type: Number of Processes Current Value/Threshold: <n><n> Resource threshold exceeded Type: Number of swap queue entries Current Value/Threshold: <n><n> Resource threshold exceeded Type: Number of zombie processes Current Value/Threshold: <n><n> Resource threshold exceeded Type: Logical volume Name: <name> Current Value/Threshold: <n><n>

Fault type	log number	Description
Application	SDM303	Package: <package> Process: <process> exceeded failure threshold Package: <package> Process: <process> Trouble condition asserted Reason: <reason>
Hardware	SDM309	Hardware device out of service Device: <device> Device state: <devicestate> Suspected module: <suspectedmodule> Location: <location> Other devices on module: <otherdevices> Fault category: <faultcatagory> Reason: <reason>
DCE	SDM317	DCE problem detected Reason: <reason>
Split mode status	SDM321	Split-system upgrade in progress Status: <spmdstatus> spmdstatus = started SwAct started SwAct completed SwAct started for fallback Completed
Network Time Protocol (MNTP)	SDM327	Network Time Protocol (MNTP) problem detected: <reason>

6 Determine the type of fault.

If the fault is	Do
a connectivity problem with fault type CM (300)	step 27
a connectivity problem with fault type LAN	step 54
a logical volume problem (301)	step 15
an exceeded resource threshold (302)	step 7
a hardware device fault (309)	step 66
a DCE problem (317)	have your system administrator isolate and clear the problem
an application problem (321)	step 17
an NTP problem (327)	have your system administrator isolate and clear the problem

At the local or remote VT100 console

7 Log into the core manager as a maint class user, or root user, and access the maintenance interface:

```
# sdmmtc
```

8 Access the maintenance level:

```
> mtc
```

9 Obtain fault status information from the core manager:

```
> querysdm flt
```

From the response, determine the type of system resource that has exceeded its alarm threshold.

If the resource exceeded is	Do
swap space	step 10
number of processes	step 10
number of swap queue entries	step 10

If the resource exceeded is	Do
number of zombie processes	step 10
CPU (number of run queue entries)	step 10
logical volume	step 12

10 Access the System (Sys) level:

> sys

Example response:

```
SDM Storage State:
# Description                    Current /
Threshold
1 CPU (run queue entries):            1 /  5
2 Number of Processes:               75 / 250
3 Number of Zombies:                  0 /  3
4 Swap Space (% full):               72 / 70 !
5 Number of Swap Queue Entries:       0 /  2
```

11 Check the current level of the software resource by locating the resource identified in step 9.

Note: A pair of numbers is located to the right of the software resource's description:

- the first number is the current level of the resource
- the second number is the alarm threshold

In the example response in step 10, the current level of "Swap Space" is 72. This level exceeded the threshold of 70. The "!" character indicates the threshold has been exceeded.

If you have	Do
exceeded the system threshold	contact your next level of support
not exceeded the system threshold	you have completed this procedure

Note: In an emergency, you can temporarily clear the problem by rebooting the core manager. When you reboot the core manager, the core manager remains out of service for approximately 15 minutes.

12

CAUTION
Potential Service Interruption
A logical volume on the core manager 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 Networks for assistance.

13 Access the storage level:

```
> storage
```

Example response:

```
Volume Groups     Status          Free(MB)
rootvg            Mirrored        1932
datavg            Mirrored        7760

Logical volume    Location    Size(MB)%  full/
threshold
1 /               rootvg      88           11/ 80
2 /usr            rootvg      600          28/ 90
3 /var            rootvg      200           7/ 70
4 /tmp            rootvg      24            5/ 90
5 /home           rootvg      304          11/ 90
6 /sdm            rootvg      504          23/ 90
7 /data          datavg     208          81/ 80 *
                Logical volumes showing: 1 to 7
of 7
```

14 The asterisk (*) indicates that you have exceeded a specific system threshold. Contact the next level of support to correct this problem.

15 At the local or remote VT100 console, determine the status of the core manager from the status field in log SDM301.

If the status is	Do
integrating	step 16

If the status is	Do
not mirrored	step 16
I/O error detected while writing to %s (possibly due to double disk fault)	step 16

16 Allow the logical volume reintegration process to complete without intervention. This process is initiated automatically whenever an I/O controller module is returned to service, and synchronizes (mirrors) data on the two hard disks.

Note: The reintegration process can take more than 30 minutes to complete. The processing time depends on the amount of data (in the affected volume group) the core manager has to integrate. The status of the volume group reintegration can be monitored by selecting the storage option from the system (Sys) level.

If the integration is	Do
successful	you have completed this procedure
not successful	contact your next level of support

Logical volumes are not mirrored under the following circumstances:

- an I/O controller module is out of service
- a hard disk drive is out of service
- a hard disk has just returned to service and the reintegration process is just about to start (as described in step 16). In rare cases, the system cannot start or complete automatic volume group reintegration. For example, the reintegration process is interrupted due to a power failure or system reboot.

If the mirroring problem is	Do
due to an abnormal reintegration process interruption or failure	contact your next level of support
due to recently returned-to-service hardware	step 16

If the mirroring problem is	Do
due to out-of-service hardware	step 67

At the local or remote VT100 console

17 Log into the core manager as a maint class user, or root user, and access the maintenance level:

```
# sdmmtc
```

18 Access the application (Appl) menu level of the RMI:

```
> appl
```

Example response:

```
# Application                          State
1 Table Access Service                   .
2 Log delivery Service                   .
3 OM Access Service                      .
4 Secure File Transfer                   ManB
5 Enhanced Terminal Access               ISTb
6 Exception Reporting                    ISTb
                    Applications showing: 1 to 6
of 6
```

19 Determine the affected application from the display and note its key number, shown under the header “#”.

20 Determine the state of the application.

If the application is	Do
ManB	step 21
ISTb	step 22
SysB	step 23
Fail	step 24

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

```
> rts <app_key_no>
```

where

<app_key_no>
is the key number next to the application you want to return to service

Example response:

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

Note: When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted” as follows:

```
Application RTS - Command submitted.
```

If the application	Do
returns to service	you have completed this procedure
does not return to service	step 20

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

If you suspect either situation to be true, wait 10 minutes for the packages 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 the problem	you have completed this procedure
cannot resolve the problem	contact your next level of support

23 Use the value in the Reason field to resolve the problem.

If you	Do
can resolve the problem	you have completed this procedure
cannot resolve the problem	contact your next level of support

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

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

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

> bsy *key*

where

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

Example response:

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

Note: When the Bsy command is finished, the "Please wait..." message and the command confirmation disappear. The word "initiated" also changes to "submitted" as follows:

```
Application Bsy - Command submitted.
```

25 Return the application to service:

> rts *key*

where

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

Example response:

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

Note: When the RTS command is finished, the "Please wait..." message and the command confirmation disappear. The word "initiated" also changes to "submitted" as follows:

```
Application RTS - Command submitted.
```

26 Determine the state of the application.

If the application	Do
remains in a Fail state	refer to the configuration or installation information modules in the core manager Configuration or Upgrade documents, specific to that application

If the application	Do
changes to InsV state	you have completed this procedure

27 Determine if the response indicates an IP address mismatch.

If the QUERYSDM FLT response indicates	Do
an SDM IP address mismatch	step 28
a CM IP address mismatch	step 31
anything else	contact your next level of support

At the MAP display

28 Access table SDMINV:

```
> table sdminv; list all
```

29 Record the datafill value for the core manager CM-side IP address (field IPADDR).

30 Go to step 33

At the MAP display

31 Access table IPNETWRK:

```
> table ipnetwrk; list all
```

32 Record the datafill value for the CM IP address (field CMIPADDR).

33 Check the address from step 29 and step 32 against office records.

If	Do
both addresses are correct	step 28
neither address is correct	contact your next level of support

At the local or remote VT100 console

34 Access the connectivity (Con) level:

```
> con
```

35 Determine how the CM IP, SDM IP, and CM/SDM netmask addresses are commissioned on the core manager:

```
> querysdm
```

Example response:

```
CM IP Address:                  47.105.155.1
SDM IP Address:                 47.105.155.6
CM/SDM Netmask:                 255.255.255.248
```

36 Record the CM IP, SDM IP, and CM/SDM netmask addresses.

At the MAP display

37 Busy the core manager:

```
> bsy
```

Response:

```
SDM Bsy initiated.
SDM Bsy completed.
```

At the local or remote VT100 console

38 Access the change editor for the CM side IP parameters:

```
> change
```

Note: Only the root user can access the editor.

39 Access the change editor for the CM side IP parameters:

```
> change <hostname_key>
```

where

<hostname_key>
is the numeric key for the hostname entry, shown under the “#”header

Note: Only the root user can perform this step.

40

CAUTION
CM connectivity is InSv.
Changing the current values may cause loss of connectivity to the CM.

The system displays a message prompting you to confirm your request.

41 Confirm your request:

> yes

42 Compare the CM IP address from step 32 to the CM IP address from step 35.

If the values are	Do
identical	step 44
not identical	step 43

43 Enter the CM IP address from step 32 (include dots; example 47.105.155.6) and press the **Enter** key.

Example response:

```
CM IP address: 47.105.155.6
```

44 Press the **Enter** key.

45 Compare the SDM IP address from step 29 to the SDM CM-side IP address from step 35.

If the values are	Do
identical	step 47
not identical	step 46

46 Enter the SDM CM-side IP address from step 32 (include dots; example 47.105.155.6) and press the Enter key.

47 Press the Enter key again.

48 Determine if the displayed values are correct.

If the values are	Do
incorrect	step 49
correct	step 51

49 At the local or remote VT100 console, edit the values:

> e

50 Go to step 42.

51 Save the change and exit the change editor:

> y

Example response:

```
Change CM Connectivity command initiated.
Please wait ...
```

At the MAP display

52 At the SDM level return the core manager to service:

```
> rts
```

Example response:

```
SDM RTS initiated.

SDM RTS completed.
```

53 Go to step 95

At the local or remote VT100 console

54 Contact your LAN network administrator to determine whether the communications problem is external to the core manager.

If external to the core manager, the problem could be due to other issues on the operating company LAN, such as the LAN host being out of service.

If the fault is	Do
not on the operating company LAN	step 55
on the operating company LAN	you have completed this procedure

55 Log into the core manager as a maint class user or root user, and access the maintenance interface:

```
# sdmmtc
```

56 Access the NET level:

```
> net
```

Example response:

```
#
Description     Host      Address         State
1 Telco's Node    bmerha83  47.208.12.237  SysB
2 OSS             sandbox   47.207.22.121  .
3
4
```

57 Determine if the IP address shown for the affected LAN hostname is correct.

If the IP address is	Do
incorrect	step 39
correct	contact your next level of support

58 Access the change editor:

> change <hostname_key>

where

<hostname_key>
is the numeric key for the hostname entry, shown under the "#" header

59 Each editable parameter is displayed in turn. Keep pressing the **Enter** key until the IP address is displayed.

60 Enter the correct IP address for the LAN node.

Example response:

```
Values to be changed for LAN Node 1:
   LAN Node Description: Telco's Node
   LAN Node Hostname:  bmerha83
   LAN Node IP Address:   47.208.12.237
```

61 Determine if the displayed values are correct.

If the displayed values are	Do
correct	step 62
incorrect	step 64

62 Save the change and exit the change editor:

> y

Note: The node state changes to InSv within 2 min.

63 Go to step 95.

64 Edit the values:

> e

65 Go to step 40.

At the local or remote VT100 console

66 Obtain fault status information from the core manager:

```
> querysdm flt
```

67 From the fault status response, determine the affected device type and its state.

If the device state is	Do
ManB	step 68
Fail	step 72

68 Determine from office records or other personnel why the device was manually removed from service. When permissible, return the device to service.

At the MAP display

69 Access the Platform level under the SDM level.

70 Return the device to service:

```
> rts <domain_no> <device>
```

where

<domain_no>
is the domain number (0 or 1) of the device that you are returning to service

<device>
is hardware device name that you are returning to service.

Example response:

```
Hardware RTS : Domain 0 Device ETH - Command
initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message, and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Example Response:

```
Hardware RTS : Domain 0 Device ETH - Command
submitted.
```

71 Go to step 95.

72 Determine if the QuerySDM FLT response indicates an interconnect module (ICM) failure.

If an ICM failure is	Do
indicated	step 73
not indicated	step 80

73 Have qualified power maintenance personnel verify that power is available from the MSP to the failed ICM.

If	Do
the ICM has failed due to interruption of its power feed	step 74
the ICM power feed is OK	step 87

Note: If the core manager loses one -48V dc power feed, it continues to provide service using the other power feed. The loss of one feed removes one input/output (I/O) domain from service.

On the affected modules, the module in-service LEDs are off, and the out-of-service LEDs are on. These modules cannot be returned to service until power is restored.

At the MAP display

74 From the SDM level, enter the Platform level.

75 Have qualified power maintenance personnel restore the power feed to the ICM.

76 Access the hardware level of the RMI:

```
> hw
```

77 Return the main chassis ICM (that has failed due to loss of power) to service:

```
> rts <domain> icm
```

where

<domain>
is the I/O domain where the ICM is located (0 or 1)

Example response:

```
Hardware RTS : Domain 0 Device ICM1 - Command
initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”.

```
Hardware RTS: Domain 0 Device ICM1 - Command
submitted.
```

Note 1: The out-of-service ICM can be identified by an “F” under its header on the RMI display. It can also be visually identified at the back of the core manager by its in-service LED off, and its out-of-service LED on.

Note 2: After the ICM returns to service, the system automatically returns all the subtending nodes in its I/O domain to service. When each affected I/O controller module has returned to service, it begins to reintegrate with its corresponding I/O controller module in the other I/O domain. During this period, the System In Service light flashes.

The disk reintegration period for each affected I/O controller module lasts about 30 minutes. The actual amount of time depends on the amount of data stored on the disks, and the current processor load.

78 Upon completion of the disk reintegration, check the MAP MTC alarm banner for SDM-related alarms. Use the alarm clearing procedures in this document to clear any remaining faults.

79 Go to step 95.

80 Determine the fault in the core manager from the QuerySDM FLT response.

If	Do
one of the CPUs shows Fail	step 81
the Ethernet device is the only faulty device on an MFIO (usually indicates a cable fault)	step 84
a fan is faulty	step 87
a disk is faulty	step 87
a dat is faulty	step 87
a DS512 card is faulty	step 89

At the MAP display

81 Access the hardware level of the RMI:

```
> hw
```

82 Return the out-of-service CPU to service and start CPU reintegration:

```
> rts <domain> cpu
```

where

domain
is the domain where the CPU is located (0 or 1)

Note: The domain is:

- 0 if the CPU controller module is in slots 6 and 7, and
- 1 if it is in slots 10 and 11 of the main chassis.

