CS 2000 Core Manager Fault Management

Fault management strategy

The Communication Server 2000 Core Manager (CS 2000 Core Manager) fault management strategy includes the dual functions of Fault Delivery and Test and Diagnostic capabilities.

The CS 2000 Core Manager component handles many of the fault delivery features.

> **CAUTION**
> **Do not attempt to RTS a failed hardware.**
> If you experience any CS 2000 Core Manager hardware failure, do not attempt to return this hardware to service (RTS). Replace the failed hardware with an available spare as soon as possible. Contact your next level of technical support for further analysis and instructions as necessary.

Tools and utilities

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

Logs

CS 2000 Core Manager events are recorded internally to the CS 2000 Core Manager in a series of log reports. CS 2000 Core Manager log reports are local to the CS 2000 Core Manager. Most CS 2000 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.

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.

CS 2000 Core Manager log reports fall into three categories: trouble (TBL) logs, state change logs, and information (INFO) logs.

- Trouble logs (SDM3xx) provide an indication of some type of fault for which corrective action can be taken. These logs are generated for connectivity failures, system resource problems, and application software and hardware failures. Each of these trouble conditions corresponds to an alarm on the alarm banner of the CS 2000 Core Manager maintenance interface.

- State change logs (SDM5xx) provide information about CS 2000 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 CS 2000 Core Manager or the Log Delivery application is returned to service from a ManB state, some logs may be delivered with the CM_CLLI in the Office ID field of the log header, instead of the data filled LOG_OFFICE_ID. This occurs only for logs generated by CS 2000 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 CS 2000 Core Manager.

- Information logs (SDM6xx) 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

SDM logs describe events general events related to the operations of the CS 2000 Core Manager. The following table lists SDM logs.

Table 1 CS 2000 Core Manager logs (Sheet 1 of 6)

Log	Trigger	Action
SDM300	The connection from the CS 2000 Core Manager to the Core or the operating company LAN server(s) is down.	Contact your system administrator or Nortel Networks for assistance.
SDM301	A logical volume is not mirrored.	Check hardware faults as mirroring may be lost due to a hard disk failure on the CS 2000 Core Manager. *Note:* If a disk has just been replaced and brought back in-service, the system may take more than 15 minutes to restore mirroring.
SDM302	The use of a system resource has exceeded its threshold.	Isolate and clear the problem.
SDM303	An CS 2000 Core Manager application or process has failed more than three times in a day, or has declared itself to be in trouble.	Users with root permissions can examine the log files in /usr/adm to determine the cause of the process failure. If required, contact your system administrator or Nortel Networks for assistance.
SDM304	The Log Delivery application cannot deliver logs to the specified UNIX file.	Use the Log Delivery online commissioning tool (logroute) to verify the existence and validity of the device name. Refer to the following procedures in this document for more information: • Adding a log device using logroute in the Configuration section • Deleting a device using logroute in the Fault section If required, contact your system administrator or Nortel Networks for assistance.

Table 1 CS 2000 Core Manager logs (Sheet 2 of 6)

Log	Trigger	Action
SDM306	The Table Access Service application on the CS 2000 Core Manager has detected that the software load on the Core is incompatible with the software load on the CS 2000 Core Manager.	Upgrade the CM software to a version that is compatible with the SDM software. ***Note:*** The software on the CS 2000 Core Manager must not be at a lower release level than the software on the Core.
SDM308	Manual 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)" in the Security and Administration section. Ensure the backup tape is inserted. If required, contact your system administrator or Nortel Networks for assistance.
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 the Fault section. Check the cabling to the module. If you cannot determine the reason for the fault, contact your next level of support.
SDM314	A DS512 link is down on the CS 2000 Core Manager.	Use the "querysdm" command from the MAP display to check for DS512 hardware faults on the CS 2000 Core Manager. Use the "trnsl" command from the MAP display to check the link status. Perform link tests from the CS 2000 Core Manager maintenance interface. Check the cabling to the DS512 port.

Table 1 CS 2000 Core Manager logs (Sheet 3 of 6)

Log	Trigger	Action
SDM315	The Table Access Service application on the CS 2000 Core Manager has detected corruption in the Data Dictionary on the Core.	Contact your next level of support with the information provided in the log. The log information contains essential information for identifying the Data Dictionary type that is corrupt.
SDM317	The system has detected a Distributed Computing Environment (DCE) problem.	Contact your next level of support to help determine the cause of the failure.
SDM318	An operational measurements (OM) report was not generated. (The OM report failed to complete within one report interval.)	Contact Nortel Networks.
SDM325	Indicates a lost connection to a Preside network management component.	None
SDM332	Indicates that the system audit completed with failures	Refer to procedure "Viewing the system audit report and taking corrective action" in the Fault section.
SDM500	Indicates the initial startup of the CS 2000 Core Manager. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM501	Indicates an CS 2000 Core Manager state change to in service (InSv). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM502	Indicates an CS 2000 Core Manager state change to manual busy (ManB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None

Table 1 CS 2000 Core Manager logs (Sheet 4 of 6)

Log	Trigger	Action
SDM503	Indicates an CS 2000 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 MAP alarms triggered by the SDM - APPL SDM critical" in this document.
SDM504	Indicates an CS 2000 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 MAP alarms triggered by the SDM - APPL SDM minor and major" in this document.
SDM505	Indicates an CS 2000 Core Manager state change to offline (OffL) state. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM550	Indicates an CS 2000 Core Manager node status change. One or more of the following can cause the status change: • CS 2000 Core Manager node state • hardware device • software component • application	Refer to the corresponding procedure in the Fault section if required. ***Note:*** Log SDM550 is generated on the CM.
SDM600	The connection from the CS 2000 Core Manager to the Core or the operating company LAN server(s) has been reestablished. This log is generated only after a connectivity failure has been corrected, and not at system startup.	None
SDM601	Mirroring has been reestablished after a logical volume mirroring failure.	None
SDM602	A system software resource has returned below its alarm threshold.	None

Table 1 CS 2000 Core Manager logs (Sheet 5 of 6)

Log	Trigger	Action
SDM603	A fault on an CS 2000 Core Manager application or process has cleared.	None
SDM604	The Log Delivery application generates this log when the Core does not have enough CPU time to format logs, and discards the logs.	Increase office parameter PER_OPC_LOGDEV_BUFFER_ SIZE to its maximum size of 22,000. (For more information about this parameter, refer to the *SuperNode Data Manager Log Report Reference Manual*, 297-5051-840.) If you still continue to receive SDM604 logs after you have increased the size of the parameter, or if large numbers of logs are lost, contact Nortel Networks for assistance.
SDM608	A system image backup (S-tape) has been completed.	None
SDM609	A hardware device has been returned to the in-service state.	None
SDM614	A DS512 link is up again on the CS 2000 Core Manager.	None
SDM616	A log delivery connection attempt was rejected.	None
SDM617	A Distributed Computing Environment (DCE) problem is cleared.	None
SDM619	The OM Access Server has detected a corrupt OM Group during an OM Schema download.	None
SDM620	Reports SDM system performance data such as CPU usage, number of processes, swap space occupancy, and logical volume capacities.	None

Table 1 CS 2000 Core Manager logs (Sheet 6 of 6)

Log	Trigger	Action
SDM622	The SDM log delivery application generates this log when the file device reaches its maximum size.	Check if you have configured enough space for the file device. If there is a software error causing the increase of logs, contact Nortel Networks for help.
SDM625	Indicates a re-established connection to a Preside network management component.	None.
SDM630	Indicates the start time and completion time of the REX test.	None.
SDM632	Indicates one of the following: • the system audit completed successfully • the system audit completed with warnings • a user cleared the system audit status • the system audit execution time is disabled or enabled	If the response is "the system audit completed with warnings", refer to procedure "Viewing the system audit report and taking corrective action" in the Fault section.
SDM650	SDM link maintenance requests the logging of a failed link maintenance action. An example of a link maintenance action is the system testing of a link.	None *Note:* Log SDM650 is generated on the CM.

SDMB logs

SDMB logs describe events related to the operations of the SuperNode Billing Application (SBA) and the SDM Billing System that resides on the SDMCS 2000 Core Manager. The following table lists SDMB logs.

Table 2 SDM Billing Application (SBA) logs (Sheet 1 of 6)

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 CS 2000 Core Manager is not communicating with the Core. Determine whether the CS 2000 Core Manager, the Message switch (MS) and the Frame Transport bus (FBus) are in service (InSv) or in-service trouble (ISTb). If the CS 2000 Core Manager is InSv or ISTb, return the billing stream to service.
SDMB315	A general software-related problem has occurred.	Contact your next level of support.
SDMB316	A billing-related process has been manually "killed".	Restart the process.
SDMB320	A billing backup-related problem occurred, which affects more than one file.	Ensure the backup volumes configured for the stream have enough available space.
SDMB321	A billing backup-related problem occurred, which affects one file.	Ensure the backup volume is not busy or full.
SDMB330	The configuration of a billing stream failed.	Configure the billing stream using procedure "Configuring a billing stream" in the Accounting section.
SDMB350	An SBA process has reached a death threshold and made a request to restart. A death threshold occurs after a process has died more than 3 times less than 1 minute apart.	SBA will automatically restart. What for logs that indicate that SBA is in normal operation. If the system generates this log more than once, contact your next level of support.

Table 2 SDM Billing Application (SBA) logs (Sheet 2 of 6)

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 CS 2000 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 CS 2000 Core Manager. You may need to FTP files or may need to clean up the disk.
	• The disk use is above the critical threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The disk use is above the major threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The disk use is above the minor threshold specified in the MIB in parameter. When this occurs, alarm LODSK is raised.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The disk is full.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape.
	• The SBA cannot close or open a file.	• Check to see if files are being sent FTP. If not, set the system up to FTP files or back up files to the DAT tape. Also check file permission for the destination directories.
	• 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 2 SDM Billing Application (SBA) logs (Sheet 3 of 6)

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

Table 2 SDM Billing Application (SBA) logs (Sheet 4 of 6)

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 2 SDM Billing Application (SBA) logs (Sheet 5 of 6)

Log	Trigger	Action
SDMB390	A schedule-related problem has occurred. When this occurs, alarm SBAIF is raised.	Clear the alarm and any alarms related to failure.
SDMB400	This log is generated for every active stream every hour and lists all of the current active alarms.	Clear alarms immediately using the corresponding procedure in the Fault section.
SDMB530	A change in the configuration or status of a stream has occurred.	None
SDMB531	The configuration for backup volumes has been corrected.	None
SDMB550	The SBA has shut down either because the CS 2000 Core Manager was busied or the SBA was turned off.	Determine the reason SBA shut down.
SDMB610	A communication-related problem with the SBA has been resolved.	None
SDMB615	A software-related condition has been resolved.	None
SDMB620	A backup-related problem with the SBA has been resolved.	None
SDMB621	A new backup file has been started.	None
SDMB625	Recovery has started on a backup file.	None
SDMB650	The SBA is restarting one or more of its processes.	None
SDMB655	• The state of a billing file has changed. • Disk utilization for a particular stream has dropped below a threshold. • A billing file could not be moved to closedSent.	Contact your next level of support.

Table 2 SDM Billing Application (SBA) logs (Sheet 6 of 6)

Log	Trigger	Action
SDMB660	A problem related to communications with other SBA features is resolved.	None
SDMB665	A software problem on the Core that prevents the synchronization (downloading) of FLEXCDR data at the CS 2000 Core Manager.	Restart the Core with a load that supports the SBA enhancements for CDR on CS 2000 Core Manager.
SDMB670	Either a CDR-to-BAF conversion process used default values to create a BAF field because a CDR field was missing, or the problem was corrected.	For the missing CDR field(s), determine which are needed to generated the BAF field. Use the BAF field displayed in the log report and refer to the applicable Billing Records Application Guide for a list of the CDR fields associated with each BAF field. Update the CDR to include the missing field.
SDMB675	A problem related to file transfer was resolved.	None
SDMB680	The file transfer mode has changed value.	None
SDMB820	Minimal backup space is available.	Increase the size of backup volumes.

Collecting DEBUG information using the PLATGATHER command

The procedures that follow provide instructions on how to collect DEBUG information from the CS 2000 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 CS 2000 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 understand 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.

At the CS 2000 Core Manager command line (UNIX prompt)

1   Run the utility to collect the output by typing

 # platgather

and pressing the Enter key.

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

2   Run the utility to collect the output by typing

 # FXgather

and pressing the Enter key.

3   Tar and compress the content of directory /var/adm by typing

     `# cd /var/adm`

     and pressing the Enter key.

     `# tar cvf varadm.tar *.day* *.log`

     and pressing the Enter key.

     `# compress varadm.tar`

     and pressing the Enter key.

     Response:

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

4   Use the following table to determine your next step.

If you used the	Do
platgather command	steps 5 and 6
FXgather command	steps 7 and 8

5   Move the following output/files of all previous commands out of the system to a secure location using FTP.

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

  Example
       /var/adm/platgather_wcary2p2_20020528091133.tar.Z

- /var/adm/varadm.tar.Z

6   Remove the output of the varadm.tar.Z file from the system by typing

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

     and pressing the Enter key.

     You have completed this procedure.

7   Move the following output/files of all previous commands out of the system to a secure location using FTP.

• /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

8   Remove the output of the varadm.tar.Z file from the system by typing

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

and pressing the Enter key.

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 CS 2000 Core Manager command line (UNIX prompt) of the active domain (domain 0)

1   Run the utility to collect the output by typing

`# platgather`

and pressing the Enter key.

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

2   Run the utility to collect the output by typing

`# FXgather`

and pressing the Enter key.

3   Tar and compress the content of directory /var/adm by typing

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

and pressing the Enter key.

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

and pressing the Enter key.

```
# compress varadm_sysold.tar
```

and pressing the Enter key.

Response:

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

At the CS 2000 Core Manager command line (UNIX prompt) of the inactive domain (domain 1)

4   Run the utility to collect the output by typing

```
# platgather
```

and pressing the Enter key.

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

5   Run the utility to collect the output by typing

```
# FXgather
```

and pressing the Enter key.

6   Tar and compress the content of directory /var/adm by typing

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

and pressing the Enter key.

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

and pressing the Enter key.

```
# compress varadm_sysnew.tar
```

and pressing the Enter key.

Example response:

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

7   Use the following table to determine your next step.

If you used the	Do
platgather command	steps 8 through 10
FXgather command	step 11 through 13

From the active domain (domain 0)

8   Move the DEBUG files from the inactive domain (domain 1) to the active domain (domain 0) by typing

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

and pressing the Enter key.

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_20020523
    223351.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
```

9   Move the following output/files of all previous commands out of the system to a secure location using FTP.

- /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

10   Remove the gathered output/files from the system from the system by typing

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

and pressing the Enter key.

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

and pressing the Enter key.

You have completed this procedure.

From the active domain (domain 0)

11   Move the DEBUG files from the inactive domain (domain 1) to the active domain (domain 0) by typing

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

and pressing the Enter key.

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
```

12   Move the following output/files of all previous commands out of the system to a secure location using FTP.

- /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

13   Remove the following gathered output/files from the system by typing

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

and pressing the Enter key.

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

and pressing the Enter key.

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

and pressing the Enter key.

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

and pressing the Enter key.

14   You have completed this procedure.

Disabling or enabling/changing the time of the system audit

The following procedure provides instructions on how to disable or enable/change the time of the system audit. Refer to "System audit overview" in the Basics section for more information on the system audit.

At the CS 2000 Core Manager UNIX command line

1   Use the following table to determine how to proceed.

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 by typing

`# sysaudit -change <value>`

and pressing the Enter key.

Where:

> **<value>**
> is the time in hours and minutes (hh:mm) or "default", which sets the time to 2:00 AM

Example command

`# 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 by typing

`# sysaudit -time`

Example response

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

4   Disable the system audit by typing

`# sysaudit -disable`

and pressing the Enter key.

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.

Performing a system audit

The following procedure provides instructions on how to perform a system audit. Refer to "System audit overview" in the Basics section for more information on the system audit.

At any workstation or console

1   Log in to the CS 2000 Core Manager using the root user ID and password.

2   Execute the desired system audit check by typing

`# sysaudit -<option>`

and pressing the Enter key

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

```
# 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 <u>Viewing the system audit report and taking corrective action</u> in the Fault section.

Viewing the system audit report and taking corrective action

The following procedure provides instructions on how to view the results of a system audit and take any necessary corrective action. Refer to "System audit overview" in the Basics section for more information on the system audit.

At the CS 2000 Core Manager

1   Display the system audit report by typing

```
# 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 21 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   Use the following table to determine your next step.

Message in sysaudit report	Type of message & action
Failed to obtain output of the rmt<#> device.	Failure - perform step 4
Failed to access device <device name>.	Failure - perform step 4
<device name> is in a failed state.	Failure - perform step 5
HW module located in slot <slot number> is not available.	Warning - perform step 5
Failed to access the content of CPU-<cpu number>.	Failure - perform step 5
CPU-0 is not online	Warning - will have been tracked and reported in the HW check (perform step 5)
CPU-2 is not online	Warning - will have been tracked and reported in the HW check (perform step 5)
The maxuproc attribute of the sys0 device is currently set to <value>, but should be set to 500.	Failure - perform step 6
The maxmbuf attribute of the sys0 device is currently set to <value>, but should be set to 0.	Failure - perform step 7
The maxpout attribute of the sys0 device is currently set to <value>, but should be set to 31.	Failure - perform step 8
The minpout attribute of the sys0 device is currently set to <value>, but should be set to 15.	Failure - perform step 9
The block_size attribute of the rmt<#> device is currently set to <value>, but should be set to 512.	Failure - perform step 10

Message in sysaudit report	Type of message & action
The isc_sp process is currently running, although the split mode upgrade is not in progress.	Failure - perform step 11
CPU <cpu_number> is not flushed after the latest split-mode upgrade.	Failure - perform step 12
The mount point and label for logical volume <logical volume name> do not match.	Failure - perform step 13
The cms_notify_meth attribute of sys0 device is not set to the appropriate value.	Failure - perform step 14
The cms_notify_attr attribute of sys0 device is not set to the appropriate value.	Failure - perform step 15
<device name> is currently offline.	Warning - perform step 16
Volume group <volume group name> is not fault tolerant.	Failure - contact your next level of support
The quorum attribute of volume group <volume group name> is set to yes.	Failure - contact your next level of support
Volume group <volume group name> is not mirrored.	Failure - contact your next level of support
Failed to obtain the list of filesystems in the <volume group name> volume group.	Failure - contact your next level of support
Failed to obtain the content of the <logical volume name> logical volume.	Failure - contact your next level of support
Failed to obtain the output of the sys0 device	Failure - contact your next level of support
Filesystem <filesystem name> is configured on rootvg, but should be configured on datavg.	Failure - contact your next level of support

Message in sysaudit report	Type of message & action
autolvfix, lresynclv or mklvcopy is running, while both rootvg and datavg are fully mirrored	Failure - contact your next level of support
cm and telcolan entries are configured on the same IP address.	Failure - contact your next level of support
The hosts file is configured with more than one <entry name> entry.	Failure - contact your next level of support
The smm process is not running on the system	Failure - contact your next level of support
The snc process is not running on the system	Failure - contact your next level of support
The sam process is not running on the system	Failure - contact your next level of support
The lmp process is not running on the system	Failure - contact your next level of support
The <user> user is not configured on the system.	Failure - contact your next level of support
The process with <process ID> is expected to be a runaway process.	Failure - contact your next level of support
Failed to obtain the output of the SDM CPU usage.	Failure - contact your next level of support
Failed to access the SDM hosts file.	Failure - contact your next level of support
Failed to obtain the content of the <volume group name> volume group.	Failure - contact your next level of support
Filesystem <filesystem name> is not mounted.	Failure - contact your next level of support
Filesystem <filesystem name> has stale partitions.	Failure - contact your next level of support
Failed to obtain the content of physical volumes.	Failure - contact your next level of support

Message in sysaudit report	Type of message & action
<disk name> has been recorded with a bogus PVID <PVID>.	Failure - contact your next level of support
The autoboot attribute of CPU-<cpu_number> is NOT set, for autoboot to be ON vb=Y.	Failure - contact your next level of support
The autorestart attribute of the sys0 device is set to false, it should be set to true.	Failure - contact your next level of support
Failures are recorded in the eeprom of module <module name>.	Warning - contact your next level of support
The system is operating under an extreme load.	Warning - contact your next level of support
The system is operating under a heavy load.	Warning - Contact your next level of support
The system is operating under full capacity.	Warning - Contact your next level of support
The system is experiencing major disk access delays.	Warning - Contact your next level of support.
The system is experiencing unbalanced disk access problems.	Warning - Contact your next level of support.
<device name> is currently integrating.	Warning - no action required
<device name> is in an integrating state.	Warning - no action required
Volume group <volume group name> is integrating.	Warning - no action required
Faults are recorded in the output of the "querysdm flt" command. Please execute the "querysdm flt" command for specifics on these faults.	Warning - execute the "querysdm flt" command

4   Use the following table to determine your next step.

If	Do
the hardware module that corresponds to the rmt<#> or <device name> is in a failed state (will have been 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   Proceed as follows to correct the hardware failure:

  a Access the hardware level and verify the status of the device by typing

      `# sdmmtc hw`

      and pressing the Enter key.

If the device is	Do
marked as "F" (failed)	replace the hardware module using the corresponding procedure in the Fault section - when complete continue with step 17 in this procedure
not marked as "F" (failed)	substep b

  b Exit the maintenance interface by typing

      `> quit all`

      and pressing the Enter key.

  c Further verify if any failures exist by typing

      `# lsstate -f`

      and pressing the Enter key.

If	Do
no failures are reported	step 17
failures are reported	contact your next level of support

6 Proceed as follows to reset the maxuproc value:

a Reset the maxuproc value by typing

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

and pressing the Enter key.

b Verify that the maxuproc value has been changed by typing

```
# lsattr -El sys0
```

and pressing the Enter key.

If the maxuproc value is	Do
set to 500	step 17
not set to 500	contact your next level of support

7 Proceed as follows to reset the maxmbuf value:

a Reset the maxmbuf value by typing

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

and pressing the Enter key.

b Verify that the maxmbuf value has been changed by typing

```
# lsattr -El sys0
```

and pressing the Enter key.

If the maxmbuf value is	Do
set to 0	step 17
not set to 0	contact your next level of support

8 Proceed as follows to reset the maxpout value:

a Reset the maxpout value by typing

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

and pressing the Enter key.

b Verify that the maxpout value has been changed by typing

`# lsattr -El sys0`

and pressing the Enter key.

If the maxpout value is	Do
set to 31	step 17
not set to 31	contact your next level of support

9 Proceed as follows to reset the minpout value:

a Reset the minpout value by typing

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

and pressing the Enter key.

b Verify that the minpout value has been changed by typing

`# lsattr -El sys0`

and pressing the Enter key.

If the minpout value is	Do
set to 15	step 17
not set to 15	contact your next level of support

10 Proceed as follows to reset the block size:

a Set the block size to 512 by typing

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

and pressing the Enter key.

Where:

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

b Verify the block size value has been changed by typing

`# lsattr -El rmt<#>`

and pressing the Enter key.

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

If the block size value is	Do
set to 512	step <u>17</u>
not set to 512	contact your next level of support

11 Proceed as follows to stop the isc process:

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

a Ensure the split-mode process is not currently running on the system by typing

`# ps -ef|grep soup`

and pressing the Enter key.

If the split-mode process is	Do
running	step <u>17</u>
not running	substep <u>b</u>

b Terminate the process by typing

`# spstop`

and pressing the Enter key.

c Verify the process was stopped by typing

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

and pressing the Enter key.

> *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 17
still running	contact your next level of support

12   Proceed as follows to flush the CPU data:

a Refresh the data on the affected CPU by typing

```
# restart -c <cpu> -z
```

and pressing the Enter key.

Where:

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

b Verify the CPU has been flushed by typing

```
# restart -c <cpu>
```

and pressing the Enter key.

Where:

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

If all the values of the CPU	Do
are "_"	step 17
are not "_"	contact your next level of support

13   Proceed as follows to match the label and mount point :

    a   Display the details of the affected logical volume by typing

       `# lslv <logical volume_name>`

    and pressing the Enter key.

    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:           /sba/ama
MIRROR WRITE CONSISTENCY: on
EACH LP COPY ON A SEPARATE PV ?: yes
```

    b   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 17
do not match	substep c

    c Change the label to match the mount point by typing

        `# chlv -L "<mount point>" <volume_name>`

        and pressing the Enter key.

        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`

    d Re-display the details for the logical volume to ensure the change was made by typing

        `# lslv <volume_name>`

        and pressing the Enter key.

        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 17
do not match	contact your next level of support

14   Proceed as follows to reset the "cms_notify_meth" attribute:

  a Reset the "cms_notify_meth" attribute by typing

```
# chdev -l sys0 -a
cms_notify_meth="/sdm/mtce/smm/smm_cms_notif
y"
```

    and pressing the Enter key.

  b Verify the attribute value changed by typing

```
# lsattr -El sys0
```

    and pressing the Enter key.

If the value	Do
changed	step 17
did not change	contact your next level of support

15   Proceed as follows to reset the "cms_notify_attr" attribute:

  a Reset the "cms_notify_attr" attribute by typing

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

    and pressing the Enter key.

  b Verify the attribute value changed by typing

```
# lsattr -El sys0
```

    and pressing the Enter key.

If the value	Do
changed	step 17
did not change	contact your next level of support

16   Determine why the device is offline. It may either need to be replaced (replace using the corresponding procedure in the Fault section), or returned to service if already replaced.

17   Use the following table to determine your next step.

If you	Do
have resolved all the failures	clear the sysaudit alarm using procedure <u>Clearing a system audit alarm</u> in the Fault section
have not resolved all the failures	return to step <u>3</u>

18   You have completed the procedure.

Performing a REX test

The following procedure provides instructions on how to execute a REX test and view the results. Refer to "Routine exercise (REX) test overview" in the Basics section for more information on the REX test.

At any workstation or console

1 Log in to the CS 2000 Core Manager using the root user ID and password.

2 Execute the desired REX test by typing

`# sdmrex <option>`

and pressing the Enter key

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)

Example command

```
# sdmrex cpu
```

Example response

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

3 Proceed as follows to view the results of the REX test.

a Access the /var/adm directory by typing

`# cd /var/adm`

and pressing the Enter key.

   b   View the rexresultlog file by typing

   # view rexresultlog

   and pressing the Enter key.

   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

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 in the following table.

Procedures for which remote access to log devices can be used

Log device	Procedure	Applies to
TCP	Accessing a TCP device from a remote location	"Adding a log device using logroute" in the Configuration section
		"Displaying or storing log records using logreceiver" in the Fault section
		"Storing logs in a file" in the Fault section
TCP-IN	Accessing a TCP-IN device from a remote location	"Adding a log device using logroute" in the Configuration section
		"Configuring a CS 2000 Core Manager for fault forwarding" in the Configuration section
		"Deleting a device using logroute" in the Fault section

Accessing a TCP device from a remote location

At the remote workstation

1 Start the logreceiver tool by typing

```
> logreceiver <port_number>
```

where:

    <port_number>
        is the port number used for the TCP device on the CS 2000 Core Manager

2 Continue with the desired procedure.

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 CS 2000 Core Manager by typing

`> telnet <ip_address> <port_number>`

where:

> **<ip_address>**
> is the address of the CS 2000 Core Manager

> **<port_number>**
> is the number of the port of the device on the CS 2000 Core Manager

2   Log into the CS 2000 Core Manager either as maint or admin.

3   Start the logroute tool by typing

`# logroute`

and pressing the Enter key.

4   Continue with the desired procedure.

5   You have completed this procedure.

SBA alarm troubleshooting

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.

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

- A problem in the FTP process: if you receive numerous FTP and LODSK alarms, this can indicate a problem with either the SBA or the general FTP process on the CS 2000 Core Manager. LODSK generally indicates that your primary files (closedNotSent) are not being moved from the CS 2000 Core Manager to the downstream processor. If there is an accompanying log, look at the whole picture. The downstream processor can be full with no space to write files to, which can cause an FTP error. When this happens, you see Communication Server 2000 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.

- An 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 of where the Communication Server 2000 core is not communicating with the CS 2000 Core Manager.

The following procedures discuss how to clear alarms based on the FTP process:

- Verifying the file transfer protocol
- Verifying the FTP Schedule

The following procedures discuss how to clear alarms based on communication problems between the Communication Server 2000 core and the CS 2000 Core Manager:

- Clearing a DSKWR alarm
- Clearing a NOCOM alarm

- [Clearing a major SBACP alarm](#)
- [Clearing a minor SBACP alarm](#)

APPL Menu level alarms

Because SBA processing takes place in both the CM and the CS 2000
Core Manager environment, the SBA program displays CS 2000 Core
Manager-generated alarms in the MAPCI;MTC window at the CM. The
following figure illustrates the SBA alarms that are displayed under the
APPL Menu level at the MAPCI;MTC level on the CM side.

Alarms layout
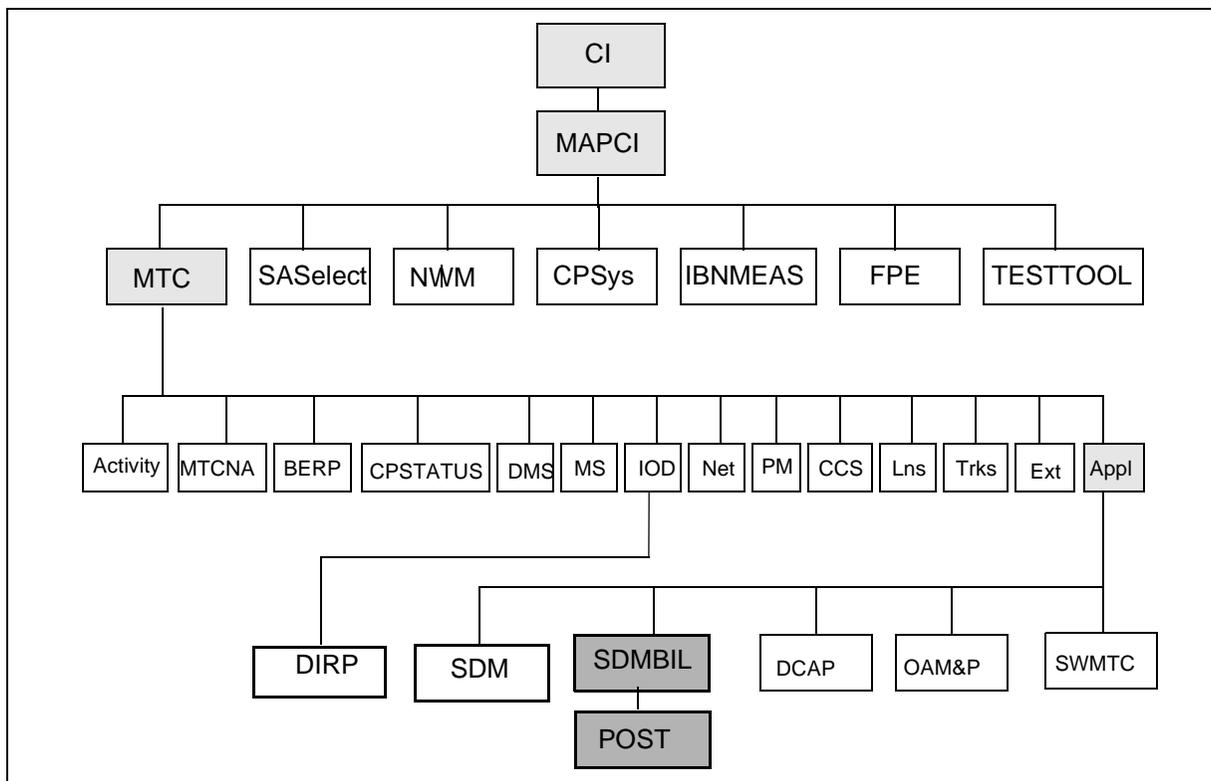
Maintenance for SBA

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 CS 2000 Core Manager side is through the interface on the SBA RMI. For example, you perform maintenance on the CS 2000 Core Manager side of SBA by using commands in the billing level (billmtc) of the CS 2000 Core Manager RMI display.

You can also display the alarms raised by the CS 2000 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.

Note: Maintenance users who log onto the CS 2000 Core Manager with the SDMRLOGIN command cannot access either the billmtc or the sdmmtc level of the CS 2000 Core Manager, but they can issue commands.

Alarm criticality

There are three levels of criticality for SBA alarms:

- Critical: indicates a severe problem with the system that requires intervention.

- Major: indicates a serious situation that can require some type of intervention.

- Minor: indicates a minor problem that deserves investigation to prevent it from evolving to a major problem.

Note: 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. It is recommended that you use the DispAl command to view all outstanding alarms, and to 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 typing:

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

and pressing the Enter key.

Where

<x> is the name of the stream.

The possible state values and their definition are as follows:

- Offline pending (OffP): indicates the stream has been turned off and is waiting for the CS 2000 Core Manager to complete processing its data.

- Offline (OffL): indicates the stream is offline.

- Manual busy (ManB): indicates the stream has been manually busied by a user from the CM; data is being written to backup files.

- System busy (SysB): indicates the stream has been busied by the SBA system due to some communications or internal software error; data is being written to backup files.

- Remote busy (RBsy): indicates the stream has been busied by the SBA system due to some communications or internal software error; data is being written to backup files.

- Backup (Bkup): indicates the stream is writing data to backup files due to a performance problem.

- Recovery (Rcvy): indicates the stream is in service and also sending backup files previously created to the CS 2000 Core Manager.

- In-service (InSv): indicates the stream is in a normal working state.

- In-service trouble (ISTb): indicates that the CS 2000 Core Manager Communication is in service trouble due to being in a split-mode state.

Common procedures

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

- The procedure Verifying the file transfer protocol helps you determine that the FTP process is set up correctly and is able to transfer files.

- The procedure Verifying the FTP Schedule helps you determine that the system is able to send FTPs on a regular basis.

- The procedures "Configuring SLM disk drive backup volumes" and "Configuring DDU disk drive backup volumes" in the Accounting section, are used to create and activate alternative backup volumes for a stream.

The following procedures discuss how to clear alarms based on insufficient storage capacity:

- Clearing a BAK50 alarm
- Clearing a BAK70 alarm
- Clearing a BAK90 alarm
- Clearing a BAKUP alarm
- Clearing a NOBAK alarm
- Clearing a NOREC alarm
- Clearing a NOSTOR alarm
- Clearing a NOVOL alarm

Clearing 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 by typing

 # sdmmtc sys

and pressing the Enter key.

Example response:

```
 # Description                      Current / Threshold
 6    1 CPU (run queue entries):        0 /    5
 7    2 Number of Processes:           82 / 250
 8    3 Number of Zombies:              4 /    3 !
 9    4 Number of Swap Queue Entries:   0 /    2
10
```

3   Look for the current number of zombie processes.

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

Example:

In the response in step 1, 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.

4   Access the APPL level menu, by typing

 # appl

and pressing the Enter key.

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 by typing

 # bsy <application_number>

and pressing the Enter key.

where:

> **<application_number>** = 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 by typing

`# rts <application_number>`

and pressing the Enter key.

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 log reports

Application

Use this procedure to display the current logs raised by the CS 2000 Core Manager for the SuperNode Billing application (SBA) that have not been acknowledged by the Core. The MIB parameter "sendBillingLogsToCM" impacts the displogs command.

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

Prerequisites

None

Action

Displaying SBA logs

At any workstation or console

1   Log into the CS 2000 Core Manager using the root user ID and password.

2   Access the billing maintenance interface by typing

`# billmtc`

and pressing the Enter key.

3   Display the logs by typing

`> displogs`

and pressing the Enter key.

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

4   You have completed this procedure.

Displaying SBA alarms

Application

Use this procedure to display the current alarms raised by the CS 2000 Core Manager for the SuperNode Billing application (SBA). The MAP CI displays the status (critical, major, minor), the stream, and the text of the alarm.

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

Prerequisites

None

Action

Displaying SBA alarms

At any workstation or console

1   Log into the CS 2000 Core Manager using the root user ID and password.

2   Access the billing maintenance interface by typing

 # billmtc

and pressing the Enter key.

3   Display the alarms by typing

> dispal

and pressing the Enter key.

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.

Changing the set of logs sent from the CM

Application

Use this procedure to change the set of logs that will be sent from the Core to the CS 2000 Core Manager.

Action

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

Summary of changing the set of logs sent from the CM

```
┌──────────────────┐
│ Begin logroute   │
│                  │
└────────┬─────────┘
         │
         ▼
┌──────────────────┐
│ Change the       │
│ CM Config file   │
└────────┬─────────┘
```

This flowchart summarizes the procedure.

Use the instructions that follow this flowchart to perform the procedure.

Flowchart:

- Begin logroute
- Change the CM Config file
- Add an item? — N → unsuppress logs? — Y → Specify logs to unsuppress
  - unsuppress logs? — N → Specify logs to suppress
  - Add an item? — N → Delete an item?
    - Delete an item? — Y → Specify item to delete
    - Delete an item? — N → Return to main menu
- Return to main menu → Save changes → Quit logroute → Busy log delivery → RTS log delivery → End

Changing the set of logs sent from the CM

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Begin the logroute application by typing

    # logroute

    and pressing the Enter key.

    The Logroute Main Menu screen appears.

At the logroute application screen

3   Change a parameter in the logroute menu by typing

> **> c**

and pressing the Enter key.

Response:

```
Enter number of main menu option ==>
```

4   Define the CM Config File by typing

> **> 3**

and pressing the Enter key.

The CM Config File screen appears.

5   Use the following table to determine your next step.

If you want to	Do
add an item	step 6
delete an item	step 14

6   Add an item by typing

> **> a**

and pressing the Enter key.

Response:

```
a:addrep or d:delrep (or n for NOCMLOGS) ==>
```

7   Use the following table to determine your next step.

If you want to	Do
suppress logs	step 8
unsuppress logs	step 11

8   Add a routing entry that suppresses logs (causes them not to be routed to the CS 2000 Core Manager) by typing

> **> d**

and pressing the Enter key.

Response:

```
Enter log identifier ("log_type", or "log_type
log_number") ==>
```

9   Enter the log type or a combination of log type and log number and press the Enter key.

> *Note 1:* An example of a log type is "PM." This entry will suppress all logs of type PM.

> *Note 2:* An example of a combined log type and log number is "PM 181." This entry will suppress the PM181 log but leave all other PM logs unchanged.

10   Use the following table to determine your next step.

If you	Do
want to make additional entries	step 6
do not want to make additional entries	step 16

11   Add a routing entry that un-suppresses logs (causes them to be routed to the CS 2000 Core Manager) by typing

```
> a
```

and pressing the Enter key.

Response:

```
Enter log identifier ("log_type", or "log_type
log_number") ==>
```

12   Enter a log type or a combination of log type and log number and press the Enter key.

> *Note 1:* An example of a log type is "PM." This entry will unsuppress all logs of type PM.

> *Note 2:* An example of a combined log type and log number is "PM 181." This entry will unsuppress the PM181 log but leave the routing of other PM logs unchanged.

13   Use the following table to determine your next step.

If you	Do
want to make additional entries	step 6
do not want to make additional entries	step 16

14   Delete an item by typing

> **> d**

and pressing the Enter key.

Response:

```
Enter item to delete ==>
```

15   Enter the item number from the CM Config list that you want to delete, and press the Enter key.

16   Return to the main menu by typing

> **> m**

and pressing the Enter key.

17   Save the changes you have made by typing

> **> s**

and pressing the Enter key.

Response:

WARNING:

You must BSY and RTS the Log Delivery application

for the CM configuration to take effect.

18   Press the Enter key to continue.

19   Exit the Logroute application by typing

> **> q**

and pressing the Enter key.

20   Access the CS 2000 Core Manager maintenance interface by typing

> **# sdmmtc**

and pressing the Enter key.

21   Access the application level by typing

> **> appl**

and pressing the Enter key.

22   Busy the log delivery application by typing

`> bsy <n>`

and pressing the Enter key.

where

> *n*
>   is the number next to the log delivery application

23   Confirm the busy command by typing

`> y`

and pressing the Enter key.

The message "Command complete" appears on the screen output.

24   Return the log delivery application to service by typing

`> rts <n>`

and pressing the Enter key.

where

> *n*
>   is the number next to the log delivery application

Response:

```
Application RTS - Command submitted.
```

25   Exit the maintenance interface by typing

`> quit all`

and pressing the Enter key.

26   You have completed the procedure.

Cleaning the DAT drive

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

Application

To clean the DAT drive, use an appropriate DAT drive cleaning cartridge. Nortel recommends 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.

Nortel recommends that you clean the tape drive heads after the first 4 hours of tape movement of a new cartridge, and then after each 25 hours of use.

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.

DAT drive
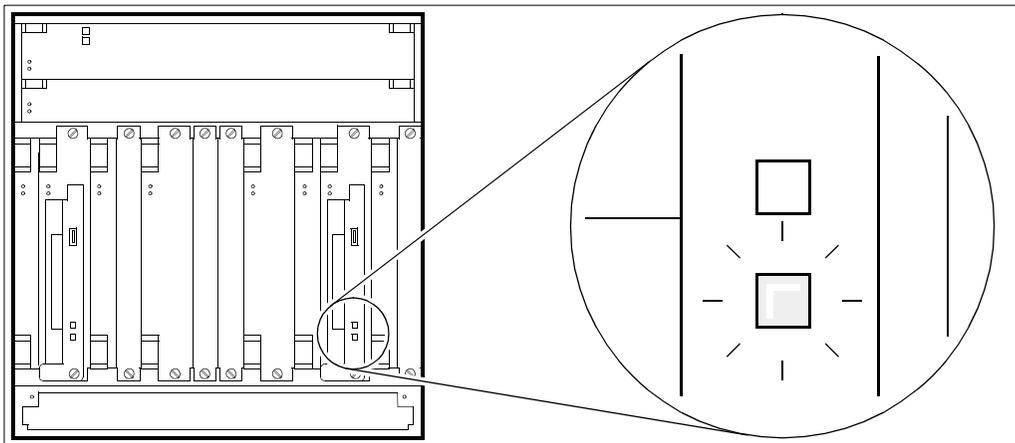
A solid green LED indicates that a tape is inserted with no errors. Slowly flashing green and amber LEDs indicates that a prerecorded audio cartridge is inserted and is being played automatically. A rapidly flashing green LED indicates that the drive cannot write to the tape correctly. Clean the DAT drive.

A solid amber LED indicates that the drive is reading or writing the tape. If the amber light flashes rapidly, 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

Get cleaning cartridge

↓

Eject tape from tape drive

↓

Insert cleaning tape

↓

Remove cleaning tape when complete

↓

Reinsert original tape if applicable

↓

End

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.
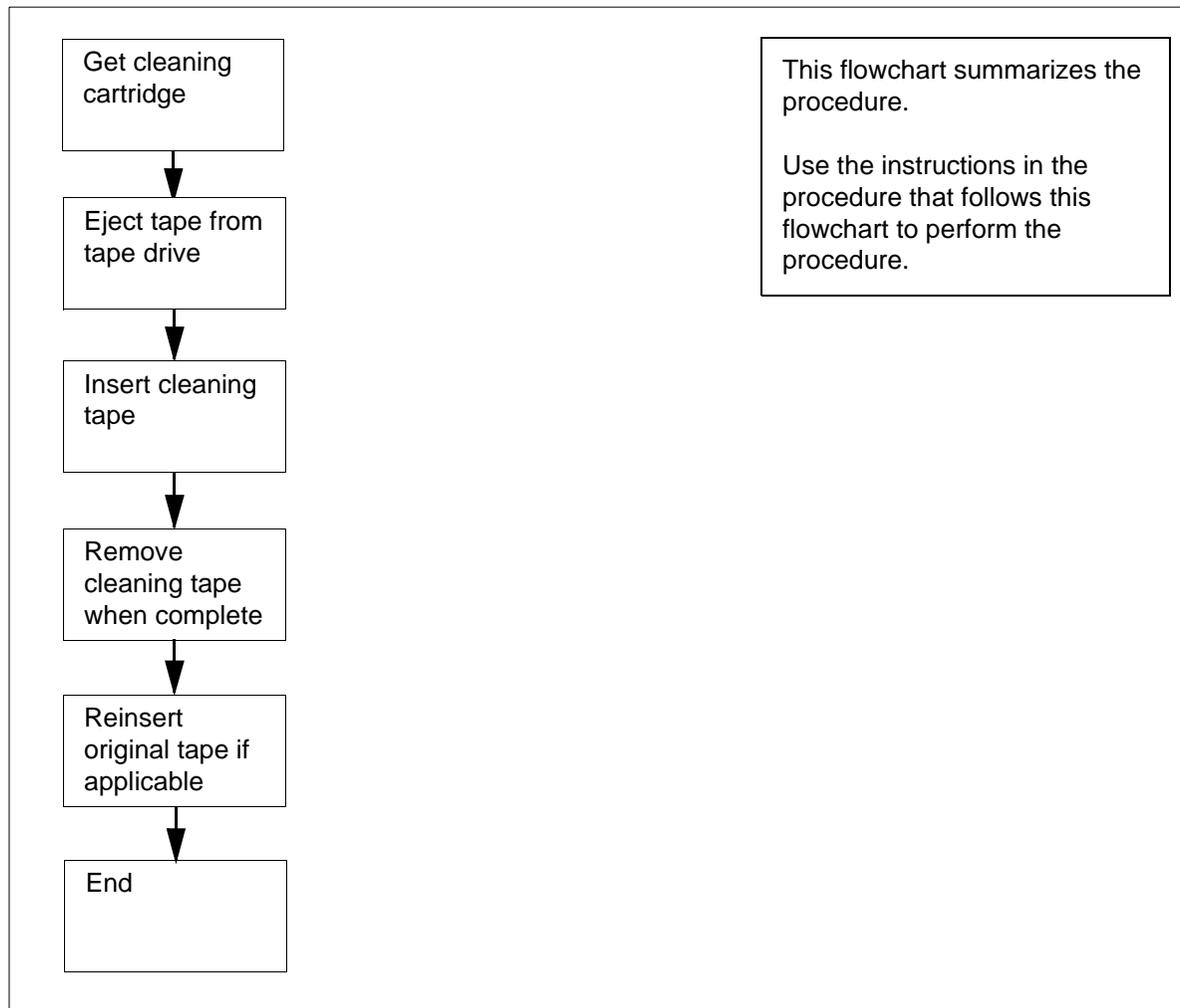
Cleaning the DAT drive

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 you removed in step 2.

6   You have completed this procedure.

Controlling the SDM Billing Application

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

Note: You must establish communications between the CS 2000 Core Manager and the Communication Server 2000 core for SBA to run successfully.

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Access the Application level by typing

 # sdmmtc appl

and pressing the Enter key.

> *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 SDM Billing Application by typing

> bsy <x>

and pressing the Enter key.

Where:

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

Response:

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

4 Confirm the busy command by typing

> y

and pressing the Enter key.

If the SBA	Do
busied successfully and you want to return the SBA to service	step 5
busied successfully but you do not want to return the SBA to service at this time	step 8
did not busy successfully	contact your next level of support

5   Return the SDM Billing Application to service by typing

    `> rts <x>`

    and pressing the Enter key.

    Where:

        `<x>`
          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 when a stream configured for RTB fails to return to service.

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

6   Use the following table to determine your next step.

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

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

    a Exit the Application level by typing

        `> quit all`

        and pressing the Enter key.

    b Access the billing maintenance level by typing

        `# billmtc`

        and pressing the Enter key.

    c Access the schedule level by typing

        `> schedule`

        and pressing the Enter key.

d Access the real-time billing level by typing

> **> rtb**

and pressing the Enter key.

e Busy the stream by typing

> **> bsy <stream name>**

and pressing the Enter key.

Where:

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

f Return the stream to service by typing

> **> rts <stream name>**

and pressing the Enter key.

Where:

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

If the billing stream configured for RTB	Do
returns to service successfully	step 8
does not return to service successfully	contact your next level of support

8 Return to the AIX prompt (#) by typing

> **> quit all**

and pressing the Enter key.

9 You have completed this procedure

Copying a snapshot file

Complete the following procedure to copy a snapshot file (snapshot.txt) to a new file.

Copying a snapshot file

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Copy the file by typing

`# cacf <source_file> <new_file>`

and press the Enter key.

where

<source_file> is the simple filename of the file to copy

<new_file> is the simple filename of the file to copy to

> *Note:* A simple filename does not contain the complete pathname of the file.

3   You have completed this procedure.

Deleting a device using logroute

Application

Use this procedure to delete a log device using the Log Delivery Application Commissioning Tool (Logroute). This procedure allows you to delete any one of the following devices:

- a TCP device (an IP and port address on the network)
- a TCP-IN device (a port on the CS 2000 Core Manager)
- a file device (a file on the CS 2000 Core Manager)

Action

The following flowchart provides a description of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of Deleting a device using Logroute

```
┌─────────────────┐
│  Begin logroute │
│                 │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Select the     │
│  device list    │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Delete devices │
│                 │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Save changes   │
│                 │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Quit logroute  │
│                 │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  End            │
│                 │
└─────────────────┘
```

This flowchart summarizes the procedure.

Use the instructions that follow this flowchart to perform the procedure.
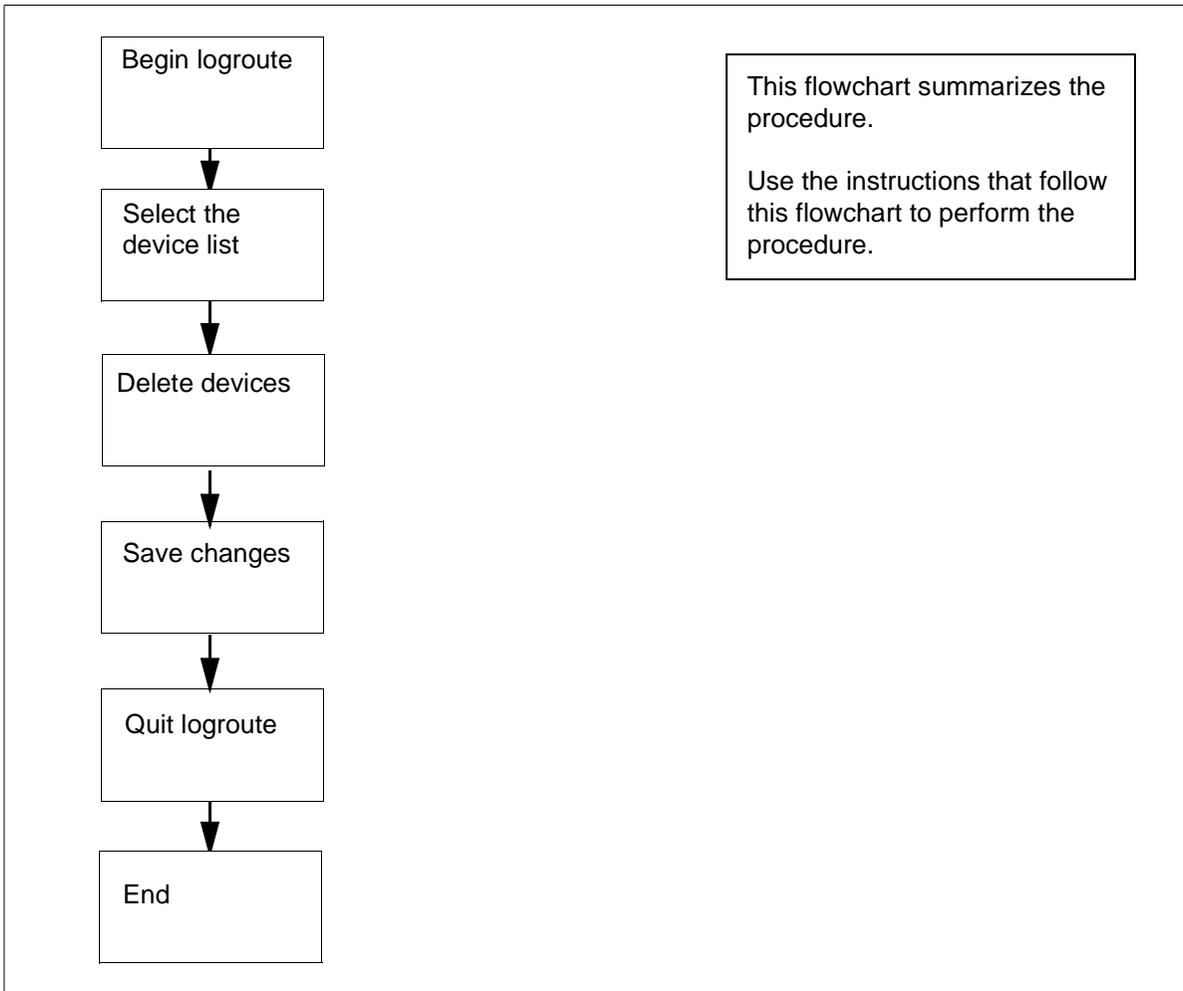
Deleting a device using Logroute

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Begin the logroute application by typing

 # logroute

and pressing the Enter key.

The Logroute Main Menu screen appears.

At the logroute application screen

3   Change the parameters of an item in the logroute menu by typing

`> c`

and pressing the Enter key.

Response:

`Enter number of main menu option ==>`

4   Display the device list by typing

`> 1`

and pressing the Enter key.

The Device List screen appears.

5   Delete a device by typing

`> d`

and pressing the Enter key.

Response:

`Enter device number to delete ==>`

6   Enter the number of the device you want to delete, and press the Enter key. Repeat from step 4 until all the devices you want to delete have been deleted from the list.

If you	Do
want to delete another device	step 5
do not want to delete another device	step 7

7   Return to the main menu by typing

`> m`

and pressing the Enter key.

8   Save the changes you have made by typing

`> s`

and pressing the Enter key.

Response:

`Save completed -- press return to continue`

9   Press the Enter key to continue.

10 Exit the Logroute application by typing

> **q**

and pressing the Enter key.

11 You have completed the procedure.

Disabling and enabling dcemonitor

Application

> **ATTENTION**
> This procedure must be performed by a trained Distributed
> Computing Environment (DCE) system administrator who knows
> DCE administration procedures.

When dcemonitor cannot solve a service-affecting DCE problem, it
attempts to solve the problem by killing the DCE daemons using
/etc/dce.clean, and restarting them using /etc/rc.dce. If this does not
solve the problem, dcemonitor waits 3 min., and repeats these
operations indefinitely.

The "DCE Monitor present action:" line in the dce_mon_status file will
be "restart" if dcemonitor is doing recovery by restarts. If dcemonitor
constantly kills DCE daemons, the DCE environment on the CS 2000
Core Manager becomes unstable. This can seriously impair your ability
to fix the problem.

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

Action

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

Summary of disabling and enabling dcemonitor