Example response

```
Hardware RTS : Domain 0 Device CPU - Command
initiated.
Hardware RTS: Domain 0 Device CPU - Command
submitted.
```

Note: At the Platform menu level of the MAP, the CPU state changes to “S”, indicating that the CPUs are reintegrating. The reintegration process takes about 3 minutes to complete. The actual time depends on the processor load.

When reintegration is complete, the CPU status changes to in-service, indicated by a dot (. f).

83 Determine the success of the return to service.

If the action is	Do
successful	you have completed this procedure
not successful	step 87

At the local or remote VT100 console

84 From the QuerySDM FLT response, determine which cable is affected and its location.

By physical inspection, determine if the cable has been disconnected or physically damaged.

If a cable	Do
requires reconnection or repair	step 85
appears undamaged and correctly connected	contact your next level of support

85 Reconnect, repair, or replace the cable as appropriate.

Note: If this is not successful, replace the MFIO.

86 Go to step 95

87 Replace the failed device using the appropriate hardware replacement procedure.

88 Go to step 95.

89 From the QuerySDM FLT response, determine which of the DS512 cards have been affected.

Example response:

```
SDM 309 Hardware device out of service
Device : 512 (1)
Device State : Fail
Suspected Module : DS512 personality module (PEC
NTRX50GH)
Location : Shelf : SDMM, Slot 12, Back
Other Devices on module : none
Fault Category : Fault on personality module
Reason : Personality Module cable fault.
```

Note: The above example points to a fault on the personality module, located in slot 12, at the back of the system.

If the response indicates the	Do
DS512 personality module	step 93
DS512 controller module	step 90

90 Check the LEDs on the affected card.

If the LEDs are	Do
on	step 92
off	step 91

91 Reseat the card.

At the MAP display

92 Try to bring the card back into service:

> rts <domain_no> 512

where

<domain_no>
is either 0 or 1

If the system	Do
recovers	you have completed this procedure
does not recover	step 94

93 Inspect the fibres and replace if necessary.

Note: Wait at least 5 minutes for the system to recover.

If the system	Do
recovers	you have completed this procedure
does not recover	step 94

94 Replace the affected card using the appropriate hardware replacement procedure.

95 You have completed this procedure.

Clearing a BAK50 alarm

Purpose

Use this procedure to clear a BAK50 alarm.

Indication

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

Meaning

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

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

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

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

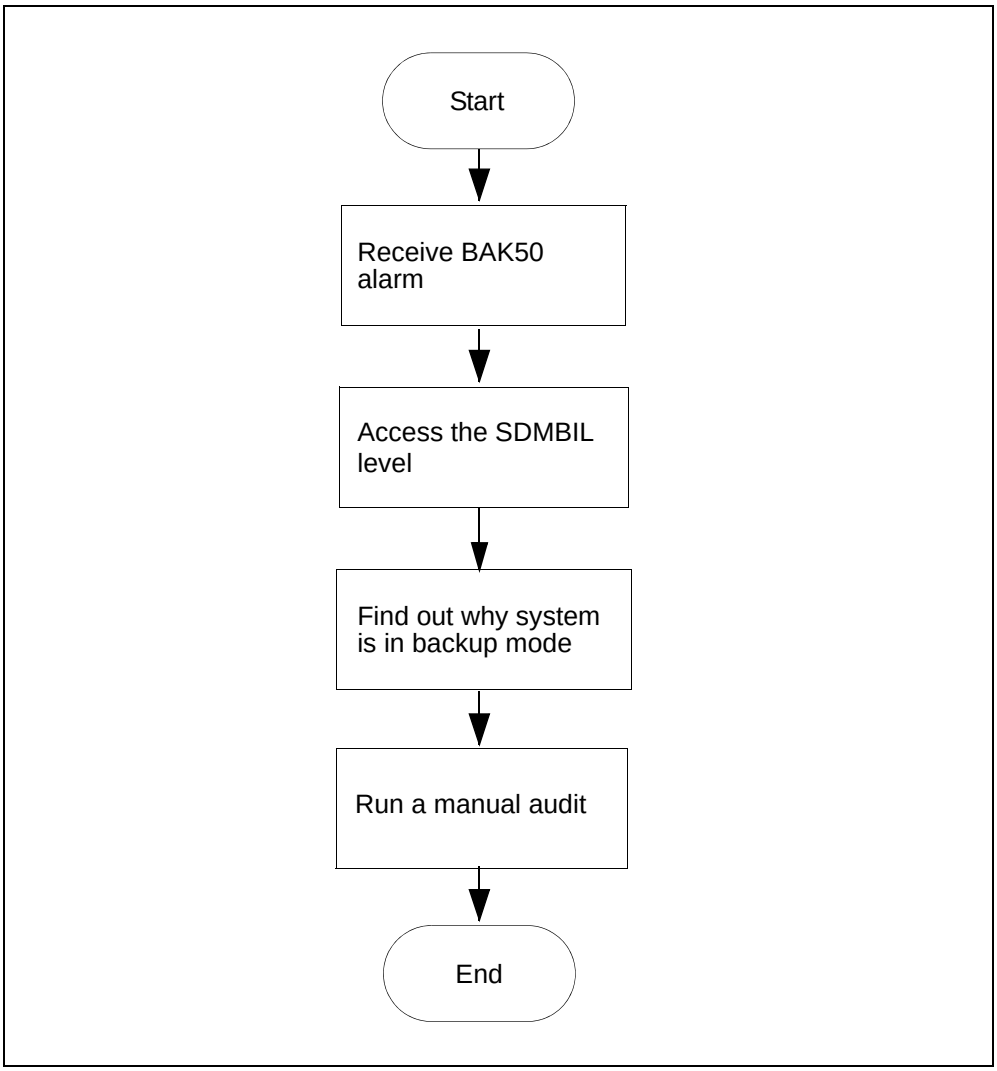
Impact

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

Procedure

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

BAK50 alarm clearing flowchart



Clearing a BAK50 alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all of the alarms that have been raised:

```
> DispAL
```

4 Determine the billing stream status.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then return to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12

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

12 You have completed this procedure.

Clearing a BAK70 alarm

Purpose

Use this procedure to clear a BAK70 alarm.

Indication

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

Meaning

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

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

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

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

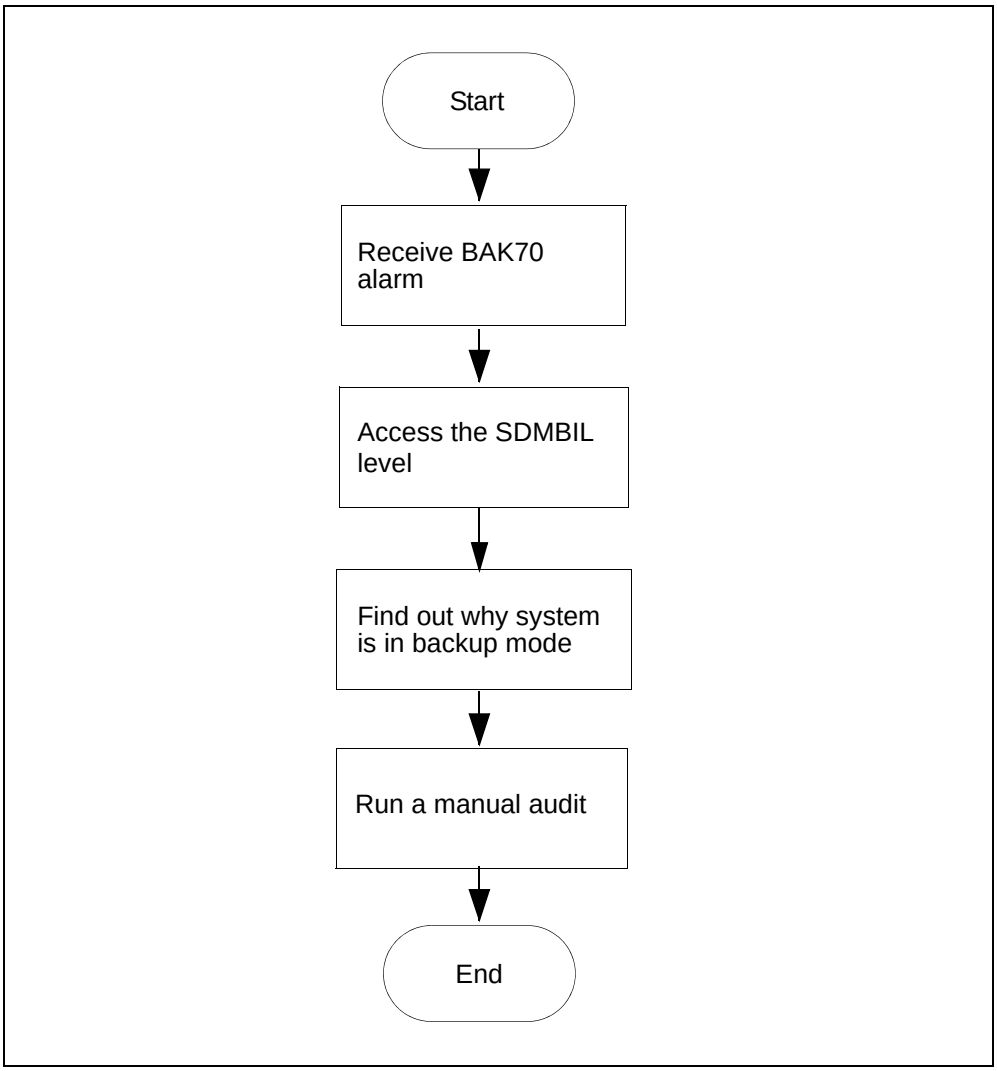
Impact

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

Procedure

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

BAK70 alarm clearing flowchart



Clearing a BAK70 alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all of the alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then return to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12

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

12 You have completed this procedure.

Clearing a BAK90 alarm

Purpose

Use this procedure to clear a BAK90 alarm.

Indication

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

Meaning

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

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

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

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

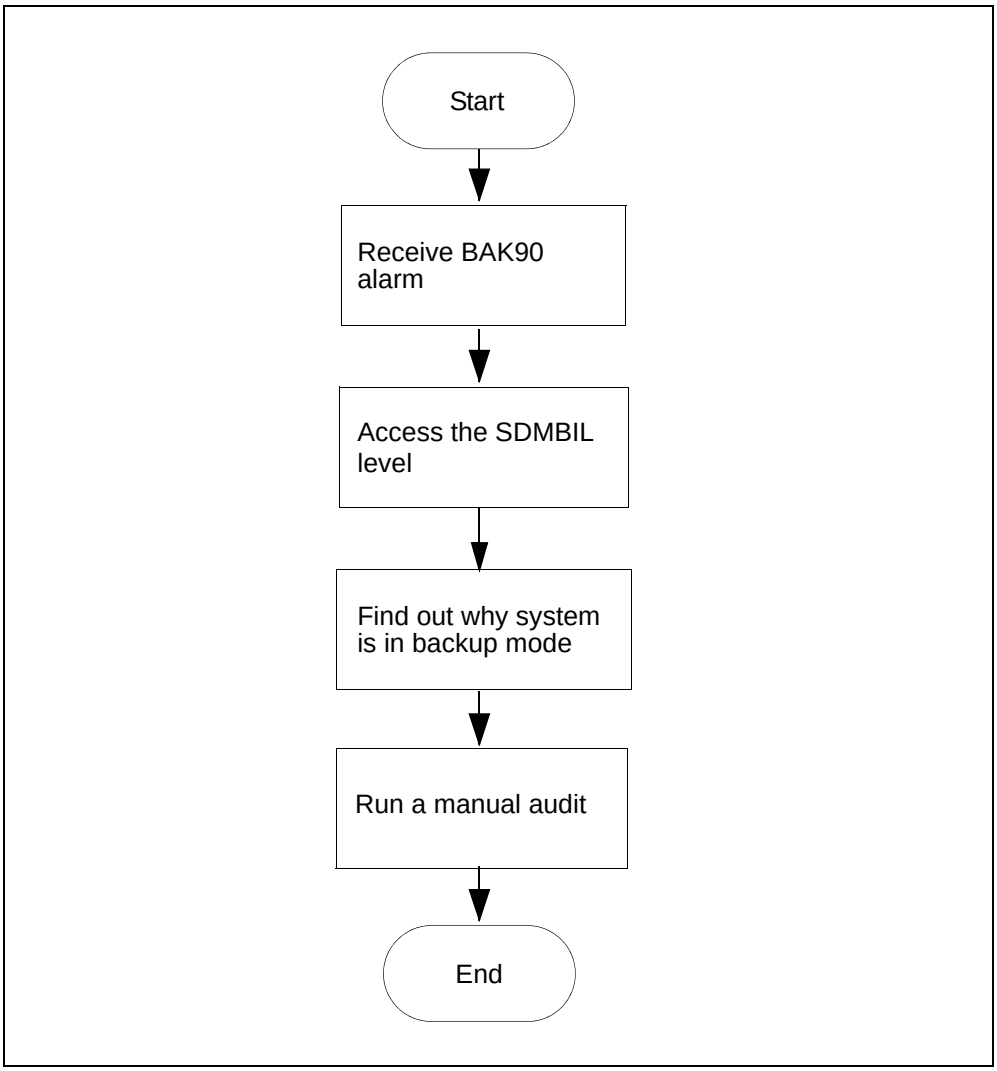
Impact

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

Procedure

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

BAK90 alarm clearing flowchart



Clearing a BAK90 alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then return to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12

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

12 You have completed this procedure.

Clearing a BAKUP alarm

Purpose

Use this procedure to clear a BAKUP alarm.

Indication

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

Meaning

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

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

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

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

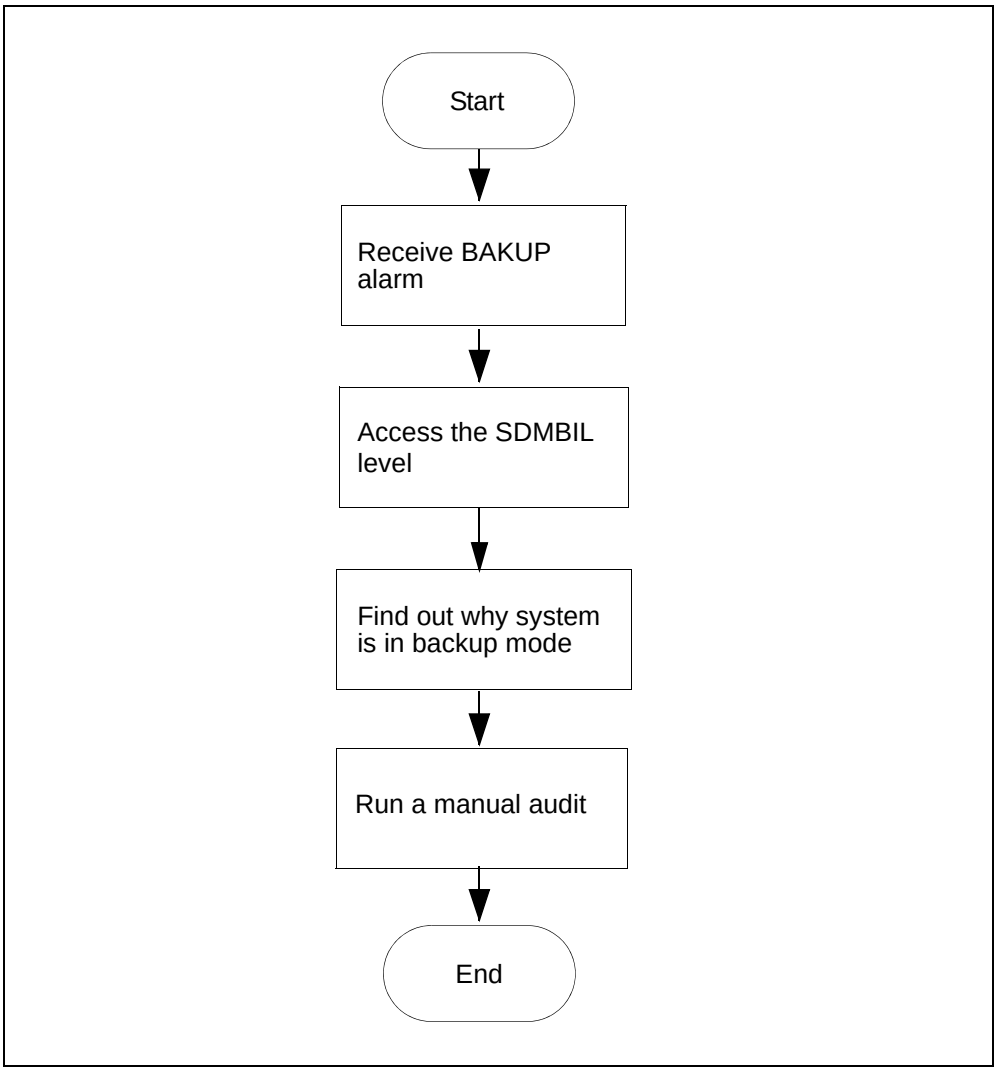
Impact

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

Procedure

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

BAKUP alarm clearing flowchart



Clearing a BAKUP alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then return to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then return to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12

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

12 You have completed this procedure.

Clearing a 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 Determine the value of the active template ID on the DMS/CM:

```
> CTMPLT “template all”
```

2 Set the CurrentTmpltID mib parameter to match the value of the active template ID:

```
> mib cdr set CurrentTmpltID <template_ID>
```

where

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

3 If you change the CurrentTmpltID MIB parameter after you have turned on the stream, you must BSY and then `rts` the SBA application to activate the change.

4 If the alarm persists, contact your next level of support.

Clearing a DSKWR alarm

Purpose

Use this procedure to clear a disk write (DSKWR) alarm.

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 core manager disk because the disk is unavailable, or the disk is full.

The core manager generates the SDMB355 log report when this alarm is raised.

Impact

The DMS/CM cannot send the billing records to the core manager. As a result, the DMS/CM sends the billing records to backup storage.

However, backup storage is limited. As the backup storage becomes filled, alarms notify you as to how much of its capacity is used.

Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

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

Action

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:

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

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

```
dispal
```

3 Determine if the NOBAK or NOSTOR alarms appear.

If the NOBAK or NOSTOR alarm	Do
appears in the alarm banner	perform the procedure • “Configuring SLM disk backup volumes”, and • (if necessary) “Configuring DDU disk backup volumes” in the Accounting document
does not appear in the alarm banner	step 4

4 Log in to the core manager as a user authorized to perform fault-admin actions.

5 Access the maintenance level:

```
sdmmtc
```

6 Access the hardware level:

```
hw
```

7 Determine the status of DSK1 and DSK2.

If DSK1 or DSK2 is	Then
InSv (represented by a dot [.])	the disk hardware is in service (InSv) and you are still receiving an alarm; go to step 10
not InSv	the disk hardware is not in service (ISTb); continue with step 8

8 Return DSK1 and/or DSK2 to service:

```
rts <domain> <device>
```

where

<domain> is the domain (0 or 1) in which the disk that is not in service resides
<device> is the device name listed at the HW level

Each DSK must be returned to service separately.

Example command:

```
rts 0 dsk2
```

Note: A DSKWR alarm is not received if only one disk is in service.

9 Determine the status of the alarm.

If the alarm	Do
clears	you have completed this procedure
does not clear	step 10

10 Access the storage level to display the storage usage:

```
storage
```

The following information is displayed:

- total size of the disk storage
- percentage of the disk storage that is being used
- threshold percentage that is set for the storage capacity

Note 1: The information helps you to determine if the logical volume assigned to the billing stream is full. The logical volume can be full if you do not send the primary files downstream or to tape.

Note 2: You can prevent a full logical volume condition by sending the billing files to the downstream processor, or by writing them to tape. However, prior to sending the billing files, first determine if you have received an FTPW critical alarm.

11 Quit the SDMMTC interface:

```
quit all
```

12 Access the BILLMTC interface:

```
billmtc
```

13 Access the FILESYS level:

```
filesys
```

14 Send the primary billing files to the downstream processor:

```
sendfile <stream_name>
```

where:

<stream_name> is the name of the stream.

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

15 Determine the SENDFILE results.

If the SENDFILE command	Do
is not successful	refer to procedures Verifying the file transfer protocol on page 402 and Verifying the FTP Schedule on page 409 in this document, then return to this procedure and repeat step 14
is successful	step 16
is not successful after you reference the procedures	contact your next level of support

16 Quit the BILLMTC interface:

```
quit all
```

17 At the AIX prompt, check for orphan files and for files that someone else has copied to the logical volume of your billing stream:

`cd/sba/<stream_name>/orphan`

where:

<stream_name> 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 of 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 experiencing a problem	step 18

18 Verify the write permission and ownership for the directories in /sba/<billing_stream>.

19 Determine the directory permissions.

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 20
ownership for a directory is not maint	step 21
the alarm fails to clear	contact your next level of support

20 Change the permissions for a directory:

`chmod 755 <directory>`

where:

<directory> is the directory in which you are changing permissions

21 Change the ownership of a directory:

`chown maint <directory>`

where:

<directory> is the directory in which you are changing ownership

22 You have completed this procedure.

Clearing an EXT FSP major alarm

Purpose

Use this procedure to clear an EXT FSP major MAP alarm that has been triggered by the CS 2000 Core Manager.

Application

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

This procedure assumes that you have isolated the CS 2000 Core Manager as the cause of the EXT FSP alarm. To clear an FSP alarm generated by equipment other than the CS 2000 Core Manager, use the EXT FSP alarm clearing procedure in the generic alarm clearing documentation for your DMS switch.

Indication

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

Meaning

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

An EXT FSP alarm triggered by the CS 2000 Core Manager means that one of the following faults has occurred:

- Input power (-48 dc) to the CS 2000 Core Manager has failed.
- The CS 2000 Core Manager has reached its maximum allowable operating temperature threshold.
- The CS 2000 Core Manager power supply has failed.

Input power failure

The status of the input power is shown by the Input Power LED on the NTRX41AA alarm card in the modular supervisory panel (MSP) at the top of the CS 2000 Core Manager cabinet. See the figure MSP LEDs at the top of the CS 2000 Core Manager cabinet on page 336.

This LED is normally on (green), but if it is off, there is no input power to the CS 2000 Core Manager.

Maximum temperature threshold reached

The status of the operating temperature is shown by the Thermal Fail LED on the NTRX41AA alarm card in the modular supervisory panel (MSP) at the top of the CS 2000 Core Manager cabinet. See the figure MSP LEDs at the top of the CS 2000 Core Manager cabinet on page 336.

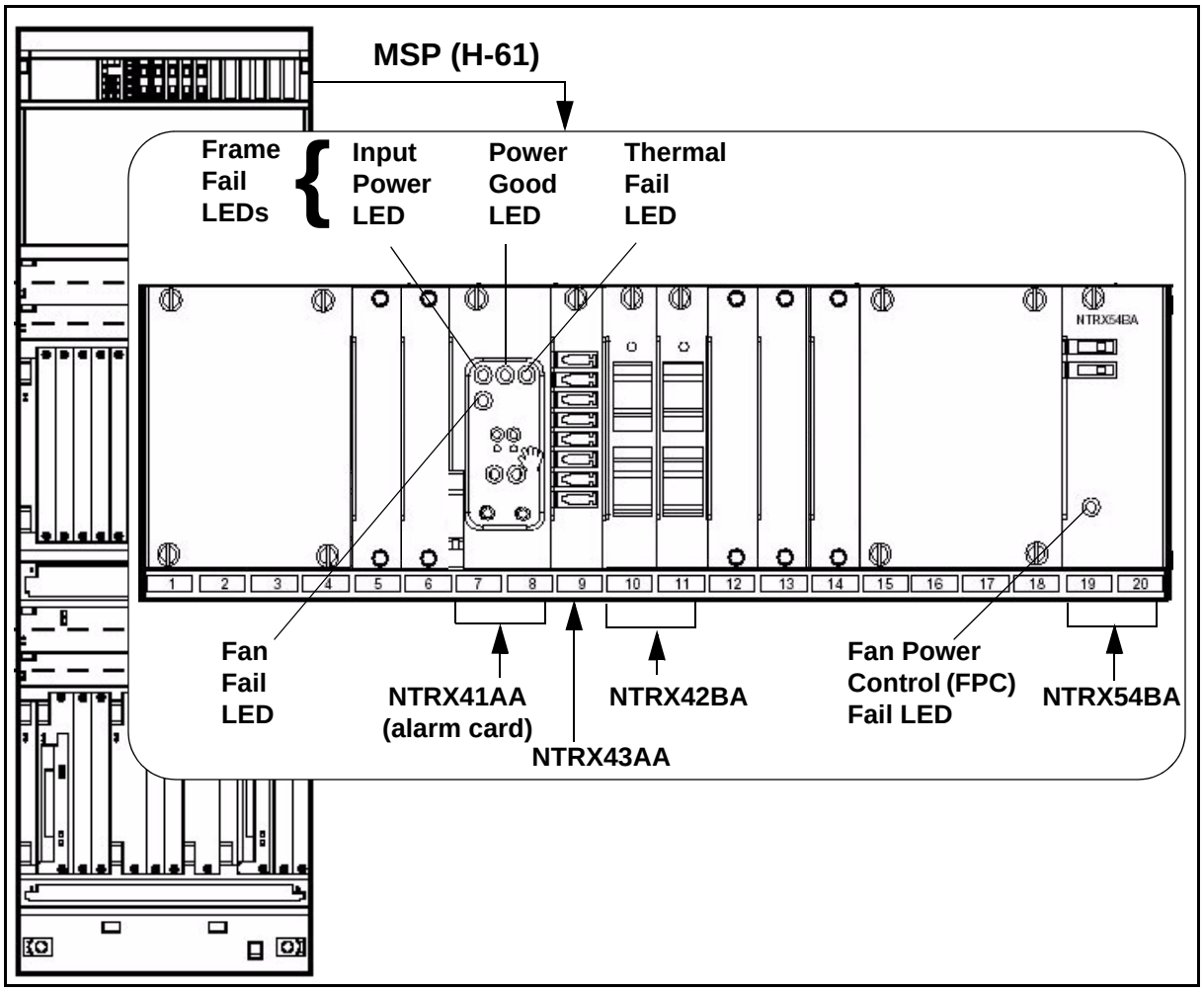
This LED is normally off, but if it is on (yellow), the thermal threshold has been reached and the CS 2000 Core Manager automatically shuts down.

Power supply failure

The status of the output power is shown by the Power Good LED on the NTRX41AA alarm card in the modular supervisory panel (MSP) at the top of the CS 2000 Core Manager cabinet. See the figure MSP LEDs at the top of the CS 2000 Core Manager cabinet on page 336.

This LED is normally on (green), but if it is off, there is no output power from the CS 2000 Core Manager power supply.