```
┌─────────────────┐
│ Log in to the CS│
│ 2000 Core Man-  │
│ ager.           │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Go to           │
│ dcemonitor      │
│ directory       │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Edit            │
│ suspension      │
│ control file    │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Change the      │
│ control word    │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Close the file  │
└─────────────────┘
        │
        ▼
   ╱─────────╲      Y   ┌──────────────┐
  ╱ Disabled  ╲─────────│ Dcemonitor   │
  ╲ dcemonitor? ╱       │ suspended for│
   ╲─────────╱          │ 1 hour       │
        │ N             └──────────────┘
        ▼
┌─────────────────┐
│ End             │
└─────────────────┘
```

This flowchart summarizes the procedure.

Use the instructions that follow this flowchart to perform the procedure.
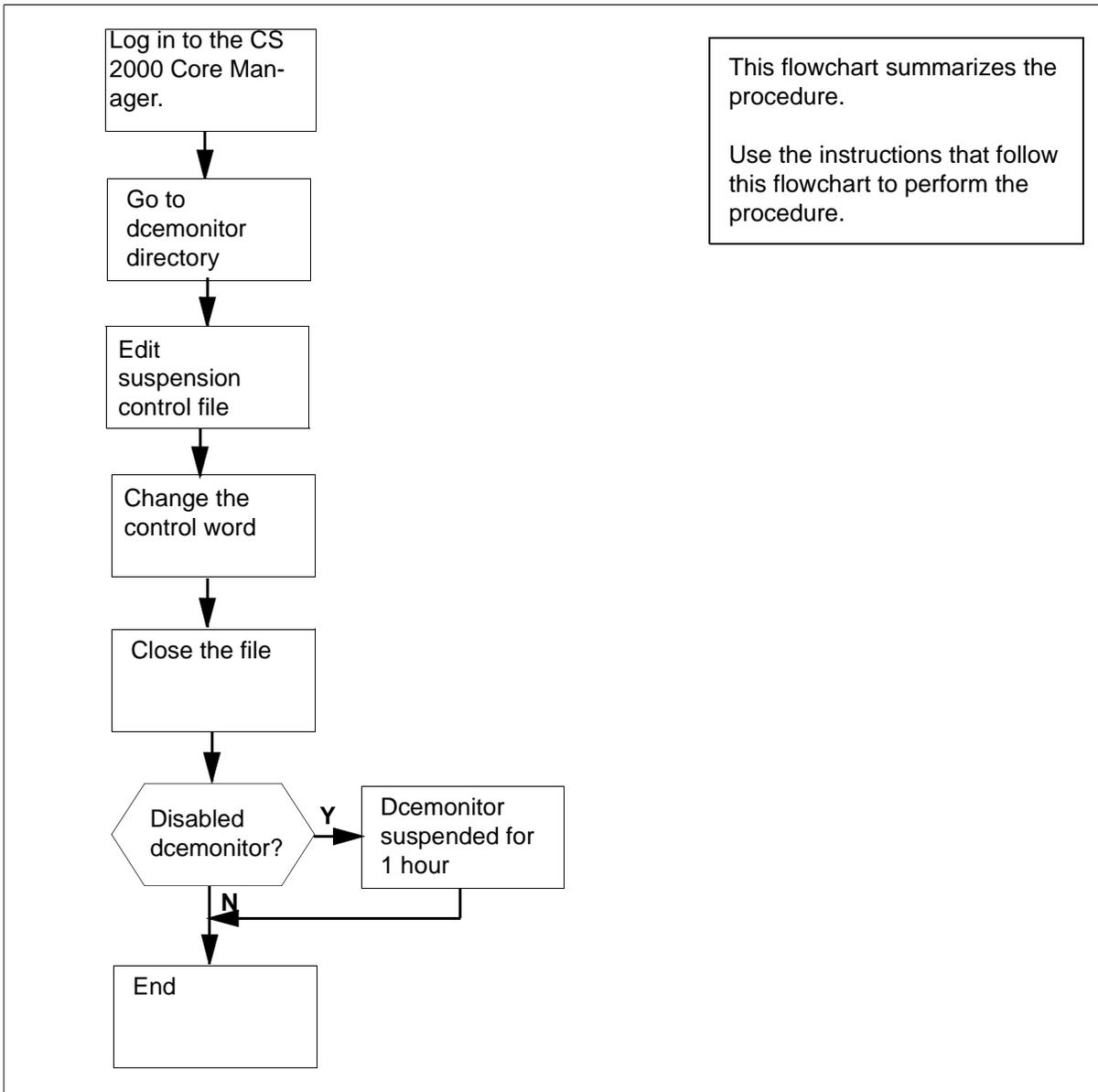
Disabling and enabling dcemonitor

At the local VT100 console or remote client workstation

1   Log in to the CS 2000 Core Manager as the root user.

2   Access the dcemonitor data directory by typing

`# cd /sdm/configdata/dce`

and pressing the Enter key.

3   Edit the dcemonitor suspension control file by typing

      `# vi dce_mon_suspend`

      and pressing the Enter key.

      This file contains one word.

4   Use the following table to determine your next step.

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

5   Modify the control word by typing

      `> cw`

      and pressing the Enter key.

      The word suspend is replaced by "suspen$".

6   Enable dcemonitor by typing the activation control word

      `> active`

      and pressing the Enter key.

      The $ from "suspen$" remains.

      Go to step 9.

7   Modify the control word by typing

      `> cw`

      and pressing the Enter key.

      The word active is replaced by "activ$".

8   Disable dcemonitor by typing

      `> suspend`

      and pressing the Enter key.

9   Close the file by pressing the Esc key and then typing

`>: wq`

and pressing the Enter key.

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

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

The command you enter to display or store log records on a workstation must include a port number. The port number must be the same as the port number used in configuring the TCP device on the CS 2000 Core Manager. The port number must not be used for any other purpose on the workstation, otherwise the following error message appears:

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

You must change the port number used in configuring the TCP device on the CS 2000 Core Manager.

Checking the port numbers in use on a workstation

At the client workstation

1 Check the port numbers in use by typing

more/etc/services

and pressing the Enter key.

You will see the list of port numbers in use on the display. Scroll through the display by pressing the Enter key again.

Storing logs in a file

At the client workstation

1 Start the logreceiver tool to store logs in a file by typing

logreceiver <port> -f <filename>

and pressing the Enter key.

where

<port> is the port number used when configuring the TCP device on the CS 2000 Core Manager

<filename> is the name of the file

> *Note 1:* If the file does not exist, it will be created automatically. The logs from the CS 2000 Core Manager will be stored in this file. If the file exists, the logs from the CS 2000 Core Manager will be added to it provided its UNIX access permissions allow writing to the file. In either case, a message

'`Accepted connection request from host xxx`' will be displayed on the screen just before the first log received is written to the file. Type "ctrl -c" and press the Enter key to terminate execution of the logreceiver tool.

Note 2: If the file exists, but its permissions do not allow writing to it, an error message '`Failed to open filename`' displays on the screen. Type "control -c" and press the Enter key to terminate execution of the logreceiver tool.

Note 3: 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.

Displaying log records on a workstation

At the client workstation

1   Start the logreceiver tool to display the log records on the screen by typing

`logreceiver <port>`

and pressing the Enter key.

where

<port> is the port number used when configuring the TCP device on the CS 2000 Core Manager

2   You have completed this procedure.

Listing snapshot files

Complete the following procedure to list all snapshot files on the CS 2000 Core Manager.

Listing snapshot files

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   List the files by typing

 # lsacf

and pressing the Enter key.

The CS 2000 Core Manager displays all snapshot files on the CS 2000 Core Manager.

Example response:

```
snapshot.txt          090499ac.txt      090599ac.txt
maint:
```

3   You have completed this procedure.

Logging a session to an output file

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

Logging a session to an output file

At your work station

1   Use the ETA client application to access the CS 2000 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 filename dialog appears.

Set a log file name

Filter

/bnr/users/guest/tmp/ETAlog.*

Directories

.

..

.endoscope

Files

ETAlog.12021448
ETAlog.12021503
ETAlog.12021523
ETAlog.12031226
ETAlog.new

Selection

/bnr/users/guest/tmp/ETAlog.12040849

[OK]   [Filter]   [Cancel]
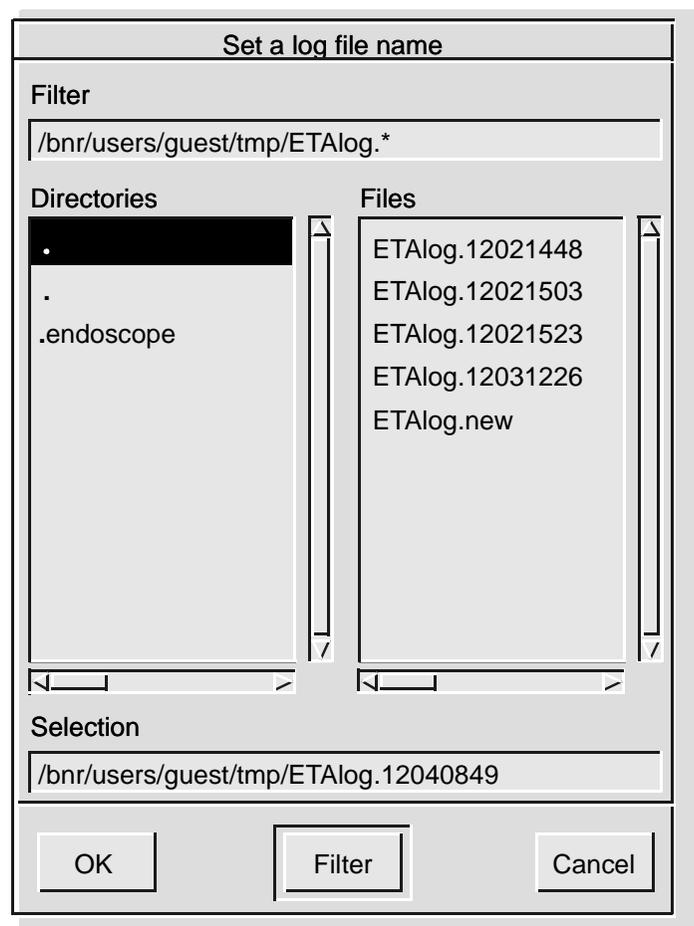
> **Note:** *You are prompted for the file name. Nortel Networks
> recommends that you accept the default file name in the
> current directory. Delete the files in the current directory that*

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 4
specify a new file name	step 5

3   Select the default file name by clicking on 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).

Go to step 6.

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

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

Go to step 6.

5   Type 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 backspace to erase.

6 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 7
do not want to save a current view of the RMI or MAP display	step 9

7 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

Filter

/bnr/users/guest/tmp/Attempt.*

Directories   Files

.   ETAmap.12021545
.   ETAmap.12031031
.endoscope

Selection

/bnr/users/guest/tmp/ETAmap.12040919

| OK | Filter | Cancel |
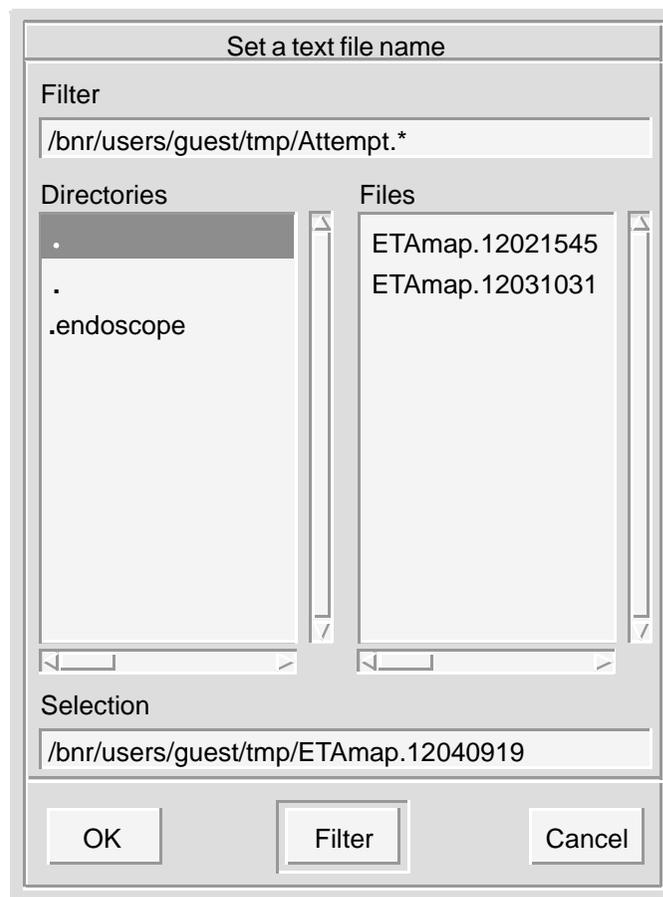
8   Select the default file name in the current directory by clicking on OK.

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

9   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.

10   Close the current ETA session window.

If	Do
a CS 2000 Core Manager session	step 11.
you are in a CI/MAP session	step 12

11   Exit the CS 2000 Core Manager session by typing

 # exit

12   Exit the CI/MAP session by typing

> logout

13   You have completed this procedure.

Performing a full restore of the software from S-tape

Application

> **ATTENTION**
> You must be a trained AIX system administrator who has root user privileges to the CS 2000 Core Manager to perform this procedure.

> **ATTENTION**
> You must mirror all volume groups on the CS 2000 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), Nortel Networks recommends that you use tape drive DAT0 to perform this procedure.

Use this procedure to perform a full restore of the CS 2000 Core Manager software load from the system image backup tape (S-tape).

You must be a root user at a local VT100 console to perform this procedure.

Interval

Perform this procedure when the CS 2000 Core Manager is out-of-service because the software load has become corrupted.

Action

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

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

This flowchart summarizes the procedure.

Log in to the CS 2000 Core Manager.

↓

Access the maintenance interface

↓

Is the maintenance interface available? — **N** → Insert the S-tape

Y ↓

Go to the Admin level and use the restore command

↓

Insert the S-tape and start reboot

↓ 1

Insert the S-tape

↓

Boot the system and disrupt the boot procedure

↓

Enter system diagnostics mode

↓ 1

1 →

Change the settings, if required

↓

Restore the system image from S-tape

↓

Remove the S-tape

↓

Log in to the CS 2000 Core Manager.

↓

Verify that disk mirroring is complete

↓ 2

2 →

Check the DCE state

↓

Check the state of the application(s)

↓

Perform DCE procedures, as required

↓

Access the backup and restore utility

↓

Create a new system image backup tape

↓

End

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 root user.

2   Access the maintenance interface by typing

     `# sdmmtc`

     and pressing the Enter key.

3   Use the following table to determine your next step.

If	Do
CS 2000 Core Manager maintenance interface is available	step 4
CS 2000 Core Manager maintenance interface is not available	step 10

4   Access the administration (Admin) level by typing

     `> admin`

     and pressing the Enter key.

5   Perform a full restore of the CS 2000 Core Manager by typing

     `> restore`

     and pressing the Enter key.

     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   Use the following table to determine your next step.

If	Do
you want to use the tape drive in slot 2	type 0, and press Enter
you want to use the tape drive in slot 13	type 1, and press Enter

7   When prompted, confirm that you want to proceed by typing

> `> y`

and pressing the Enter key.

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 CS 2000 Core Manager from the selected tape drive.

At the CS 2000 Core Manager

10   Ensure that one of the CS 2000 Core Manager tape drives (slot 2 or 13 in the main chassis) contains the system image backup tape (S-tape).

   Note: Nortel Networks recommends that you 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 CS 2000 Core Manager. If the prompt is available at a local VT100 console, reboot the CS 2000 Core Manager by typing

`# shutdown -Fr`

and pressing the Enter key.

If the prompt is not available, reboot the CS 2000 Core Manager by turning the power off, then on, using the MSP breaker that supplies power to the CS 2000 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 min. 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" by typing

> 3

and pressing the Enter key.

Go to step 16.

15   Switch the directory to FX-Bug, by typing

> **sd**

and pressing the Enter key.

16 View the input/output devices on the CS 2000 Core Manager to verify the address of the tape drive from the FX-Bug prompt. Type

Fx-Bug> ioi

and press the Enter key.

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 end up at the FX-Bug prompt, then continue with this step. Otherwise, go to .

Fx-Bug> pboot <address for Archive Python>

and press the Enter key.

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 min. until the system completes the reboot. The system asks 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 "1" on the screen.

Type1 to select the language setting, and press the Enter key. The Welcome to Base Operating System Installation and Maintenance menu is then displayed.

19   Select "Change/Show Installation Settings and Install" by typing

`> 2`

and pressing the Enter key. 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:* "..." shown under Current Choice(s) indicates that more than one disk is currently in use.

20   The default disk for the installation is hdisk0 which is located in slot 2 of the main chassis. If your CS 2000 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 21
you want to use the current settings	step 24

21 Change the disks where you want to install the backup image by typing

> **> 1**

and pressing the Enter key.

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 >>>.

> *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 21 are hdisk0 and hdisk5. The rootvg disks for installation should have location codes c1-f2-00-0 for domain 0, and c1-f13-00-0 for domain 1.

22 To select a disk or disks, enter the number of the disk, and press the Enter key. To deselect a selected disk, enter its number again and press the Enter key.

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

> **0**

and press the Enter key. Go to step .

24 Accept the current settings by typing

> **0**

and pressing the Enter key.

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: As part of the restore process, the system reboots automatically and displays the login prompt.

At the CS 2000 Core Manager

25 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

26 Log in to the CS 2000 Core Manager as a root user. Press the Enter key when you see the "TERM=(vt100)" prompt.

27 Start the CS 2000 Core Manager maintenance interface by typing

 # sdmmtc

and pressing the Enter key.

28 Access the storage level by typing

> **> storage**

and pressing the Enter key.

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
```