MSP LEDs at the top of the CS 2000 Core Manager cabinet



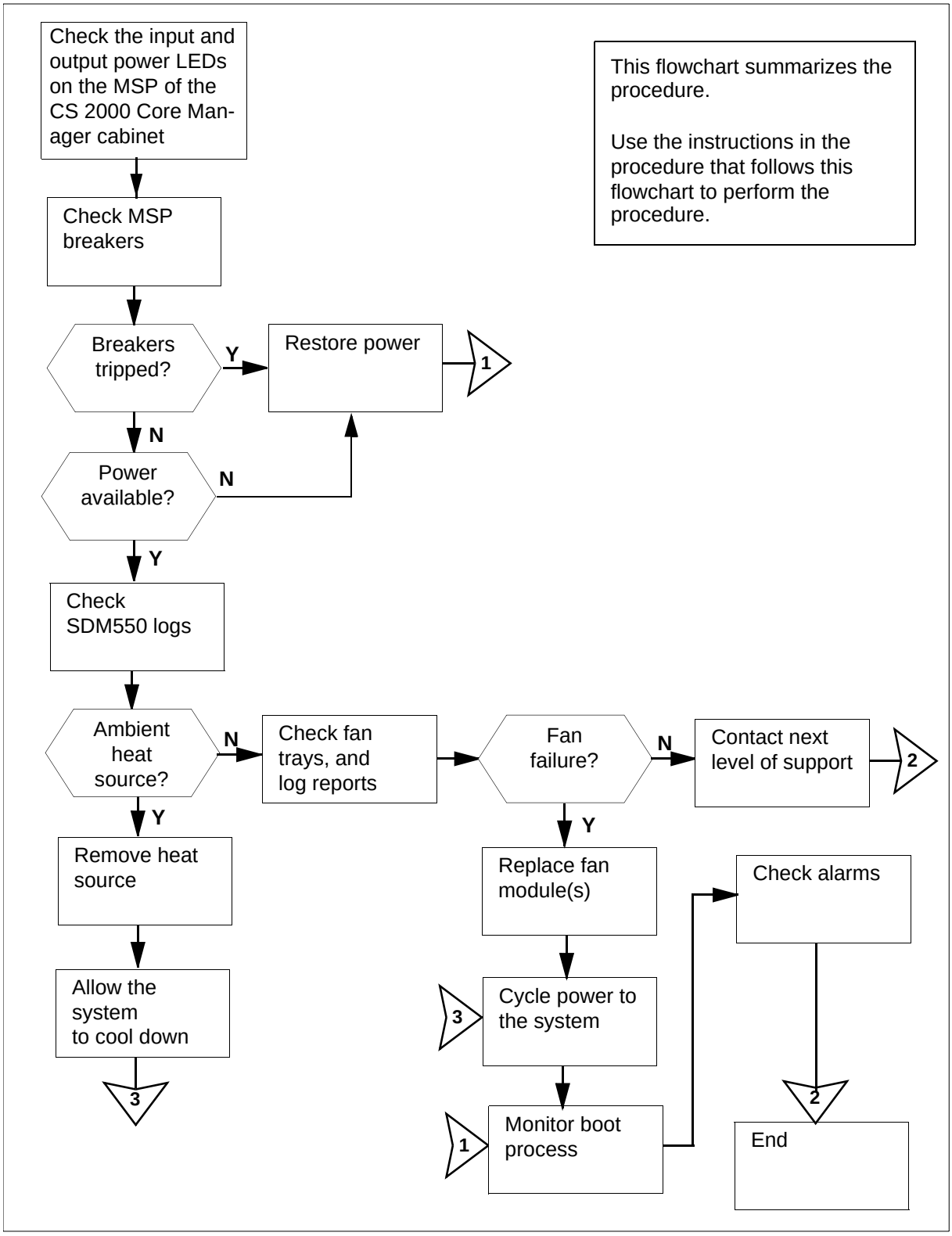
Impact

The CS 2000 Core Manager is out of service and no applications can run.

Action

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

Summary of clearing an Ext FSP major alarm



Clearing an Ext FSP major alarm

At the MSP

1 Check the Input Power LED on the MSP at the top of the CS 2000 Core Manager cabinet.

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

2 The -48 V dc supply to the CS 2000 Core Manager is faulty. Have qualified power maintenance personnel restore input power to the CS 2000 Core Manager. Contact Nortel Networks for assistance if required.

When power is restored, continue this procedure at step 23.

3 Check the power supply output (Power Good) LED on the MSP at the top of the CS 2000 Core Manager cabinet.

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

4 Check the modular supervisory panel (MSP) breakers that supply -48V dc power to the CS 2000 Core Manager.

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

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

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

When power is restored, continue this procedure at step 23.

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

7 Determine the state of the system.

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

8 Have qualified power maintenance personnel determine if power is available from the MSP to the CS 2000 Core Manager.

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

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

When power has been restored, continue this procedure at step 23.

10 Check the Thermal Fail LED on the MSP at the top of the CS 2000 Core Manager cabinet.

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

At the MAP display

11 The CS 2000 Core Manager has shut down due to thermal failure (overheating). Verify this by checking for recent SDM550 logs. If the CS 2000 Core Manager shut down is due to thermal failure, two logs were generated.

- SDM550 log was generated when the CS 2000 Core Manager reached its thermal warning threshold (60× C or 140× F)
- SDM550 log was generated to indicate that shutdown will occur in 1 minute because its shutdown thermal threshold has been reached (80 degrees C or 176 degrees F)

At the C28B cabinet containing the CS 2000 Core Manager

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

Note: Thermal shutdown can result from high ambient air temperature in the vicinity of the CS 2000 Core Manager, or excessive heat from an adjacent frame, or a combination of these factors.

If	Do
ambient air temperature is high	step 20
the high temperature is in the vicinity of the CS 2000 Core Manager	step 13

At the front of the CS 2000 Core Manager

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

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

At the local VT100 console

14 Check for recent CS 2000 Core Manager-related PM128 logs indicating failure of one or both fan tray units.

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

15 Ensure that the local VT100 console is connected to the CS 2000 Core Manager with the designated cable, and that the VT100 console is operational.

At the MSP

16 At the MSP, cycle power to the CS 2000 Core Manager by turning the MSP breakers (located at the front of the MSP) off

and on. The MSP breakers supply power to the CS 2000 Core Manager. Proceed according to the chassis in your system.

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

At the local VT100 console

17 The CS 2000 Core Manager begins to reboot. Monitor the boot process. When you see the following prompt,

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

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

The FX-Bug prompt is then displayed.

At the front of the CS 2000 Core Manager

18 Check the operation of the three fans in each fan tray module by:

- unseating the fan module
- physically verifying that the fan blades in each fan are rotating, and
- reseating the fan module

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

19 Replace the faulty fan module(s), and then continue this procedure at step 22.

At the C28B cabinet containing the CS 2000 Core Manager

20 Remove or eliminate the heat source that caused the thermal shutdown.

21 Allow the CS 2000 Core Manager to cool below its thermal shutdown warning threshold
(60 degrees C or 140 degrees F).

At the MSP

22 Cycle power to the CS 2000 Core Manager by turning both MSP breakers, located at the front of the MSP, off and on. The MSP breakers supply power to the CS 2000 Core Manager. Proceed according to the chassis in your system.

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

At the CS 2000 Core Manager

23 When power is restored, the CS 2000 Core Manager automatically reboots and returns to service. Monitor the system progress as follows:

- critical alarm LED shows red
- component Out-of-Service LED flashes
- component Out-of-Service LED turns solid
- LEDs on the various service modules show green as they go into service
- critical alarm LED and the Component Out-of-Service LED turn off: the System in Service LED and the CPU1 service module LED flash
- System-in-Service LED and the CPU1 service module LED are solid green indicating completion of the reboot
- all LEDs on the MSP are off

At the MAP display

24 When disk reintegration is complete, check the APPL alarm banner for CS 2000 Core Manager-related alarms. Use the alarm clearing procedures in this document to clear any faults.

25 You have completed this procedure.

Clearing a FREE SPACE alarm

Purpose

Use this procedure to clear a disk Free Space alarm.

Indication

At the storage level of the SuperNode Data Manager (SDM) maintenance tool sdmmtc, an exclamation symbol (*!*) at the end of a volume group entry indicates an alarm for the free space when the volume group is not performing re-integration.

Meaning

A minor alarm is raised if the remaining free space for a volume group is less than the free space threshold. The default threshold value is 400 Mbytes.

Impact

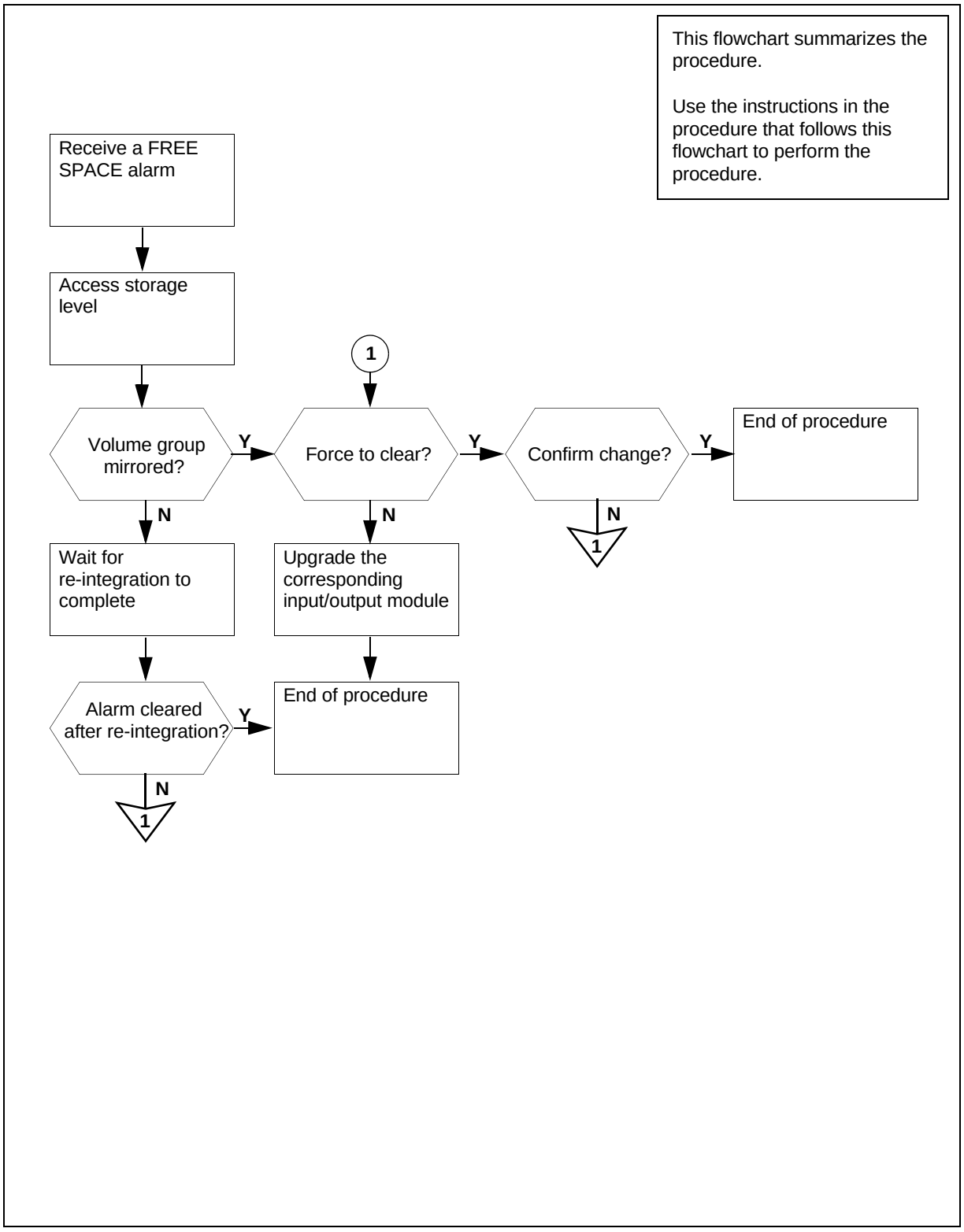
The free space for a volume group is lower than the default threshold, which can cause problems during upgrade.

Action

ATTENTION
Do not attempt to clear a free space alarm when the volume group is performing re-integration.

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

FREE SPACE alarm clearing flowchart



Clearing a FREE SPACE alarm

At the maintenance interface

1 Access the storage level:

```
> sdmmtc storage
```

If the state is	Do
not mirrored	step 2
mirrored	step 3

2 Wait until the re-integration is complete, determine the alarm state.

Is the alarm	Do
not cleared after re-integration	step 3
cleared after re-integration	step 7

3 Determine the alarm clearance method required.

Is the alarm cleared	Do
normally	step 4
by force to clear	step 5

4 Determine the alarm source.

If the alarm is for	Do
rootvg	procedure “Upgrading the rootvg MFIO to MFIO or to UMFIO” in the CS 2000 Core ManagerUpgrades document to add more space to rootvg
datavg	procedure *“Upgrading a datavg MFIO to MFIO or to UMFIO”* in the CS 2000 Core ManagerUpgrades document to add more space to datavg

5 Force to clear the alarm:

```
> change <volume_group_name> <new_threshold>
```

where:
<volume_group_name> is the real name of the volume group

that has the FREE SPACE alarm **<new_threshold>** value is either equal to or less than the current free space

6 The system displays a warning message that prompts you to confirm the change.

If your answer to confirm the change is	Do
no	step 3
yes	step 7

7 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

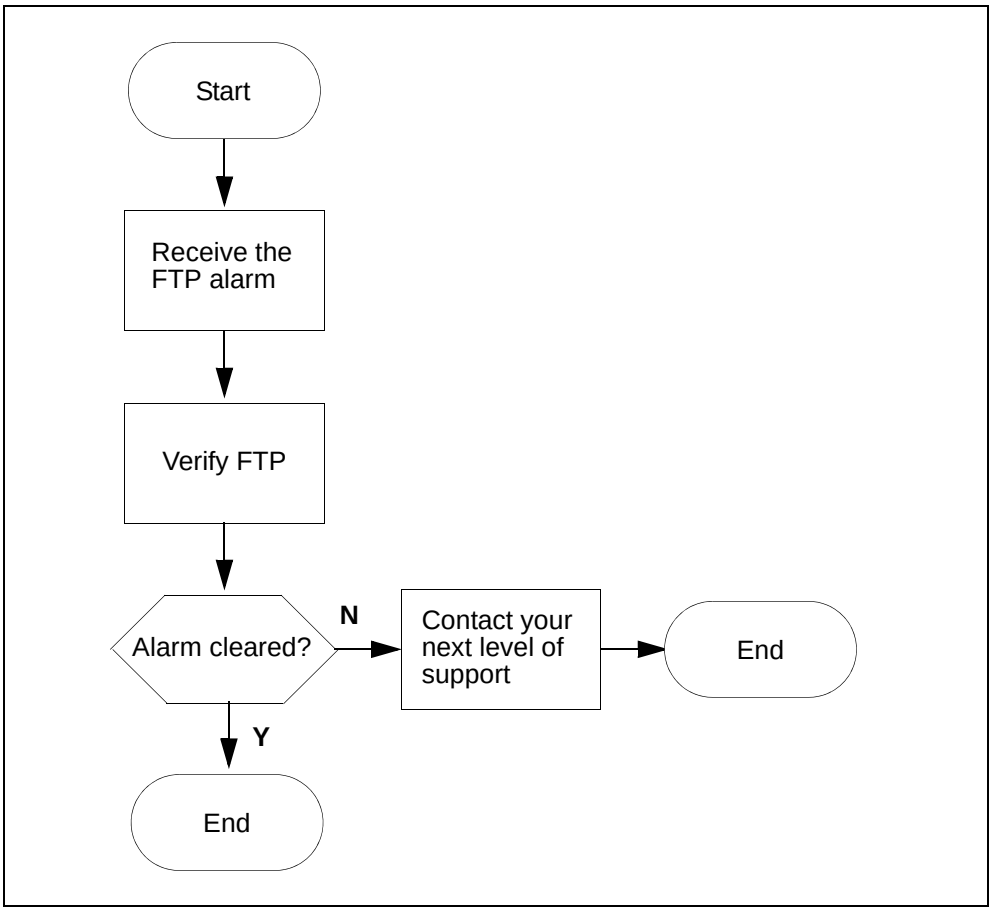
The core manager cannot FTP files to the downstream destination. It is possible that the core manager has reached its storage capacity limit, depending on the amount of storage and the volume of records.

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.

Procedure

The following flowchart provides 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 402 in this document.

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

4 You have completed this procedure.

Clearing an FTPW alarm

Purpose

Use this procedure to clear an FTPW alarm.

Indication

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

Meaning

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

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

Impact

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

Action

Clearing an FTPW alarm

At the core manager

1 Complete procedure Verifying the file transfer protocol on page 402 in this document.

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

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

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

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

4 You have completed this procedure.

Recovering from a half shelf down power failure

Purpose

Use this procedure to bring the X.25 link back into service following routine maintenance or a power failure.

Application

This procedure is only valid for a system configured with a single X.25 card.

Gather all related logs, reports, and system information for analysis to help ensure that the next level of maintenance and support can find the problem.

Action

To perform this procedure, refer to “Recovering from a half shelf down power failure” in *Lawful Intercept Product and Technology Fundamentals, Intl,* NN10194-113.

Clearing an inbound file transfer alarm

Purpose

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

Indication

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

Meaning

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

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

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

Impact

Inbound file transfer for the billing stream is not possible.

Action

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

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

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

Clearing an IFT alarm

At the MAP

1 Log in to the core manager as maint user.

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

2 Change the permissions of the /home/maint/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 402 for more information.

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

Meaning

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

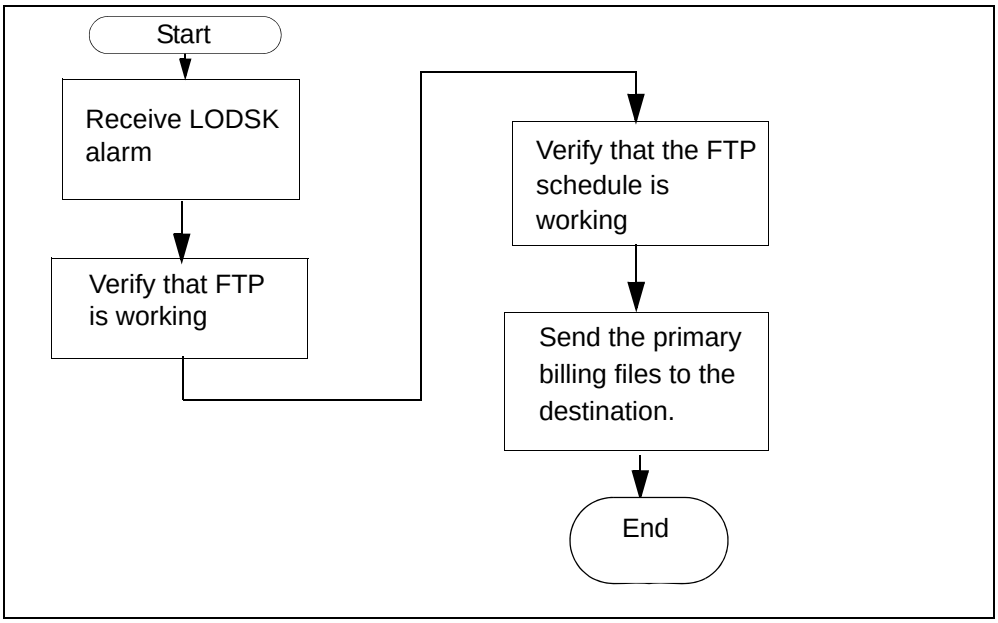
Impact

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

Action

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

LODSK alarm clearing flowchart



Clearing a LODSK alarm

At the MAP

1 Use the procedure Verifying the file transfer protocol on page 402 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 409
	if the alarm persists, contact your next level of support

Clearing a NOBAK alarm

Purpose

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

Indication

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

Meaning

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

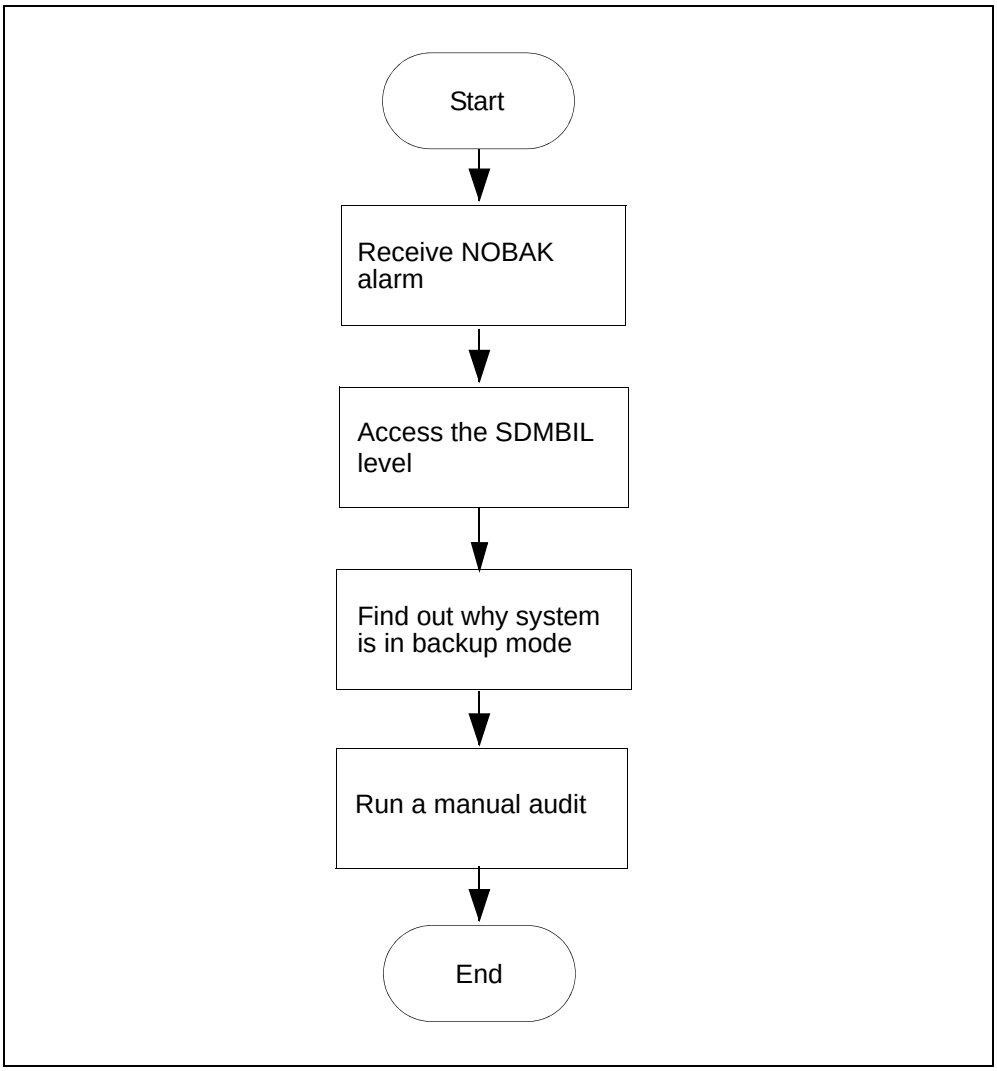
- `both`
  the alarm severity level is major
- `on`
  the alarm severity level is critical

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

Procedure

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

NOBAK alarm clearing flowchart



Clearing a NOBAK alarm

At the MAP

1 Post the billing stream:

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

where

<billing_stream> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then go to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then return to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12

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

12 You have completed this procedure.

Clearing a NOCLNT alarm

Purpose

Use this procedure to clear a NOCLNT alarm.

Indication

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

Meaning

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

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

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

Impact

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

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

Action

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

Clearing a NOCOM alarm

Purpose

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

Indication

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

Meaning

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

The most likely causes of this alarm are

- DS-512 links are not in-service making the core manager SysB
- core manager power is off, or
- core manager is rebooting

Impact

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

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

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

Procedure

At the core manager

1 Check for log SDMB375.

If the system	Do
generates log SDMB375	step 2

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

2 Access the billing maintenance level:

```
# billmtc
```

3 Access the schedule level:

```
> schedule
```

4 Access the real-time billing level:

```
> rtb
```

5 Busy the stream:

```
> bsy <stream_name>
```

where:

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

6 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

Adjusting disk space in response to SBA backup file system alarms

Purpose

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

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

Procedure

Adjusting disk space in response to SBA backup file system alarms

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream.

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

```
conf view <stream_name>
```

where

<stream_name> is the name of the billing stream.

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

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

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

where

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

4 Repeat step 3 for each volume name that you recorded in step 2, and then proceed to step 5.

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

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

where

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

6 Repeat step 5 for each volume name that you recorded in step 2.

If the volumes	Do
have enough disk space	step 7
do not have enough disk space	perform procedure “Configuring SBA backup volumes on the core” in the Accounting document for your core manager.

7 You have completed this procedure.

Clearing a NOFL alarm

Purpose

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

Indication

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

Meaning

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

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

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

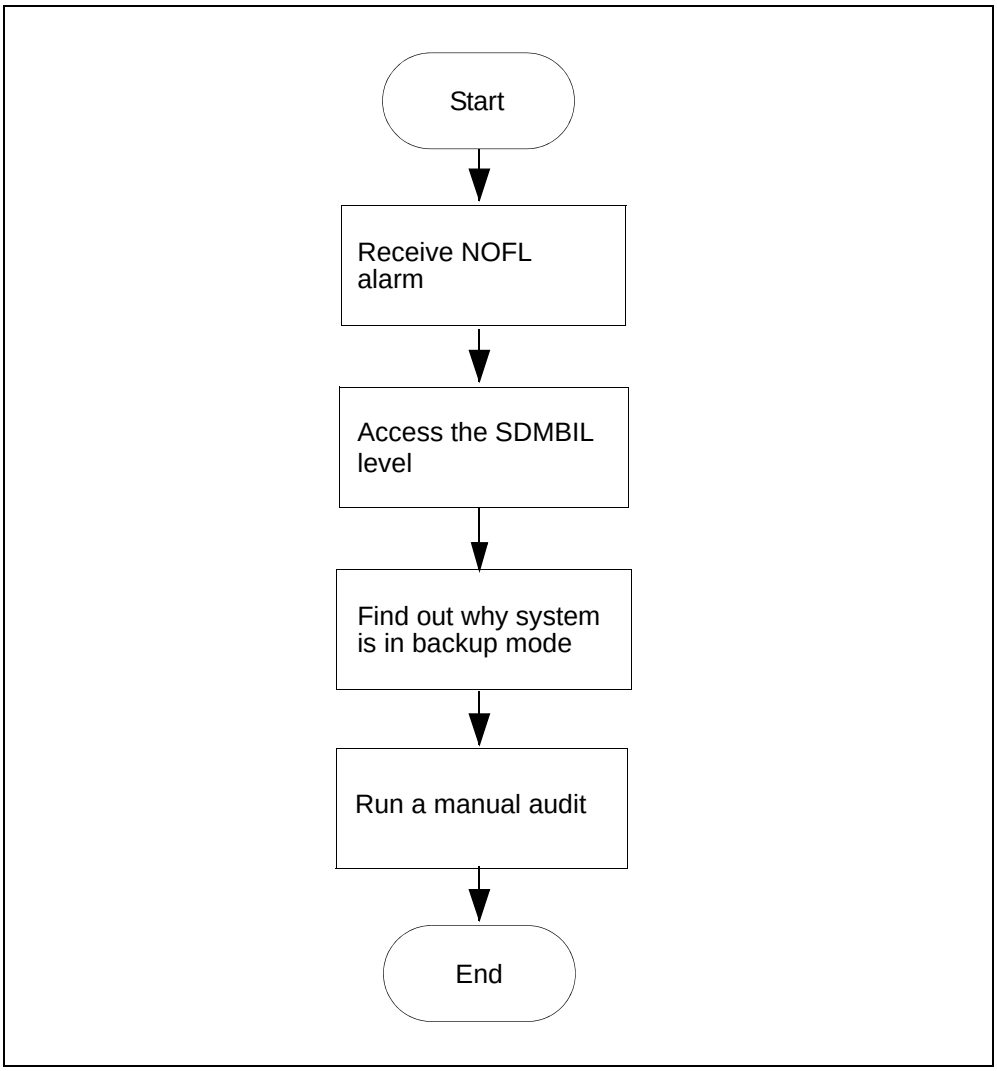
Impact

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

Procedure

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

NOFL alarm clearing flowchart



Clearing a NOFL alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream.