29 Use the following table to determine your next step.

If the disks are	Do
Mirrored	step 31
Integrating or Not Mirrored	step 30

30 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.

31 Access the LAN level by typing

> **> lan**

and pressing the Enter key.

Check the state of DCE.

Example response:

```
DCE State: SysB
```

32   Access the application (APPL) level to check the state of any DCE-based applications by typing

```
> 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
```

33   DCE and DCE-based applications may 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 31), and the logs displayed indicate an error with the security client service in DCE, restore the service by performing the following procedures:

- "Removing a CS 2000 Core Manager from a DCE cell" under Configuration

- "Configuring a CS 2000 Core Manager in a DCE cell" under Configuration

If some DCE-based applications are faulty (Fail state, see step 32), try to restore them by BSYing and RTSing the applications from the SDM APPL level (see step 32). If this approach fails, restore them by performing the procedure to add the application server to the DCE cell. Use the procedure in this document that is specific to each application.

34   You must create a new system image backup tape. Refer to the procedure "Creating system image backup tapes (S-Tapes)" in the Security and Administration section.

35   You have completed this procedure.

Performing a partial restore of the software from S-tape

Application

> **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 CS 2000 Core Manager software.

> **ATTENTION**
> This procedure must be performed by a trained AIX system administrator who has root user privileges to access the CS 2000 Core Manager.

> **ATTENTION**
> All volume groups on the CS 2000 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), Nortel recommends that you use tape drive DAT0 to perform this procedure.

Use this procedure to restore individual files or sets of files from the system image backup tape (S-tape). This procedure can be performed by the root user from a local or remote terminal.

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 task.

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

Log in to the CS 2000 Core Manager.

↓

Verify that disk mirroring is Mirrored

↓

Access the backup and restore utility

↓

List the contents of the S-tape, if required

↓

Select the tape drive

↓

Restore files or directories as appropriate

↓

1

Successful? — **N** → Contact your next level of support

| **Y**

View the s-tape.restore file? — **N** → List the S-tape? — **N** → Remove the S-tape → End

Y
2

Y
3

2

Exit the maintenance interface

↓

View the s-tape.restore file

↓

1

This flowchart summarizes the procedure.

Use the instructions that follow this flowchart to perform the procedure.

3

List the contents of the S-tape

↓

Select the tape drive

↓

Insert the DAT tape

↓

1

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

At the local or remote console

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

2   Access the maintenance interface by typing

       # sdmmtc

       and pressing the Enter key.

3   Access the storage level by typing

       > storage

       and pressing the Enter key.

       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   Use the following table to determine your next step.

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

5   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 by typing

> **admin**

and pressing the Enter key.

7   Access the System Image Backup and Restore Menu by typing

> **backup**

and pressing the Enter key.

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

If you	Do
wish to list the S-tape	step 9
do not wish to list the S-tape	step 18

9   From the System Image Backup and Restore Menu, select "List Contents of the System Image Tape (S-tape)" by typing

> **3**

and pressing the Enter key.

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

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:*** *Nortel recommends that you 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, type "y" and press the Enter key. If you do not wish to use DAT1, type "n" and press the Enter key. 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 CS 2000 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, type

> **y**

and press the Enter key.

15   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.

Response:

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

16   Return to the System Image Backup and Restore Menu by typing

> **y**

and pressing the Enter key.

17   Use the following table to determine your next step.

If you are listing the contents of the tape to verify	Do
that the file has been restored	step 26
the file name or directory that you wish to restore	step 18

18   From the System Image Backup and Restore Menu, select "Restore Files from the System Image Tape (S-tape)" by typing

```
> 4
```

and pressing the Enter key.

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

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: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

20   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 tape drive 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, type "y" and press the Enter key. If you do not wish to use DAT1, type "n" and press the Enter key. The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

21   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

CS 2000 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.

Response:

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

22 Continue this procedure, by typing

```
> y
```

and pressing the Enter key.

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.

==>
```

23 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. A log file /tmp/s-tape.restore is created when the restore is completed.

> *Note:* An error message is displayed if the restore is unsuccessful. If this occurs, go to step <u>26</u>.

24 During the restore process, the screen will 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.

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.

25 Return to the System Image Backup and Restore Menu by typing

> **y**

and pressing the Enter key.

26 Determine if the restore was successful. The system displays the file that you have restored, as described in step 24. 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 27
you wish to list the S-tape	step 9

27 Exit the System Image Backup and Restore Menu, by typing

> **0**

and pressing the Enter key.

28 Exit the maintenance interface by typing

> **quit all**

and pressing the Enter key.

29 Access the s-tape.restore file by typing

cd /tmp

at the prompt and pressing the Enter key.

30 Scroll through the file by typing

more s-tape.restore

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

31   Use the following table to determine your next step.

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

32   Exit the System Image Backup and Restore Menu, by typing

> 0

and pressing the Enter key.

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

At the CS 2000 Core Manager

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

Go to step 34.

34   You have completed this procedure.

Purging snapshot files

Complete the following procedure to purge all snapshot files from the CS 2000 Core Manager.

Purging snapshot files

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Purge all files by typing

   # pgacf

   and pressing the Enter key.

3   The CS 2000 Core Manager displays the prompt.

4   You have completed this procedure.

Recovering a standalone X.25 SYNC personality module

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

Log into the CS 2000 Core Manager.

↓

Apply the X.25 software if required.

↓

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

↓

Verify the X.25 SYNC module is in a "should_be_on" state.

↓

Return the X.25 SYNC module to a usable state.

↓

End

This flowchart summarizes the following procedure.

To complete the procedure, use the step-action procedure that follows the flowchart.
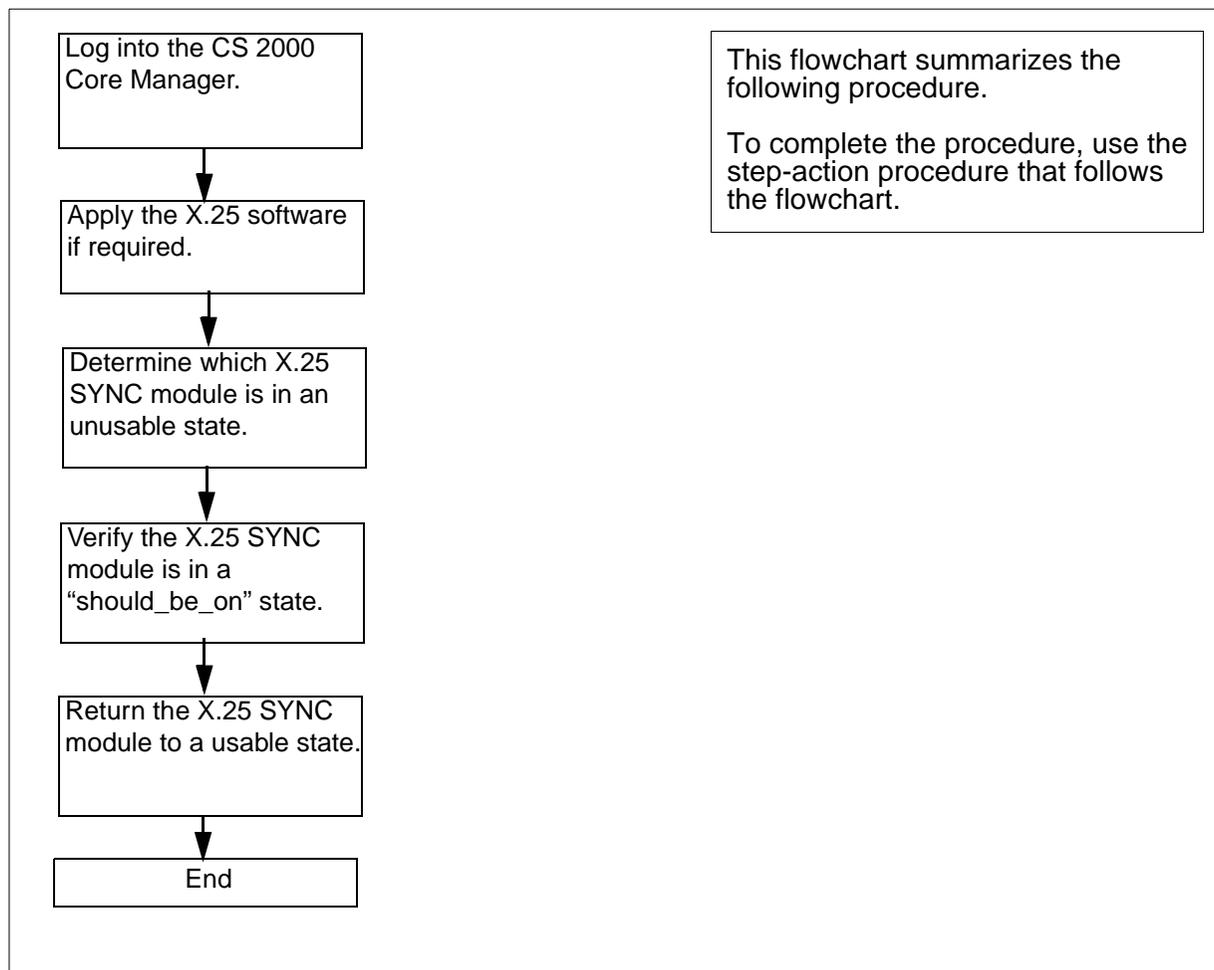
Recovering a standalone X.25 SYNC personality module

At the local or remote VT100 console

1   Log into the CS 2000 Core Manager.

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

`# lsstate -s | grep SYNC-`

and pressing the Enter key

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 by typing

`# lsmod -D1 SYNC-0`

and pressing the Enter key

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 by typing

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

and pressing the Enter key

where

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

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

120

Recovering backup files from lost backup volumes

Application

You need to recover backup files from lost backup volumes if the SBA becomes unaware of backed up files when the SWACT and RESTART processes occur when you are performing procedure "Configuring SBA backup volumes" in the Accounting section.

The following procedure swaps back old volumes as the primary backup volumes.

Before starting the procedure, you need

- the names of the swapped out volumes
- to have performed "Configuring SBA backup volumes" in the Accounting section, at which point, the SBA completed its recovery of the volumes from the backup volumes you configured during these procedures.

Action

Recovering backup files from lost backup volumes

At the MAP

1   Post the billing stream by typing

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

     and pressing the Enter key.

     Where

     <x> is the name of the billing stream.

2   Quit back to the appl;sdmbil level by typing

     > **quit**

     and pressing the Enter key.

3   Confirm that the names of the billing stream's existing backup volumes are the swapped in volumes you created earlier by typing

> **`> conf view <x>`**

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

4   Reference the notes you made when you performed "Configuring SBA backup volumes" in the Accounting section, to confirm that the backup volumes are the backup volumes you created during these procedures.

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

If the backup volume names are	Do
the names you setup when you performed procedure "Configuring SBA backup volumes" in the Accounting section	continue with step 6
not the names you setup when you performed procedure "Configuring SBA backup volumes" in the Accounting section	determine if someone else reconfigured the backup volumes before you continue with step 6

6   Configure the billing stream of the logical volumes you created when you performed procedure "Configuring SBA backup

volumes" in the Accounting section, once you receive confirmation that the files are successfully created by typing

> **`conf set <x> <y> <z>`**

and pressing the Enter key.

Where

<x> is the name of the stream, <y> is the dms_backup_1 volume, and <z> is the dms_backup_2 volume.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

7   Quit back to the command prompt by typing

> **`quit all`**

and pressing the Enter key.

> *Note 1:* The non-empty backup volumes are automatically detected by the SBA audits. In addition, the SBA places the billing stream into recovery mode and the volumes from the original backup volumes are sent to the CS 2000 Core Manager.

> *Note 2:* You must alert all operating company personnel who are associated with the DMS switch as to the names of the old and new backup volumes and the procedure you used to swap the volumes. These same personnel must be made aware of that any RESTARTs or SWACTs that occur before the billing stream returns to normal mode can cause a serious loss of billing records.

8   You have completed this procedure.

Removing a snapshot file

Complete the following procedure to remove a snapshot file from the CS 2000 Core Manager.

Removing a snapshot file

At any workstation or console

1 Log in to the CS 2000 Core Manager.

2 Remove the file by typing

 # racf <file>

and pressing the Enter key.

where

<file> is the simple filename of the file to remove

> *Note:* A simple filename does not contain the complete pathname of the file.

The CS 2000 Core Manager displays the prompt.

3 You have completed this procedure.

Replacing an MFIO/UMFIO LAN personality module

Application

Use the following procedure to replace either a Multifunction Input/Output (MFIO) LAN personality module or an Ultra-Multifunction Input/Output (UMFIO) LAN personality module, located at the rear of the main chassis and the I/O expansion chassis in a fault-tolerant CS 2000 Core Manager.

Nortel PEC	Name
NTRX50FS	MFIO LAN personality module
NTRX50NK/NTRX50NN	UMFIO LAN personality module

Note: Each I/O controller module must have an associated LAN personality module (NTRX50FS or NTRX50NK/NTRX50NN) installed at the back of the CS 2000 Core Manager.

Action

The following flowchart is only 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

Obtain the replacement module

↓

Log in to the CS 2000 Core Manager.

↓

Access the hardware level.

↓

Determine the location of the hardware

↓

Access the system level.

↓

Determine the status of disk mirroring

↓

Allow reintegration, if required

↓

Access the hardware level.

↓ 1

1 ↓

Manually busy the appropriate I/O module

↓

Unseat the I/O controller module

↓

Disconnect the ethernet cable if required

↓

Remove the LAN module to be replaced

↓

Replace the MFIO / UMFIO LAN module

↓

Reconnect the ethernet cable if required

↓

Seat the I/O controller module

↓

Return the I/O controller module to service → End

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

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 written at the top of the module.

At the local or remote VT100 console

2   Log into the CS 2000 Core Manager as the root or maint user.

3   Access the maintenance interface by typing

`# sdmmtc`

and pressing the Enter key.

4   Access the hardware (Hw) level by typing

`> hw`

and pressing the Enter key.

5   Display the hardware location information for the CS 2000 Core Manager by typing

`> locate`

and pressing the Enter key.

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 get 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
NTRX50FS BACK
```

7   Access the storage level by typing

> **storage**

and pressing the Enter key.

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.

9   Use the following table to determine your next step.

If disk mirroring is in the	Do
Integrating state	step 10
Mirrored or Not Mirrored state	step 11

10

	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 min. for each Gbyte. The actual time required varies upwards or downwards depending on the amount of data in the volume group, and the current processor load.

Go to step 8.

11   Access the hardware (Hw) level by typing

> **hw**

and pressing the Enter key.

12 Busy the I/O controller module associated with the MFIO or UMFIO LAN personality module you want to replace by typing

> **> bsy <*n*> eth**

and pressing the Enter key.

where

> *n*
> 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

- 0 if the module is located in slot 2 of the main chassis

- 1 if the module is located in slot 13 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

> **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")
```

13 Confirm the busy command by typing

> **> y**

and pressing the Enter key.

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 CS 2000 Core Manager

14

> **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.

15

> **CAUTION**
> **Potential service interruption**
> Unseat only the I/O controller module that you busied in step 12, and not the corresponding I/O controller module in the other I/O domain. The in-service LED on the module busied in step 12 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 the captive type, and cannot be removed from the module.

16 Depress the tip of the locking lever on the face of the I/O controller module.
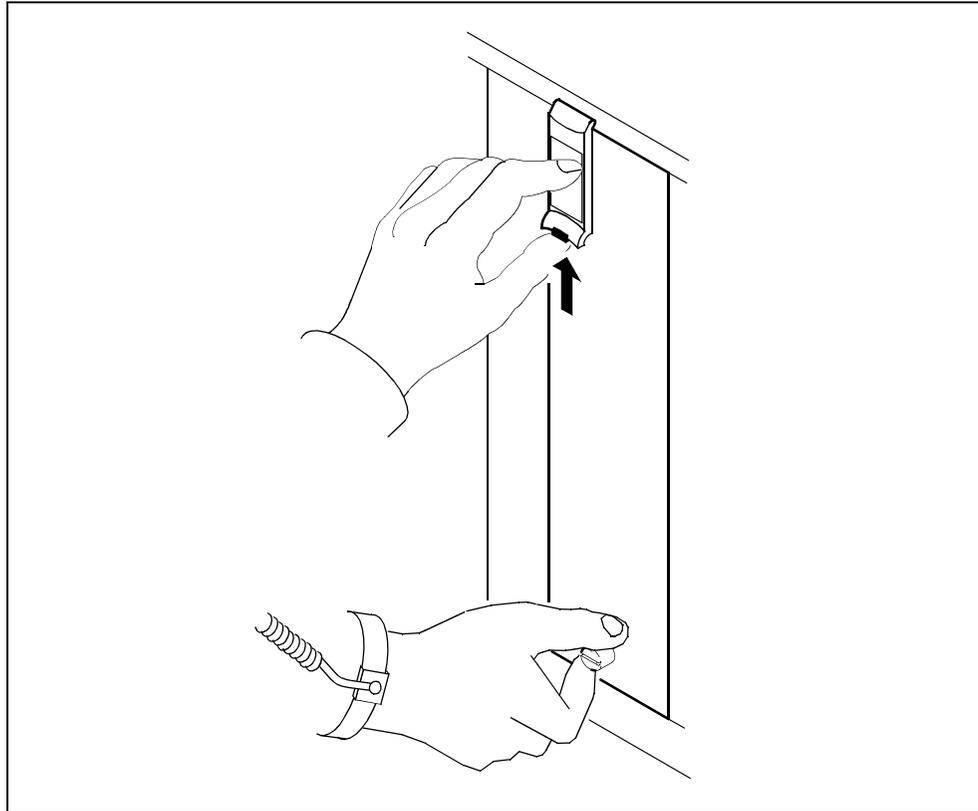
17   Open the locking lever on the face of the module by moving the lever outwards.
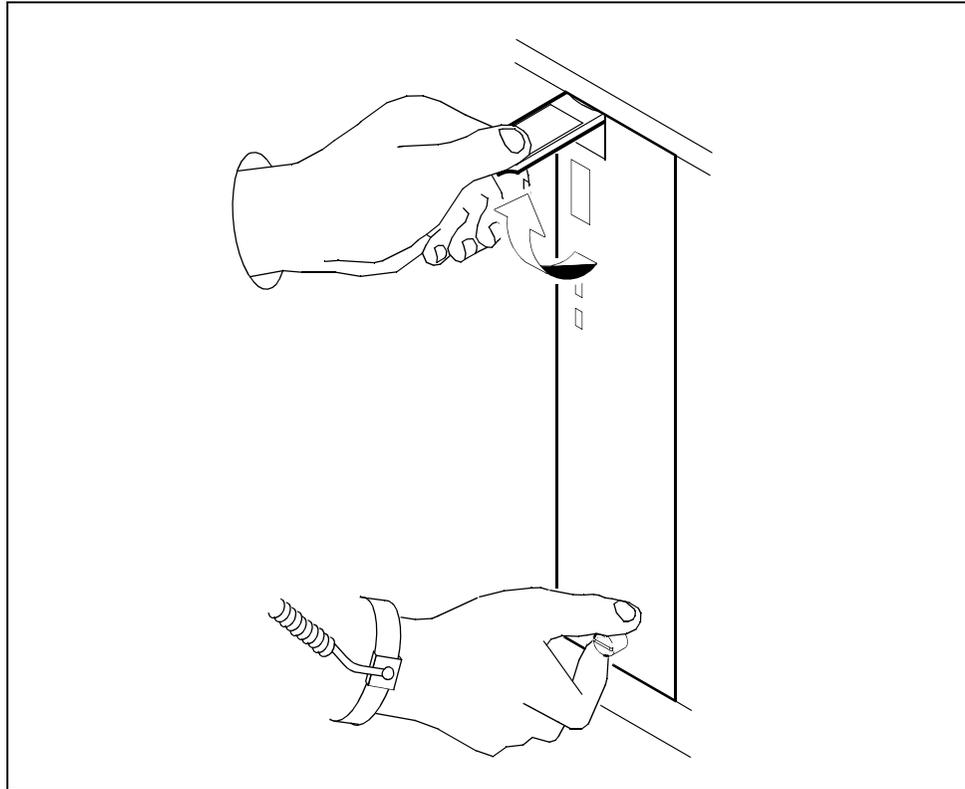
At the back of the CS 2000 Core Manager

18   Label the ethernet cable connected to the LAN personality module you want to replace.

19 Disconnect the ethernet cable, as shown in the following diagram.
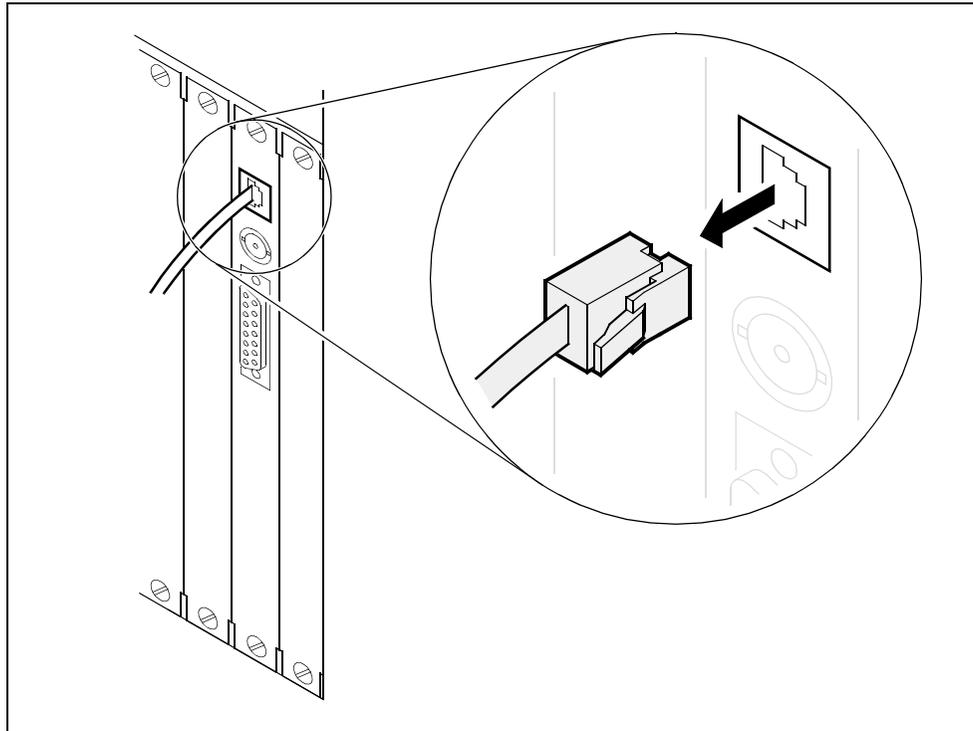
20 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module.

> *Note:* The thumbscrews are the captive type, and cannot be removed from the module.

21 While grasping the thumbscrews, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the CS 2000 Core Manager shelf.
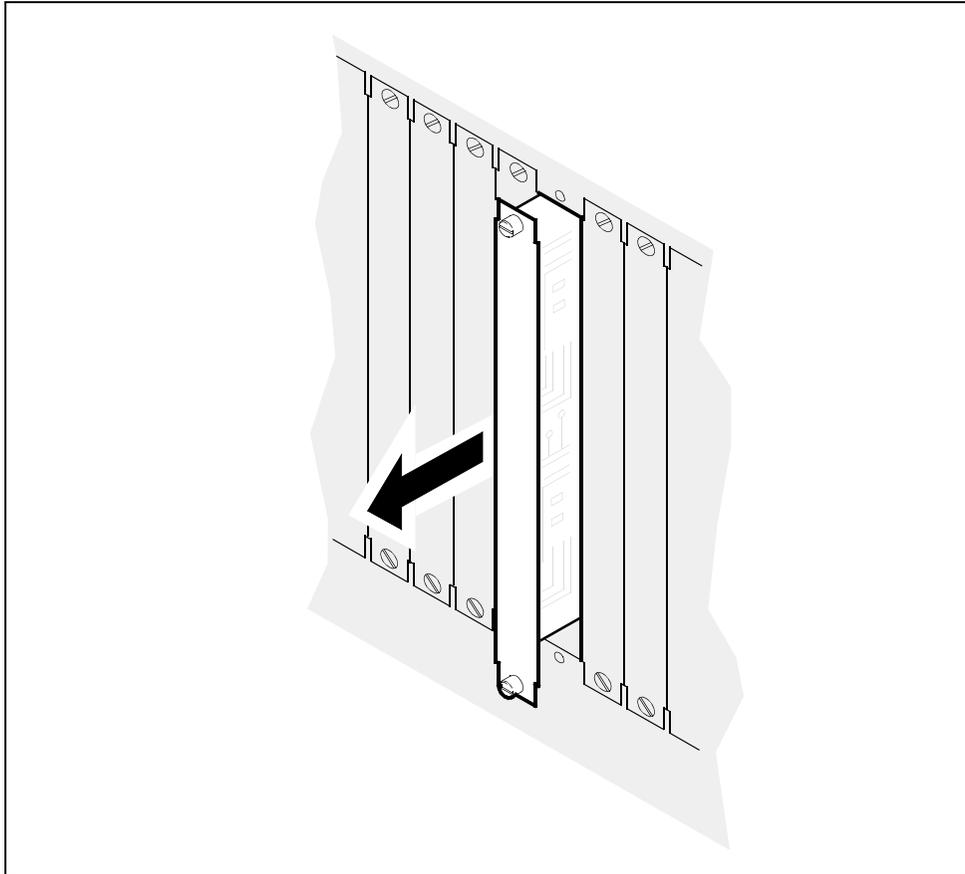
22   Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.
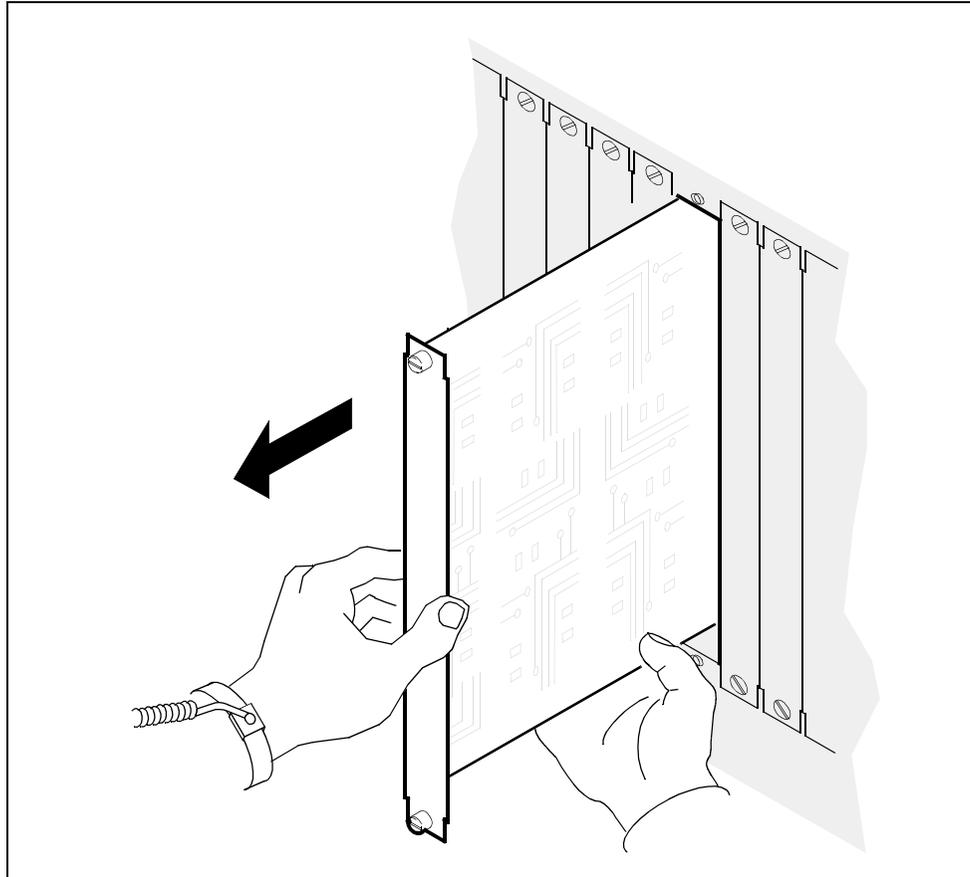
23   Place the module you have removed in an ESD protective container.

24   Insert the replacement MFIO or UMFIO LAN personality module into the CS 2000 Core Manager shelf.

25 Gently slide the module into the shelf until it is fully inserted.
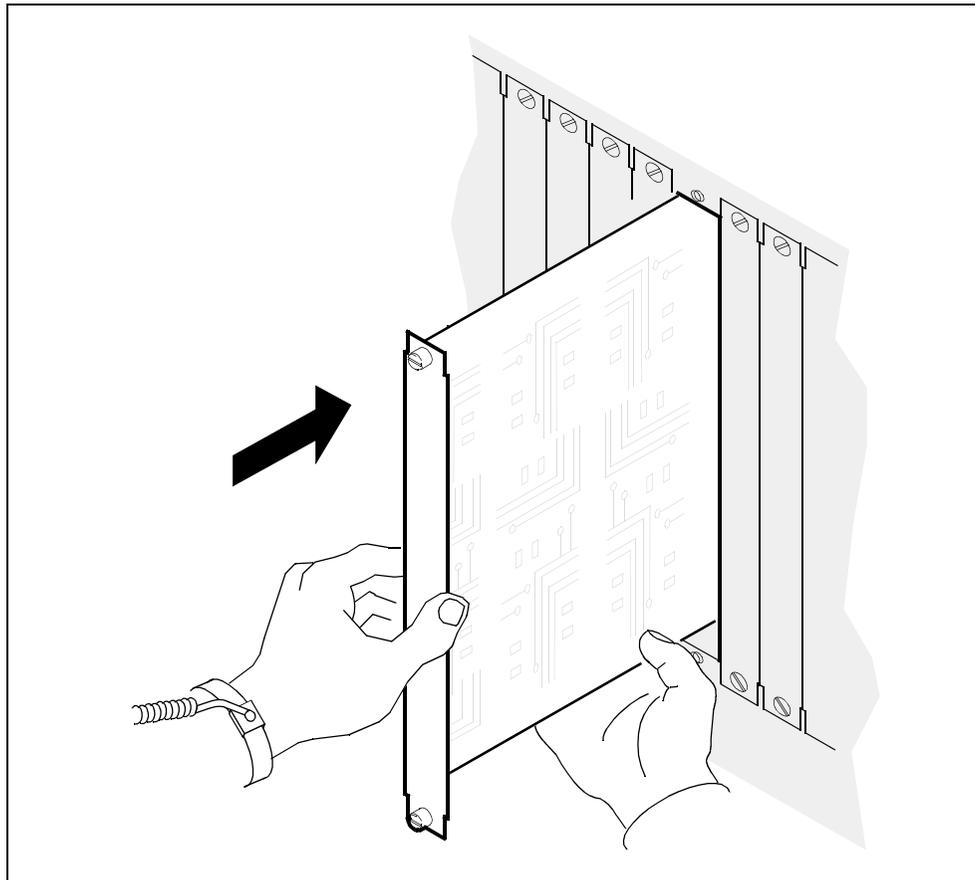
26 Tighten the thumbscrews at the top and the bottom of the module.

27 Reconnect the ethernet cable to the module. If you want, remove the label that you put on the cable in step 18.
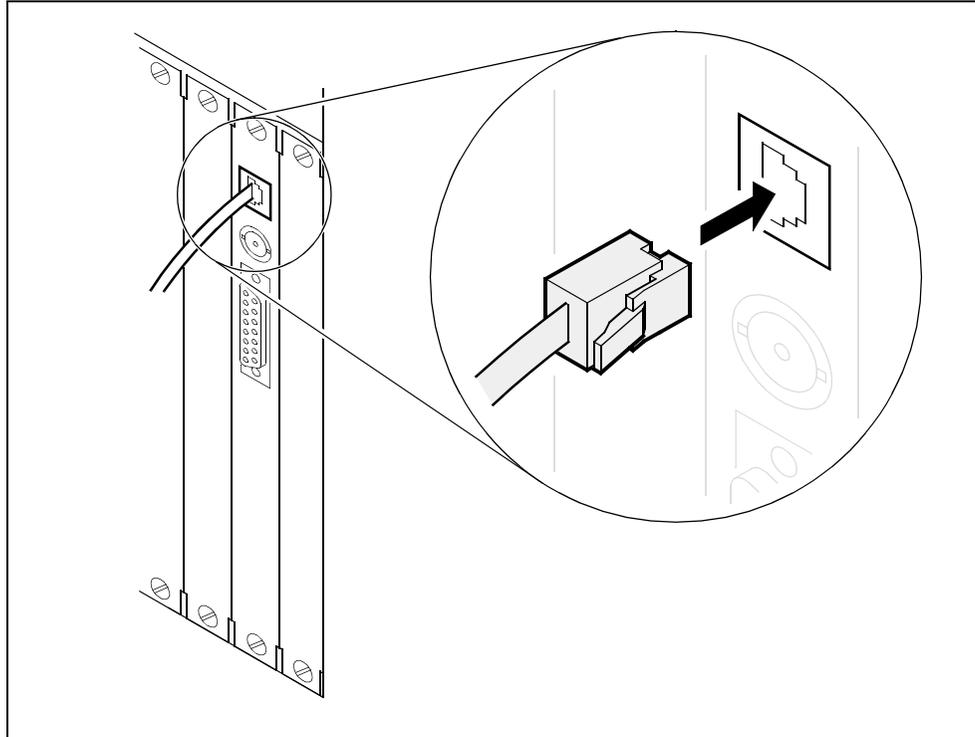
At the front of the CS 2000 Core Manager

28 Close the locking lever to secure the I/O controller module you unseated in step 15. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.

Micro switch
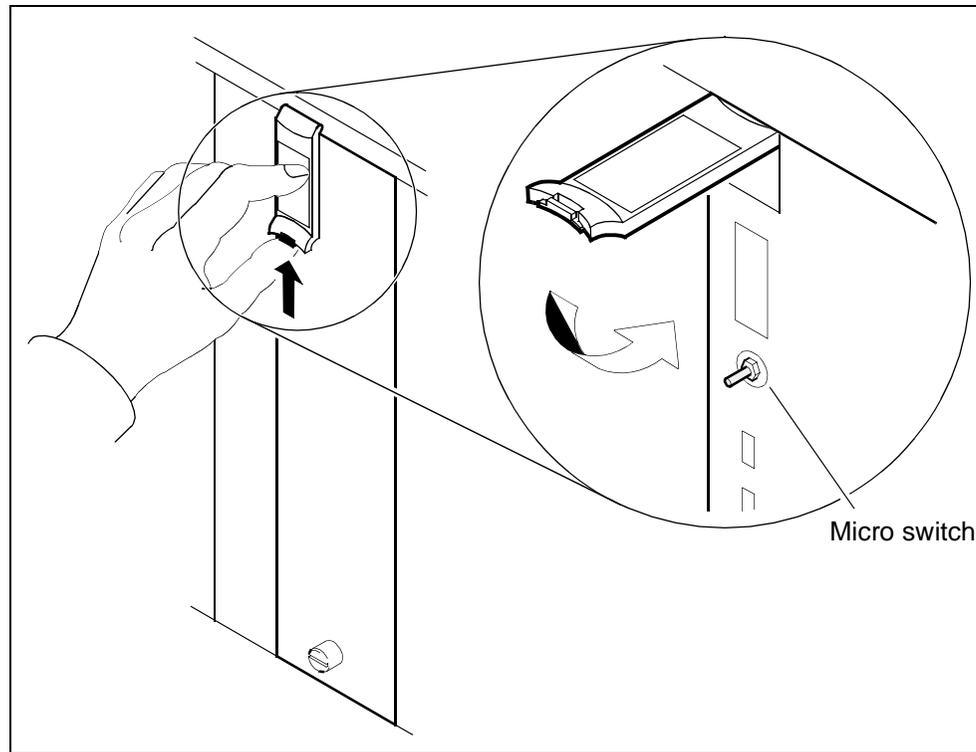
29 Tighten the thumbscrews on the I/O controller module.

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, is receiving power, and has 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

30 Return the I/O controller module to service by typing