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
> DispAL
```

4 Determine the status of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then go to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then return to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
> post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

12 You have completed this procedure.

Clearing a NOREC alarm

Indication

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

Meaning

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

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

If the stream is set to if the stream is set to:

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

Impact

No backup files are recovered by the SBA system.

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

Action

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

Clearing an NOSC alarm

Indication

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

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

Meaning

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

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

Impact

The CDR2BAF conversion process does not create BAF records.

Action

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

Clearing a NOSTOR alarm

Purpose

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

Indication

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

Meaning

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

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

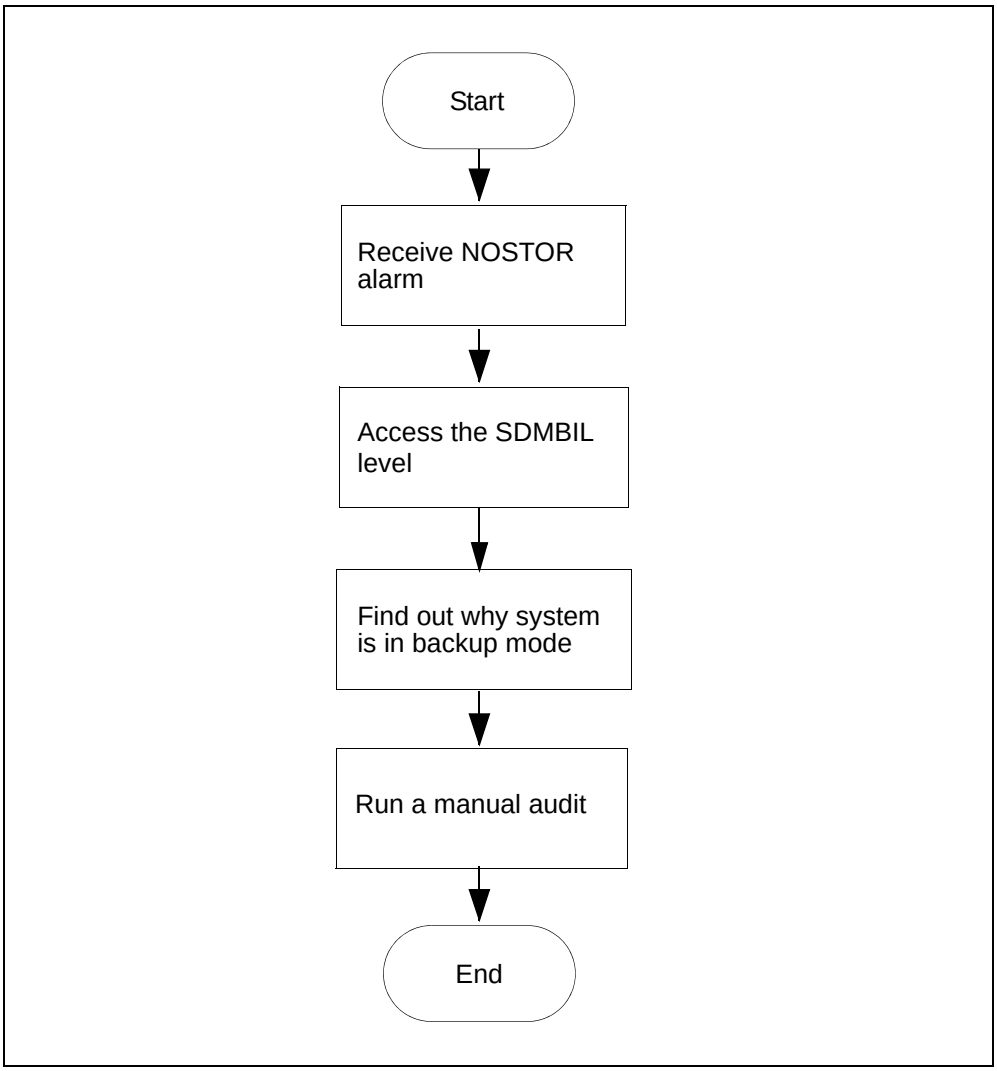
- `both`
  the alarm severity level is major
- `on`
  the alarm severity level is critical

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

Procedure

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

NOSTOR alarm clearing flowchart



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

Clearing a NOSTOR alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
DispAL
```

4 Determine the state of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then go to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then go to step 5.
ManB	RTS the billing stream
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

12 You have completed this procedure.

Clearing a NOVOL alarm

Purpose

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

Indication

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

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

Meaning

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

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

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

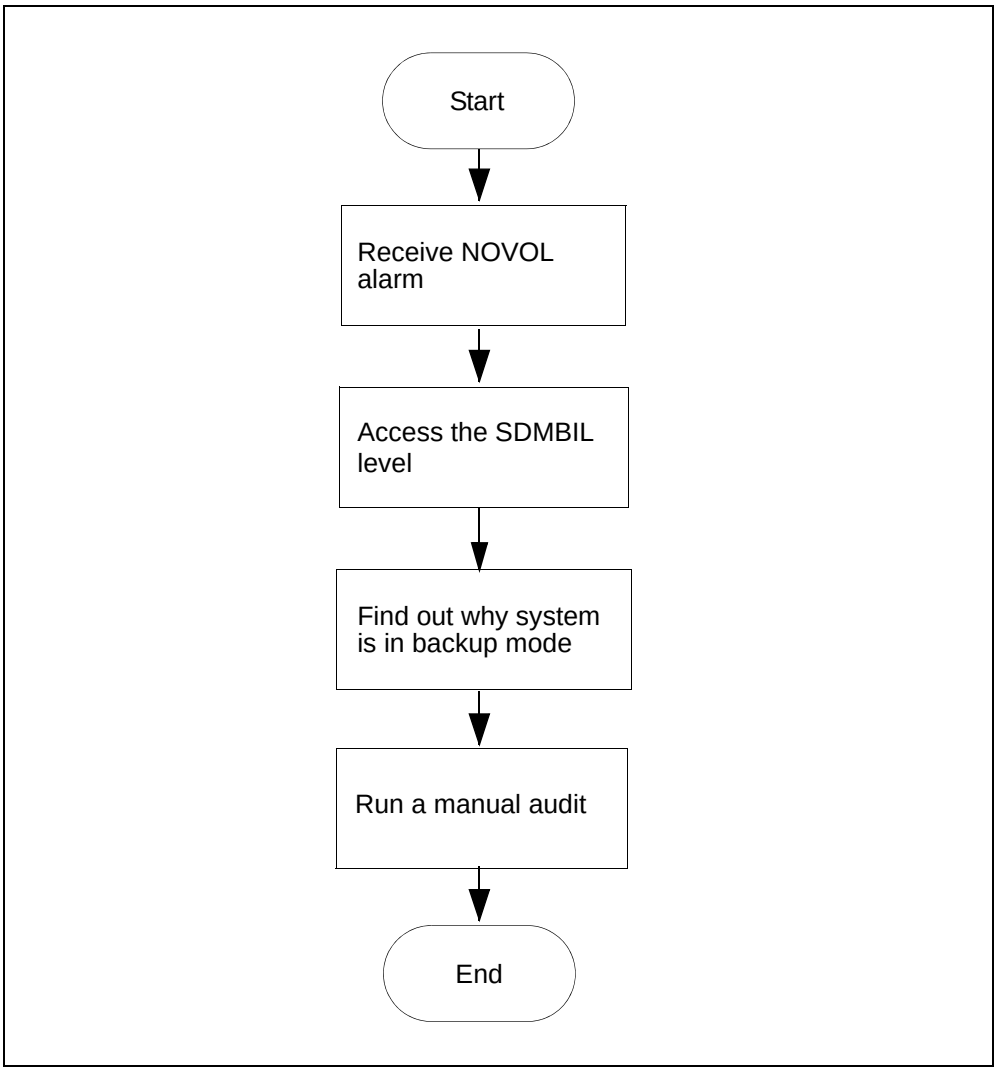
Impact

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

Procedure

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

NOVOL alarm clearing flowchart



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

Clearing a NOVOL alarm

At the MAP

1 Post the billing stream:

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

where

<stream_name> is the name of the billing stream

2 Determine why the system is in backup mode.

3 Display all alarms that have been raised:

```
DispAL
```

4 Determine the status of the billing stream.

If the billing stream is	Perform the following steps
SysB	perform the procedure for the alarm or the condition, and then go to step 5.
RBsy	refer to Clearing a major SBACP alarm on page 389, and then go to step 5.
ManB	Go to step 8
Bkup	Go to step 8

5 Use Audit to clear the alarm.

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

6 Ensure that the billing system is in recovery:

```
post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

8 Perform the procedure Adjusting disk space in response to SBA backup file system alarms on page 364

9 Use Audit to clear the alarm.

If the alarm	Do
cleared	step 10
did not clear	contact your next level of support

10 Ensure that the billing system is in recovery:

```
post <streamname>
```

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

If the billing system	Do
is in recovery (Rcvy)	step 12
is not in recovery	contact your next level of support

12 You have completed this procedure.

Clearing a PAGING SPACE alarm

Indication

At the storage level of the SuperNode Data Manager (SDM) maintenance tool sdmmtc, an exclamation symbol (*!*) at the end of the paging logical volume name indicates an alarm for the paging space available. The condition can appear only when the percentage full (*% full*) is within the logical volume threshold.

Note: When the percentage full exceeds the threshold, refer to the procedure "Changing logical volume thresholds" in the CS 2000 Core Manager Security and Administration document.

Meaning

A critical alarm indicates that the size of paging space configured on the SDM is less than 250 Mbytes. A major alarm indicates that the size of paging space configured on the CS 2000 Core Manager is between 250 Mbytes and the normal size.

Impact

If a problem occurs when the paging space is extended during a CPU upgrade, an alarm indicates the current and required sizes of paging space in the following format: *xx/yy*.

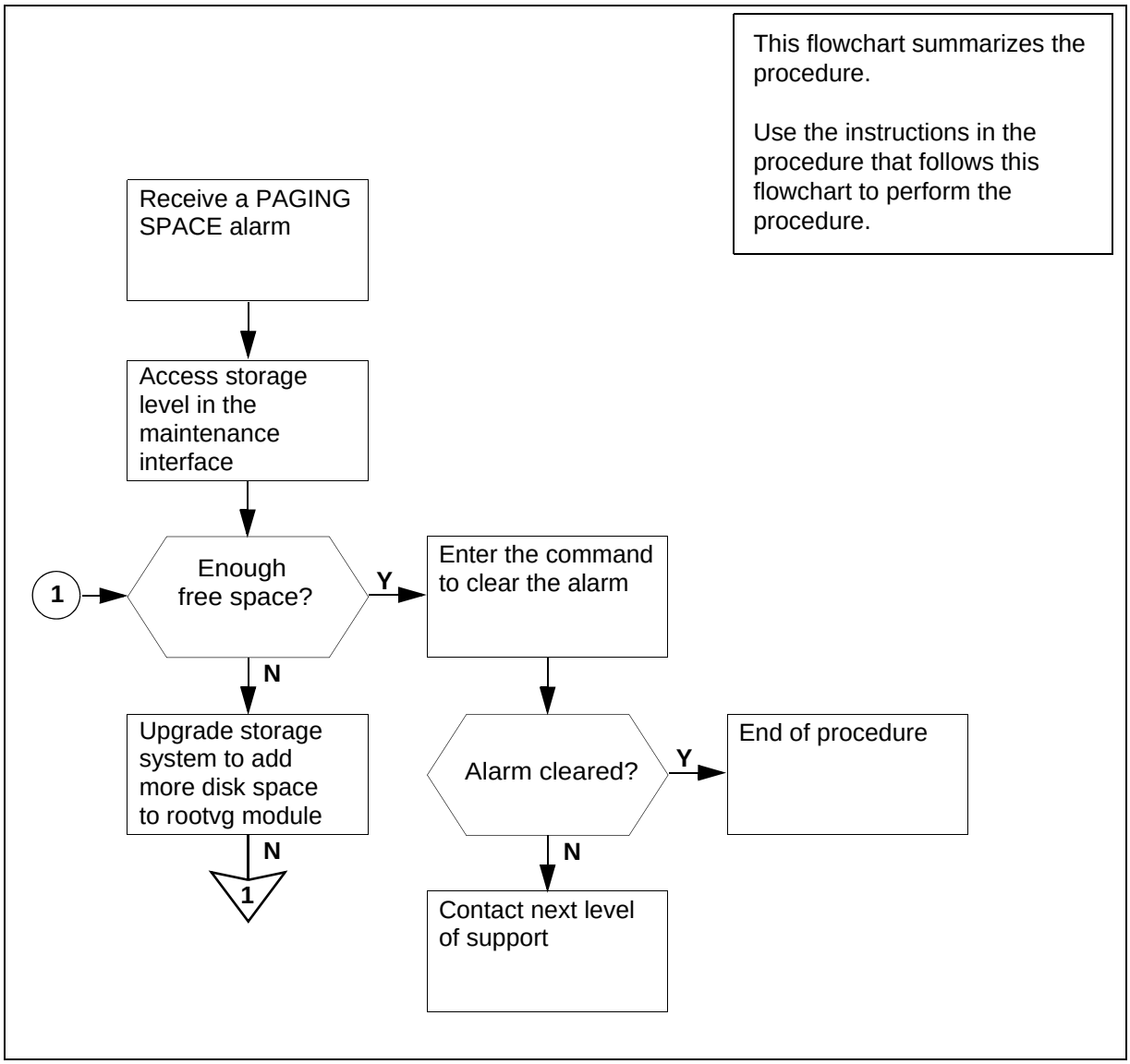
where:
xx = current size of the paging space
yy = required size of paging space

When the paging space is not configured correctly, system performance can be degraded because of excessive paging activity. The degree of the degradation depends upon the current size of paging space, and the loads of the system.

Action

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

PAGING SPACE alarm clearing flowchart



Clearing a PAGING SPACE alarm

At the maintenance interface

1 Access the storage level:

```
> sdmmtc storage
```

2 Use the following calculation to determine if there is enough free space left for the extra paging space:

spaceOK = x-(z-y)

where:
x = free space available for the rootvg
y = normal paging space size required
y = current paging space size

- *x* can be obtained on the volume group list at the storage level of the maintenance interface
- *y* and *z* can be obtained from the corresponding logs: **querysdm flt** at the storage level of the maintenance interface

If the spaceOK is	Do
less than 0	procedure "Upgrading the rootvg MFIO to MFIO or to UMFIO" (in the CS 2000 Core Manager Upgrades document) to add more disk space to the rootvg module, and repeat step 2.
greater than 0	step 3

3 Correct the size of the paging space at the storage level:

```
> change lv paging normal
```

If the command	Do
does not clear the alarm	step 4
clears the alarm	step 5

4 Contact your next level of support.

5 You have completed this procedure.

Clearing an RTBCD alarm

Indication

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

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

Meaning

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

Impact

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

Action

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

Clearing an RTBCF alarm

Indication

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

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

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

Meaning

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

Impact

RTB moves to the SysB state and stops transferring open files.

Action

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

Clearing an RTBER alarm

Purpose

Use this procedure to clear an RTBER alarm.

Indication

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

Meaning

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

Impact

This alarm has the following impact:

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

Action

At the MAP

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

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

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

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

Clearing an RTBFM alarm

Purpose

Use this procedure to clear an RTBFM alarm.

Indication

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

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

Meaning

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

Impact

RTB moves to the SysB state.

Action

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

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

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

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

Clearing an RTBPD alarm

Purpose

Use this procedure to clear an RTBPD alarm.

Indication

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

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

Meaning

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

Impact

RTB moves to the SysB state.

Action

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

Clearing an RTBST alarm

Indication

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

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

Meaning

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

Impact

RTB moves to the SysB state.

Action

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

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

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

If required, contact your next level of support.

Clearing a major SBACP alarm

Purpose

Use this procedure to clear an SBACP alarm.

Indication

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

Meaning

The SBA is shutting down because either

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

Impact

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

Action

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

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

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

At the core manager

1 Go to the Appl level of the sdmmtc tool by typing:

```
sdmmtc appl
```

If the SBA application is	Do
ISTB, Offl, or SysB	step 2
ManB	step 3
InSv, and the alarm is cleared	step 10

If the SBA application is	Do
InSv, but the alarm is still present	contact your next level of support

2 Busy the SBA application:

bsy <SBA_no>

where

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

3 Return the SBA application to service:

rts <SBA_no>

where

<SBA_no> is the number of the SBA application.

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

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

If the SBA	Do
returned to service successfully and the alarm is cleared	step 4
returned to service successfully and the alarm is still present	contact your next level of support
did not return to service successfully	contact your next level of support

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

quit all

5 Access the billing maintenance level:

billmtc

6 Access the schedule level:

schedule

7 Access the real-time billing level:

```
rtb
```

8 Busy the stream:

```
bsy <stream_name> DIRP <destination_name>
```

where:

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

9 Return the stream to service:

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

where:

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

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

10 You have completed this procedure.

Clearing a minor SBACP alarm

Indication

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

Meaning

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

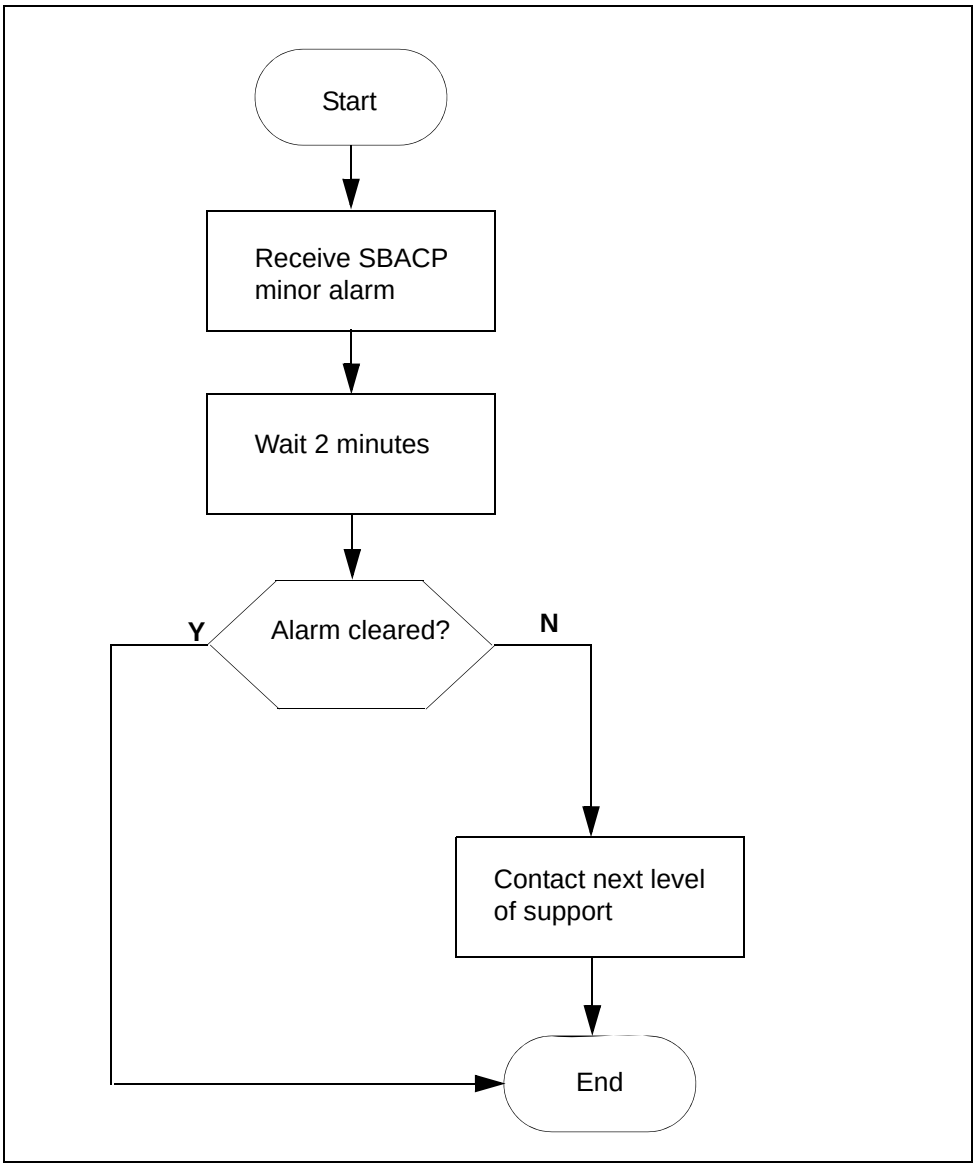
Impact

The SBA program ends, but restarts within two minutes.

Action

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

SBACP (minor) alarm clearing flowchart



Clearing a minor SBACP alarm

At the MAP

1 Wait 2 minutes for the SBA to restart.

2 Contact your next level of support if the

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

3 You have completed the procedure.

Clearing an SBAIF alarm

Purpose

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

Indication

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

The system also generates an SDMB390 log.

Meaning

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

Impact

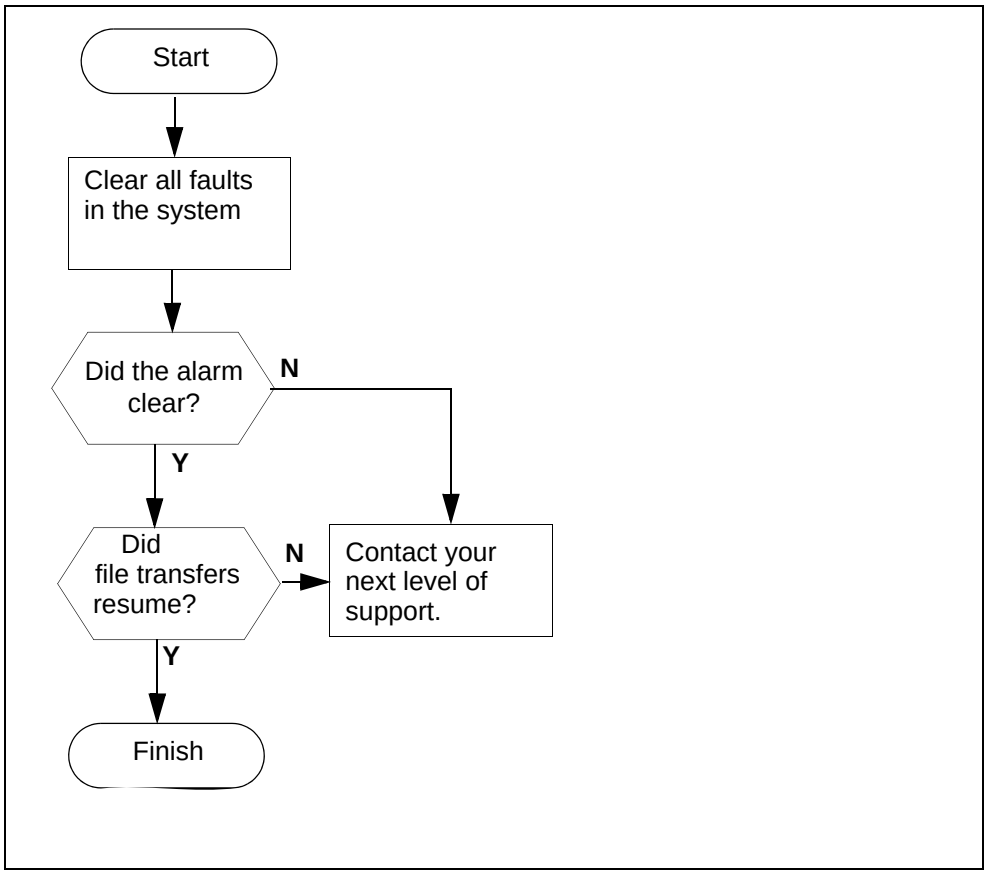
If the alarm does not clear, SBA is not able to transfer files to the downstream destination:

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

Action

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

SBAIF alarm clearing flowchart



Clearing an SBAIF alarm

At a workstation or console

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

The SBAIF alarm clears when the fault is corrected.

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

2 Access the core manager.

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

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

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

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

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

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

5 You have completed this procedure.

Clearing an SDM CONFIG alarm

Purpose

Use this procedure to clear an SDM Configuration alarm.

Indication

At the storage level of the maintenance interface, the word *“Fail”* at the end of “SDM Configuration State” indicates an alarm for the SuperNode Data Manager (SDM) automatic configuration.

Meaning

A problem exists related to the SDM automatic commissioning.

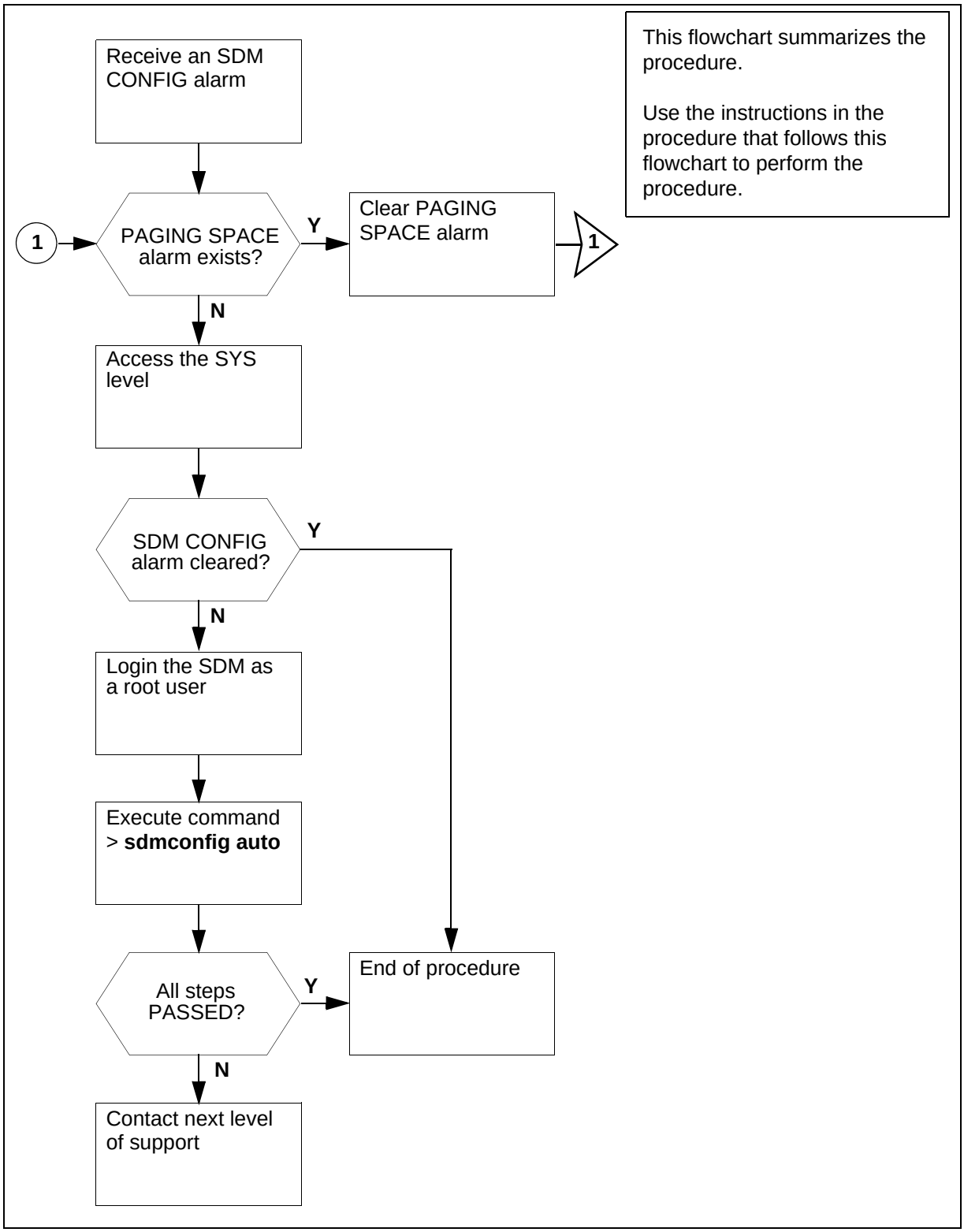
Impact

The problem with the commissioning can prevent the completion of a fresh installation or upgrade.

Action

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

SDM CONFIG alarm clearing flowchart



Clearing an SDM CONFIG alarm

At the maintenance interface

1 Access the storage level:

```
> sdmmtc storage
```

If a PAGING SPACE alarm	Do
exists	procedure *"Clearing a PAGING SPACE alarm"* to clear the alarm, and repeat step 1
does not exist	step 2

2 Access the SYS level:

```
> sys
```

If the SDM CONFIG alarm is	Do
not cleared	step 3
cleared	step 6

3 Log into the SDM as a root user:

```
> telnet <host_name_of_the_SDM>
```

4 Execute the command:

```
# sdmconfig auto
```

If all steps	Do
did not pass	step 5
passed	step 6

5 Contact your next level of support.

6 You have completed this procedure.

Clearing a system image backup Required or Failed alarm

Purpose

Use this procedure to clear a system image Required or Failed alarm.

Indication

At the SYS level of the maintenance interface on the CS 2000 Core Manager, the Backup Status indicates “Required” or “Failed”. The associated log report is SDM308.

Meaning

A system image backup (S-tape) is required when one of the following conditions occurs on the system:

- filesets are installed or upgraded
- logical volumes are added or changed
- configuration changes are made at the Config level of the maintenance interface
- a fresh install occurs
- platform configuration changes are made

The Backup status values are listed in the following table:

Backup Status values

Value	Associated alarm	Meaning
.		The node is in service (InSv). No changes have occurred since the last backup or cleared command.
Required	ISTb	A configuration change has occurred, and a new S-tape image should be made.
In Progress	ISTb	An S-tape image is in progress.
Failed	ISTb	The last attempt to make an S-Tape failed.

Impact

Electronic software delivery (ESD) delivers software loads over a network. Because no backup tapes are delivered with ESD, the backup

Required alarm prompts you to perform regular backups in the event that system recovery becomes necessary.

Note: You can schedule automatic backups using procedure "Scheduling system image backups" in the Administration and Security section. You can also disable the backup Required alarm using procedure Clearing a BAKUP alarm on page 322 in this document.

Action

Perform a system image backup (S-tape) using procedure *"Creating system image backup tapes (S-tapes) manually"* in the CS 2000 Core ManagerSecurity and Administration document, or force-clear the alarm using this procedure.

Note: Force clearing can only be applied with Backup Required and Failed alarms.

At the local VT100 console

1 Access the System level:

```
> sys
```

Note: If you are at the AIX prompt (#), access the System level:

 # sdmmtc sys

2 Clear the Backup Required alarm:

```
> backup clear
```

3 When prompted, confirm you want to clear the alarm:

```
> y
```

4 You have completed this procedure.

Verifying the file transfer protocol

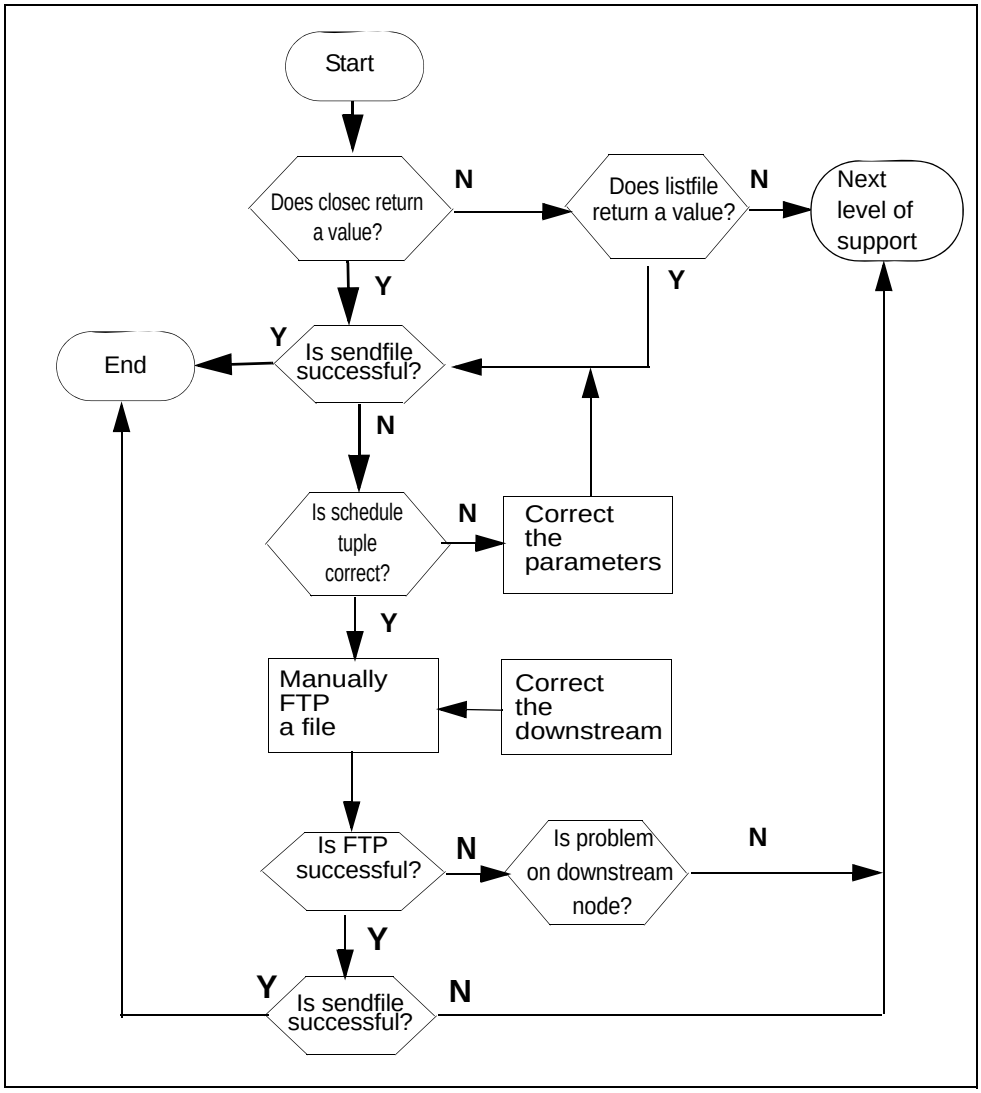
Purpose

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

Action

The following flowchart summarizes the steps outlined in the procedure.

FTP verification flowchart



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

Verify the FTP

At the core manager

1 Access the bill maintenance level:

```
billmtc
```

2 Access the file system:

```
filesys
```

3 Close active billing files:

```
closec <stream_name>
```

where

<stream_name> is the name of the stream.

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

4 Determine the results of the closec command.

If the “closec” command	Do
returns a filename	step 7
does not return a filename	step 5

5 List the primary file (closedNotSent directory):

```
listfile <stream_name>
```

where

<stream_name> is the name of the stream

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

7 Send the primary file (closedNotSent directory):

```
sendfile <stream_name>
```

where

<stream_name> is the name of the stream.

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

8 Go to the previous level:

`quit`

9 Determine the results of the sendfile command.

If the “sendfile” command is	Do
successful	you have completed this procedure
not successful	step 10

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

10 Access the schedule level:

`schedule`

11 List the parameters of the schedule tuple:

`list`

If the parameters are	Do
correct, but you are receiving an alarm	step 21
incorrect	step 12

12 Reset the schedule tuple parameters:

`change`

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

14 Enter the file format.

15 Enter the destination name.

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

16 Observe the schedule tuple displayed.

17 Enter the corrected parameters.

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

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

19 Save the changed parameters:

`save`

If you have	Do
corrected the parameters in the schedule tuple	step 7
determined that the parameters are correct	• step 20 (verify login and write permissions are correct for FTP process without testing a billing file), OR • step 23 (verify login and write permissions are correct for FTP process while testing an actual billing file)

20 Exit the maintenance interface:

`quit all`

21 Login as root user.

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

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

23 Exit back to the command prompt:

`quit all`

24 Login as root user.

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

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

where

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

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

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

26 Access the /tmp directory:

```
cd /tmp
```

27 FTP to the downstream node:

```
ftp <address> <port>
```

where

<address> is the Primary_Destination IP address of the destination node

<port> is the Primary_Port of the destination node

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

Note: A successful login is confirmed by a “230 User <user_name> logged in” message returned by the FTP.

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

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

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

where

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

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

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

31 Set the file transfer mode to binary:

```
ftp> binary
```

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

32 Execute the “structure” command and verify the returned message:

```
ftp> stru f
```

Note: The response from a UNIX machine for a successful command would be: “We only support file structure, sorry.” The response from an AS400 machine for a successful command would be: “250 Data structure is File”.

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

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

where

<file> is the name of a billing file that is copied to the /tmp directory in step 25.

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

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

34 Rename the <file.tmp> file:

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

where

<file.tmp> is the name of the billing file with .tmp extension appended that you created in step 33.

<file> is the name of billing file to which the .tmp extension was appended in step 33.

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

35 Exit from the FTP session:

```
ftp> quit
```

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

36 Correct the directory permissions to allow write access.

37 Repeat steps 21 through 35.

38 Send the primary files in the closedNotSent directory:

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

where

<billing_stream> is the name of the billing stream

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

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

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

Verifying the FTP Schedule

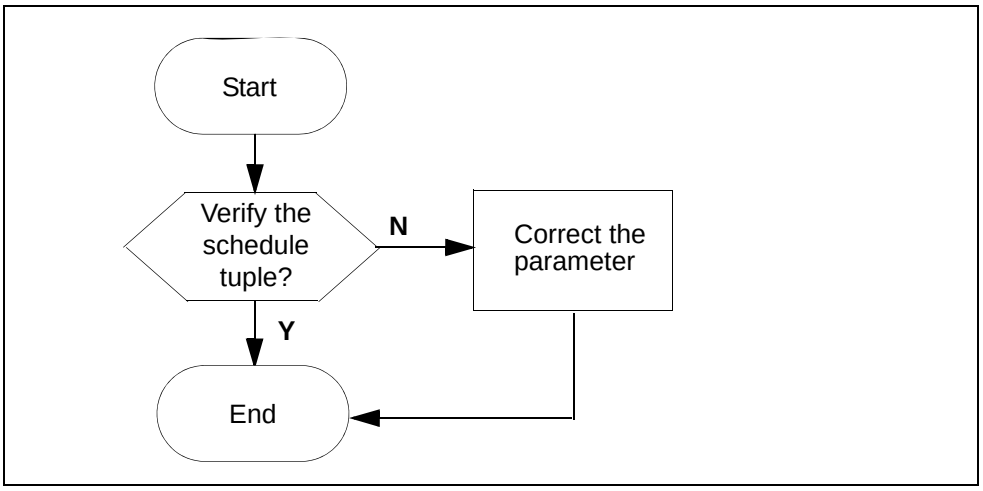
Purpose

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

Action

The following flowchart summarizes the steps in the procedure.

Verifying the FTP schedule flowchart



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

Verifying the FTP schedule

At any workstation or console

1 Log in to the core manager.

2 Access the bill maintenance level:

```
billmtc
```

3 Verify the schedule tuple:

```
schedule
```

4 List the parameters of the schedule tuple:

list

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

5 Reset the schedule tuple parameters:

change

6 Enter the stream name (billing file name).

7 Enter the file format.

8 Enter the destination name.

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

9 Observe the schedule tuple displayed.

10 Enter the parameters that you need to correct.

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

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

12 Save the changed parameters:

save

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

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

14 You have completed the procedure.

Resetting SDM user passwords for DDMS

Application

Use this procedure to reset the passwords for users SDM01-04 when both of the following conditions have occurred:

- the DDMS applications, OSS Comms Svcs and OSS and Application Svcs, remain in in-service trouble (ISTb) after busying and returning the DDMS applications to service
- the QUSER command from the core does not show users SDM01-04

Resetting the passwords for users SDM01-04 consists of

- Resetting the passwords on the CM on page 411
- Changing passwords in the DDMS configuration file on page 412

Prerequisites

To complete this procedure you need the following:

- access to the core
- root-user access to the CS 2000 Core Manager
- passwords for users SDM01-04

Action

Complete all the steps that follow to reset the password for users SDM01-04.

Resetting the passwords on the CM

At the CI prompt on the switch

1 Enter each of the following commands:

```
> unpermit sdm01
> unpermit sdm02
> unpermit sdm03
> unpermit sdm04
```

2 Enter each of the following commands:

```
> permit sdm01 <sdm01_pswd> 4 10000 english all
> permit sdm02 <sdm02_pswd> 4 10000 english all
> permit sdm03 <sdm03_pswd> 4 10000 english all
> permit sdm04 <sdm04_pswd> 4 10000 english all
```

Where

<sdm0n_pswd>
is the password for user SDM0n

Note 1: If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

Note 2: If Enhanced Password Control is in effect on the CM, and any of the SDM01-SDM04 passwords are changed on the CM, you need to apply the same password changes in the DDMS configuration file. Refer to Changing passwords in the DDMS configuration file.

3 You have completed this procedure. Proceed to Changing passwords in the DDMS configuration file on page 412.

Changing passwords in the DDMS configuration file

At the CS 2000 Core Manager

1 Log in to the CS 2000 Core Manager as the root user.

2 Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.

3 Locate and busy OSS Comms Svcs by typing

```
> bsy <n>
```

and pressing the Enter key.

<n>
is the number next to the OSS Comms Svcs fileset

4 Locate and busy OSS and application Svcs by typing

```
> bsy <n>
```

and pressing the Enter key.

<n>
is the number next to the OSS and application Svcs fileset

5 Exit the application level by typing

`> quit all`

and pressing the Enter key.

6 Access the configuration level of the maintenance interface by typing

`# sdmmtc config`

and pressing the Enter key.

7 Access the OSS Comms Svcs configuration level by typing

`> config <n>`

and pressing the Enter key.

<n>
is the number next to the OSS Comms Svcs fileset

8 Press Enter to begin configuration.

9 When prompted to enter the logroute tool, as shown in table DDMS logroute tool banner, press Enter.

DDMS logroute tool banner

```
##############################################################
 # Adding DDMS logroute configuration
##############################################################
Please add DDMS log routing:
            Device type         = file
            File                = /data/logs/ossaps/ossapslog
            Routing             = addrep
            log_type            = DDMS
Press <RETURN> when ready
```

The Logroute Main Menu appears, as shown in figure Logroute tool main menu.

Logroute tool main menu

```
                    Logroute Main Menu


                    1 –    Device List
                    2 –    Global Parameters
                    3 –    CM Configuration File
                    4 –    GDD Configuration
                    5 –     Help
                    6 –     Quit Logroute




Enter Option    ==>
```

10 Enter the number next to Quit Logroute.

The CM User Setup screen is displayed as shown in the example that follows.

Example of DDMS CM User Setup screen

```
                    CM User Setup

                0. QUIT
                1. Add user
                2. Delete user(by ID)
                3. Update passwd(by ID)
                4. Display users(ID)

                Enter choice:
```

11 Enter the number next to Display users(ID).

12 Note the user ID next to SDM01-04.

13 Enter the number next to Update passwd(by ID).

14 Enter the user ID (not user name) for SDM01.

15 Enter new password for SDM01.

The passwords for SDM0n must be the same as that entered in Resetting the passwords on the CM on page 411.

Note: The userIDs and passwords are not case sensitive.

16 Repeat step 15 for SDM02, SDM03, and SDM04, then proceed to step 17.

17 Enter the number next to QUIT in the CM User Setup screen.

18 Exit all levels of the maintenance interface by typing

```
> quit all
```

and pressing the Enter key.

19 Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.

20 Locate and return OSS Comms Svcs to service by typing

```
> rts <n>
```

and pressing the Enter key.

<n>
is the number next to the OSS Comms Svcs fileset

21 Locate and return OSS and application Svcs to service by typing

```
> rts <n>
```

and pressing the Enter key.

<n>
is the number next to the OSS and application Svcs fileset

22 Exit all levels of the maintenance interface by typing

```
> quit all
```

and pressing the Enter key.

You have completed this procedure.