```
> rts <n> eth
```

and press the Enter key.

where

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

eth
is the ethernet number 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.

31 You have completed this procedure.

Replacing a fan tray

Application

Use this procedure to replace a fan tray located at the front of the main and I/O expansion chassis of the CS 2000 Core Manager.

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 only 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 the      │
│ replacement     │
│ module          │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Log in to the CS│
│ 2000 Core Man-  │
│ ager.           │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Access the      │
│ hardware level. │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Manually busy   │
│ the fan tray to │
│ be replaced     │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Remove the      │
│ fan tray to be  │
│ replaced        │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Replace the     │
│ fan tray        │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ Return the fan  │
│ tray to service │
└─────────────────┘
        │
        ▼
┌─────────────────┐
│ End             │
└─────────────────┘
```

> This flowchart summarizes the procedure.
>
> Use the instructions in the procedure that follows this flowchart to perform the procedure.
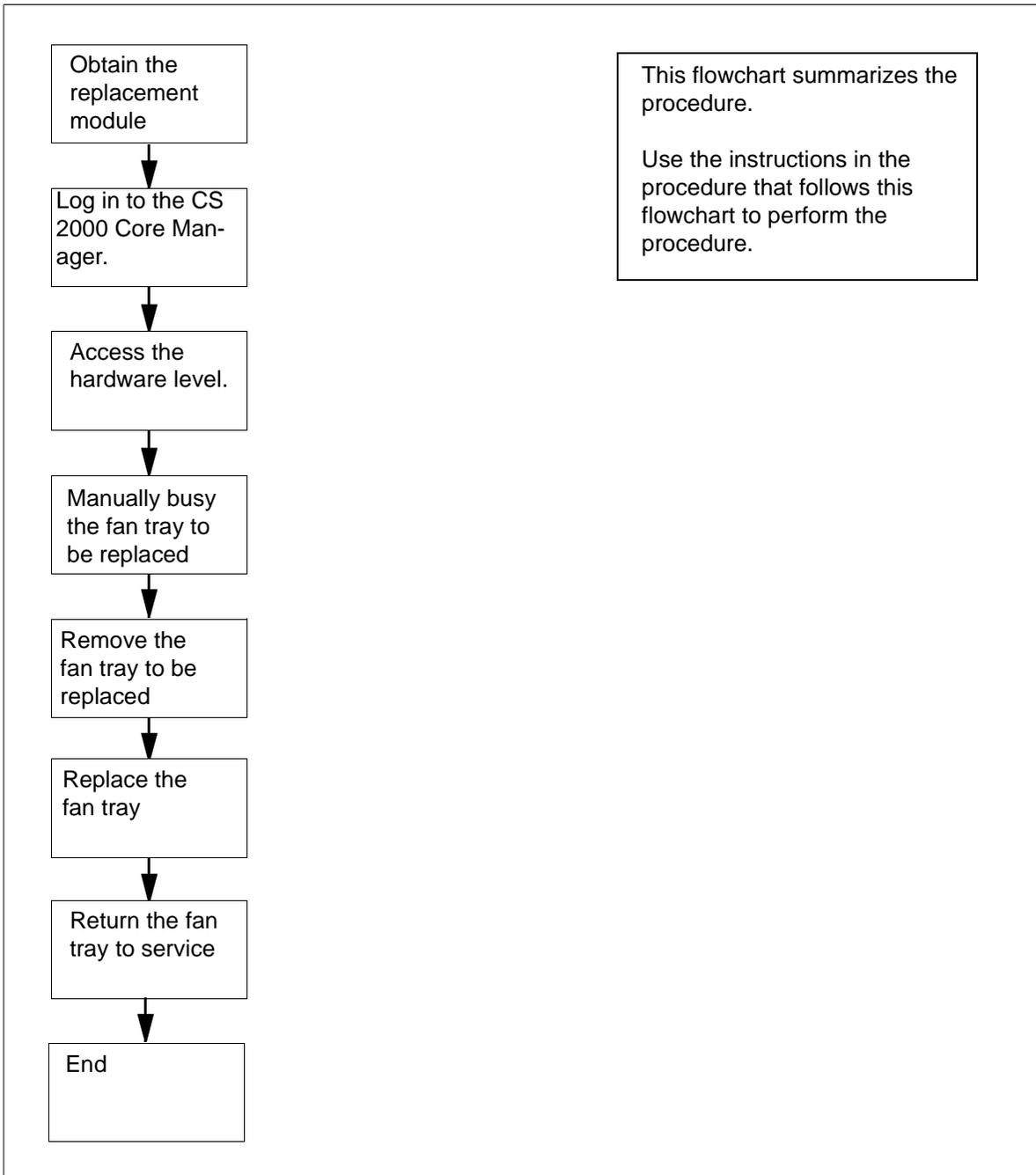
Obtain a replacement fan tray

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

At the local or remote VT100 console

2   Log into the CS 2000 Core Manager as the root or maint user.

3   Access the maintenance interface by typing

`# sdmmtc`

and pressing the Enter key.

4   Access the hardware level by typing

`> hw`

and pressing the Enter key.

5   Busy the fan tray module by typing

`> bsy <domain> fan`

and pressing the Enter key.

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 by typing

`> y`

and pressing the Enter key.

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 CS 2000 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.
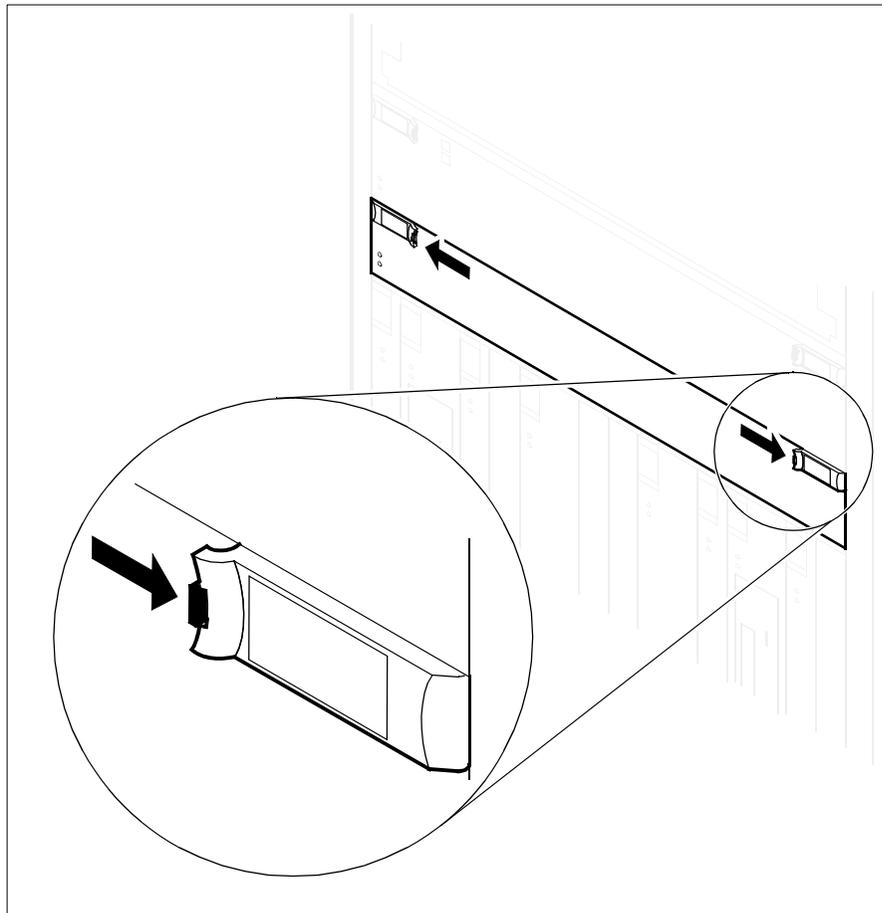
9 Open the locking levers on the face of the fan tray by moving the levers outwards.
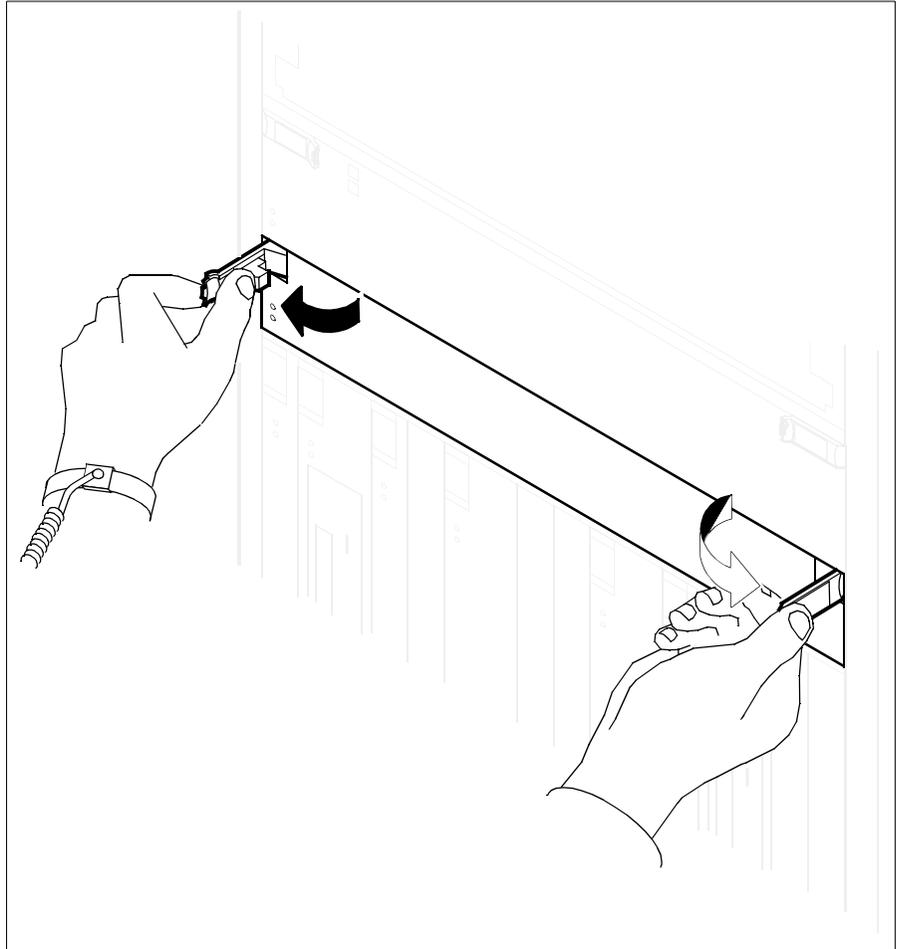
10 While grasping the locking levers, gently pull the fan tray towards you until the fan tray protrudes about 2 in. (5.1 cm) from the equipment shelf.
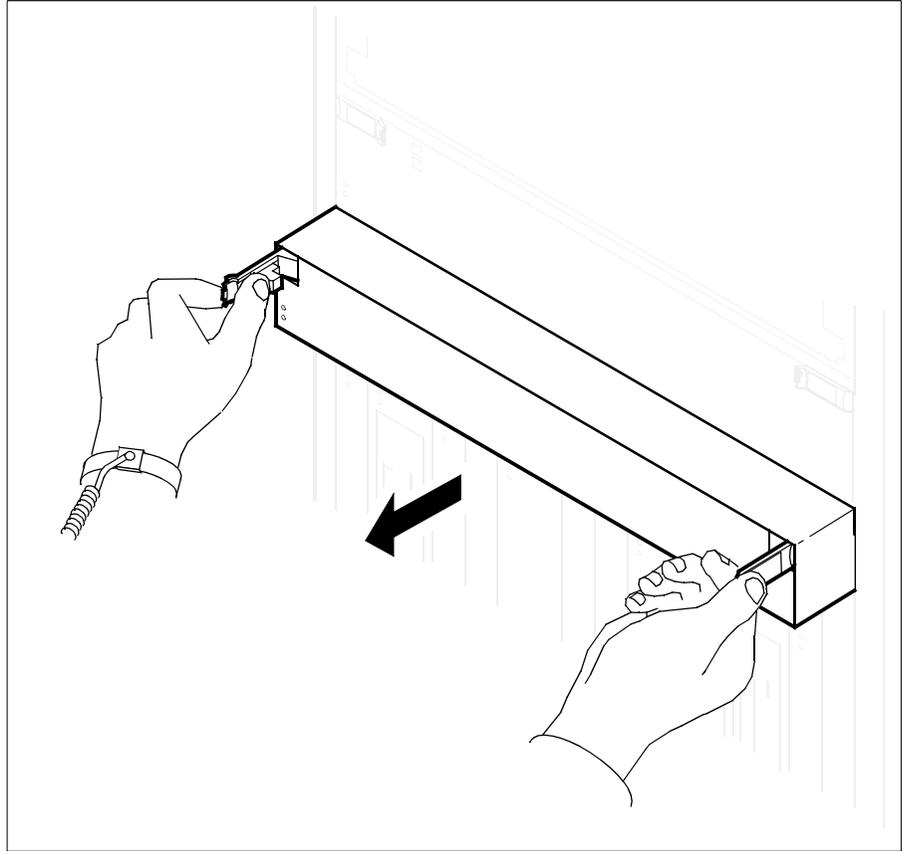
11   Hold the fan tray by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the fan tray toward you until it clears the shelf.
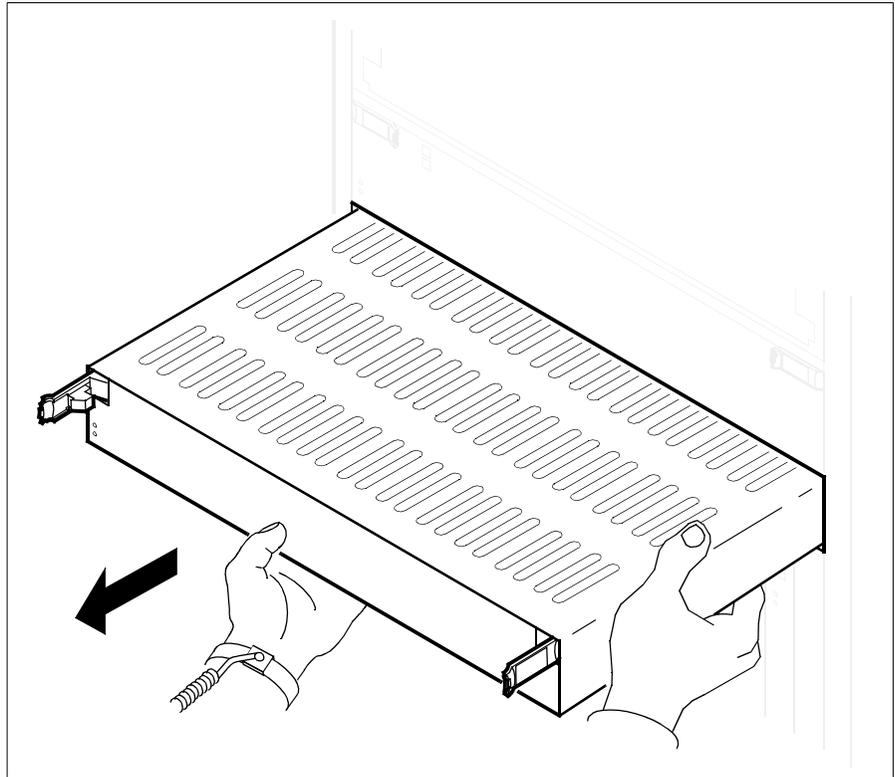
12   Place the fan tray you have removed in an ESD protective container.

13   Insert the replacement fan tray into the shelf.

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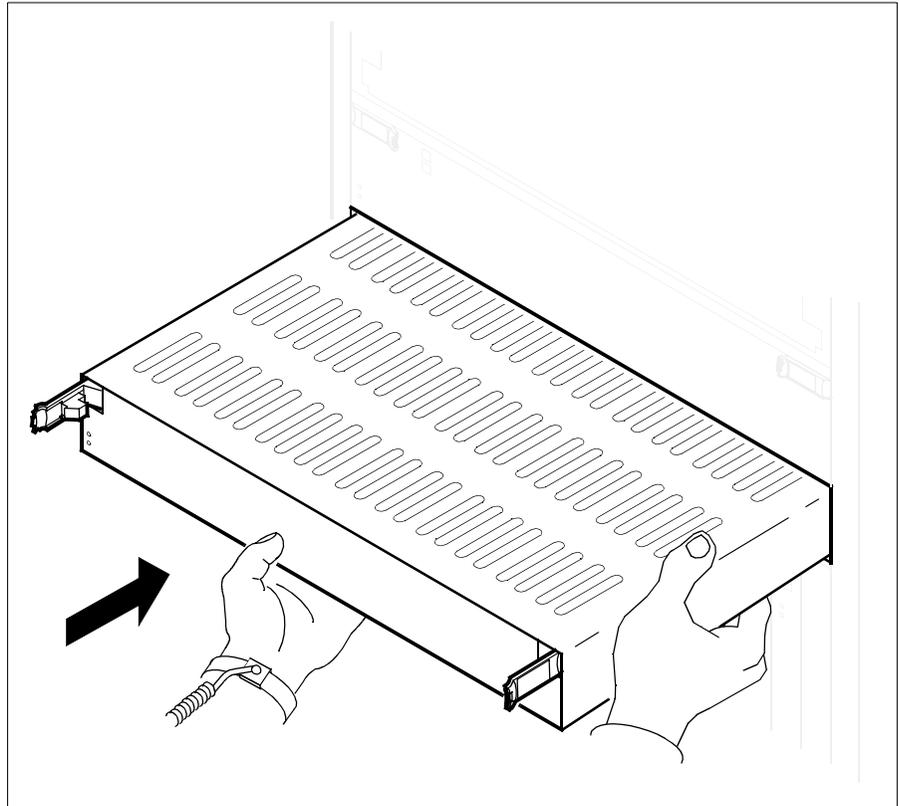
15   Partially close the locking levers, and continue to slide the fan tray until it is fully inserted into the shelf. The locking levers lock by themselves when the fan tray is fully inserted.

At the local or remote VT100 console

16   Return the fan tray to service by typing

> **> rts <domain> fan**

and pressing the Enter key.

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.

152

Replacing an interconnect module

Application

Use this procedure to replace an interconnect module (ICM) located at the rear of the main or I/O expansion chassis of the CS 2000 Core Manager.

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 CS 2000 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 only 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

```
Obtain the
replacement
module.
        |
        v
Log in to the CS
2000 Core Man-
ager.
        |
        v
Access the
storage level.
        |
        v
Determine the
state of disk
mirroring.
        |
        v
Allow
reintegration, if
required.
        |
        v
Access the
hardware level.
        |
        v
Manually busy
the ICM.
        |
        v
Turn off power to the CS
2000 Core Manager
chassis.
        |
        v
       (1)
```

```
       (1)
        |
        v
Determine if
the CPU is out
of service.
        |
        v
Return the CPU
to service, if
required.
        |
        v
Disconnect the
power cable from
the ICM.
        |
        v
Disconnect alarm
cable (if present)
from the ICM.
        |
        v
Remove the ICM.
        |
        v
Replace the ICM.
        |
        v
Reconnect the
power cable to
the ICM.
        |
        v
Reconnect alarm
cable (if present)
to the ICM.
```

```
Restore power to the
CS 2000 Core Manager
chassis.
        |
        v
Return the ICM
to service.
        |
        v
End
```

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

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 written at the top, left-hand side of the ICM.

At the local or remote VT100 console

2 Log into the CS 2000 Core Manager as the root or maint user.

3 Access the maintenance interface by typing

 # sdmmtc

and pressing the Enter key.

4 Access the storage level by typing

> storage

and pressing the Enter key.

Example response:

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

5 Verify the disk mirroring status for each volume group commissioned on the CS 2000 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 beyond this point 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 min. for each Gbyte. The actual time required varies depending on the amount of data in the volume group, and the current processor load.

7   Access the hardware (Hw) level by typing

   ```
   > hw
   ```

   and pressing the Enter key.

8   Busy the ICM by typing

   ```
   > bsy <n> icm
   ```

   and pressing the Enter key.

   where

   n
      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 by typing

> **y**

and pressing the Enter key.

> *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.

> *Note 3:* For systems with an IO expansion chassis, 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 CS 2000 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 CS 2000 Core Manager chassis according to where the ICM is located.

If you are replacing	Do
ICM0 in the main chassis	turn top left breaker off
ICM0 in the I/O expansion chassis	turn bottom left breaker off
ICM1 in the main chassis	turn top right breaker off
ICM1 in the I/O expansion chassis	turn bottom right breaker off

At the back of the CS 2000 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 CS 2000     │
│            Core Manager shuts down.                       │
└─────────────────────────────────────────────────────────┘
```

Disconnect the power cable from the ICM you are replacing.
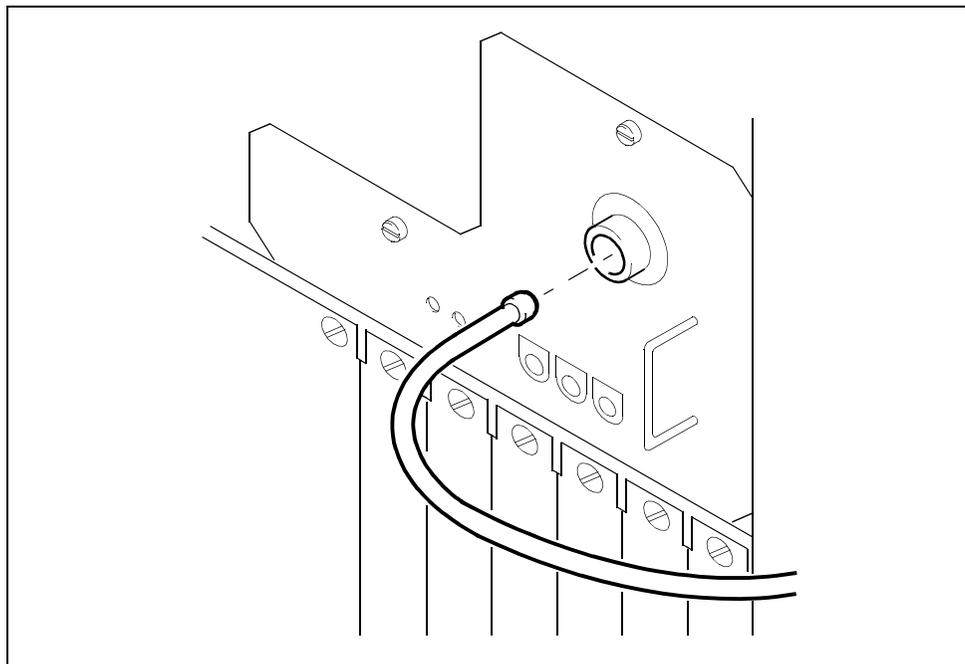
At the local or remote VT100 console

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]
> **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 CS 2000 Core Manager maintenance interface, or the platform MAP level under the CS 2000 Core Manager MAP level.

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

```
> rts <n> CPU
```

and pressing the Enter key.

where

> **n**
> 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 CS 2000 Core Manager maintenance interface, the CPU state changes to "S", indicating that the CPUs are reintegrating. The reintegration process takes about 2 min. 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   Use the following table to determine your next step.

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 CS 2000 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.
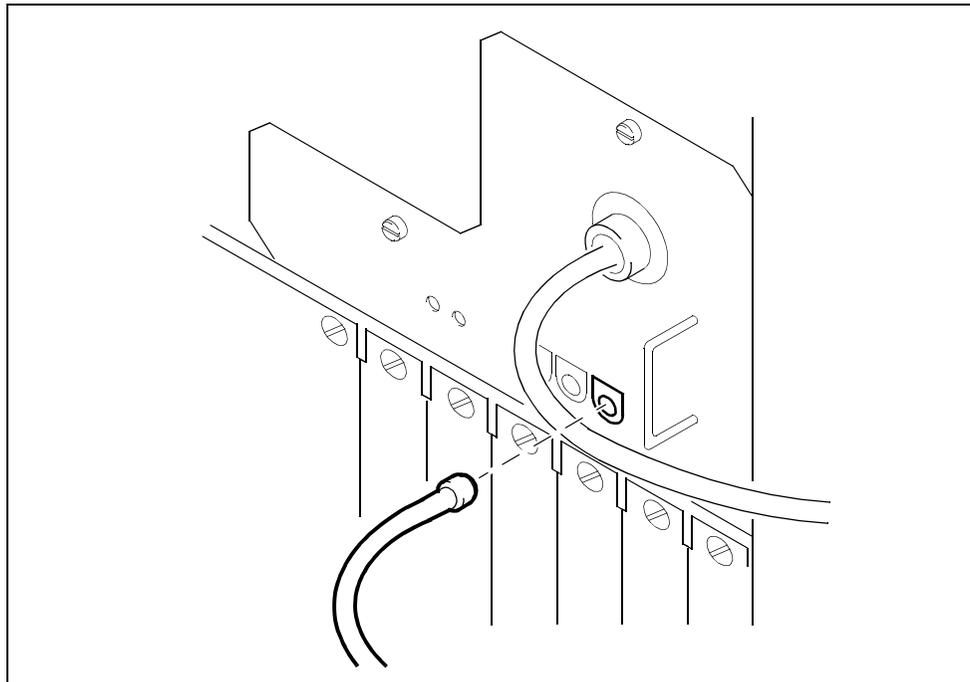
17 Loosen the two thumbscrews on the ICM you are replacing.

> *Note:* The thumbscrews are the captive type, and cannot be removed from the module.

18 Remove the ICM by gently sliding it out of the chassis.
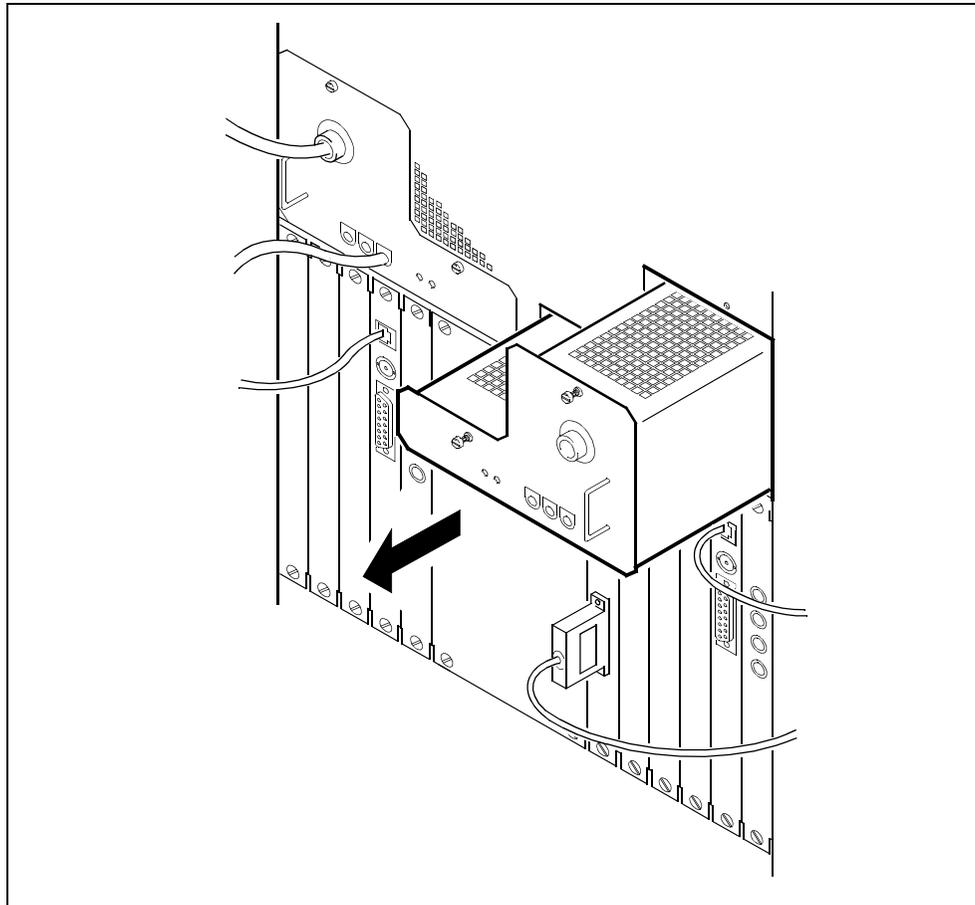
19 Place the ICM you have removed in an ESD protective container.

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 CS 2000 Core Manager chassis.

If you replaced	Do
ICM0 in the main chassis	turn top left breaker on
ICM0 in the I/O expansion chassis	turn bottom left breaker on
ICM1 in the main chassis	turn top right breaker on
ICM1 in the I/O expansion chassis	turn bottom right breaker on

At the local or remote VT100 console

25   Return the ICM to service by typing

> **> rts <n> icm**

and pressing the Enter key.

where

>   **n**
>   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 CS 2000 Core Manager by accessing the storage menu level of the CS 2000 Core Manager maintenance interface. Access the storage menu level by typing

```
> storage
```

and pressing the Enter key.

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 varies depending on the amount of data in the volume group, and the current processor load.

29 You have completed this procedure.

Replacing a standalone X.25 controller module

Application

Use this procedure to replace a standalone X.25 controller module (SYNC X.25), located at the front of the main, or expansion, chassis of the CS 2000 Core Manager.

Nortel PEC	Name
NTRX50FY	X.25 SYNC controller module

Action

The following flowchart is only 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

```
┌─────────────────┐          ┌──────────────────────────┐
│ Obtain the      │          │ This flowchart summarizes│
│ replacement     │          │ the procedure.           │
│ module          │          │                          │
└────────┬────────┘          │ Use the instructions in  │
         │                   │ the procedure that       │
         ▼                   │ follows this flowchart   │
┌─────────────────┐          │ to perform the           │
│ Log in to the CS│          │ procedure.               │
│ 2000 Core Man-  │          └──────────────────────────┘
│ ager.           │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Access the      │
│ hardware level  │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Manually busy   │
│ the X.25        │
│ controller module│
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Replace the     │
│ X.25 controller │
│ module          │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Return the X.25 │
│ controller module│
│ to service      │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ End             │
│                 │
│                 │
└─────────────────┘
```

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 written on the module's top locking lever.

At the local or remote VT100 console

2   Log into the CS 2000 Core Manager as the root or maintenance user.

3   Access the maintenance interface by typing

 # sdmmtc

and pressing the Enter key.

4   Access the hardware (Hw) level by typing

> hw

and pressing the Enter key.

5   Busy the X.25 controller module by typing

> bsy <n> X25

and pressing the Enter key.

where

> **n**
> is the domain number (0 or 1) of the X.25 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 one of slots 1 to 6 on the main chassis or slots 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 slots 9 to 16 on the expansion chassis

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")
```

6   Confirm the Bsy command by typing

> **> y**

and pressing the Enter key.

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 *complete*.

Example response:

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

> *Note:* At the hardware menu level of the CS 2000 Core Manager maintenance interface, the state of the X.25 controller module changes to "M".

At the front of the CS 2000 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

> **CAUTION**
> **Potential service interruption**
> Unseat only the X.25 controller module that you busied in step 5, and not the corresponding X.25 controller module in the other I/O domain. The in-service LED on the module busied in step 5 is off, and the out-of-service LED is on (red).

Unseat the correct X.25 controller module.

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

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

11 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the CS 2000 Core Manager shelf.
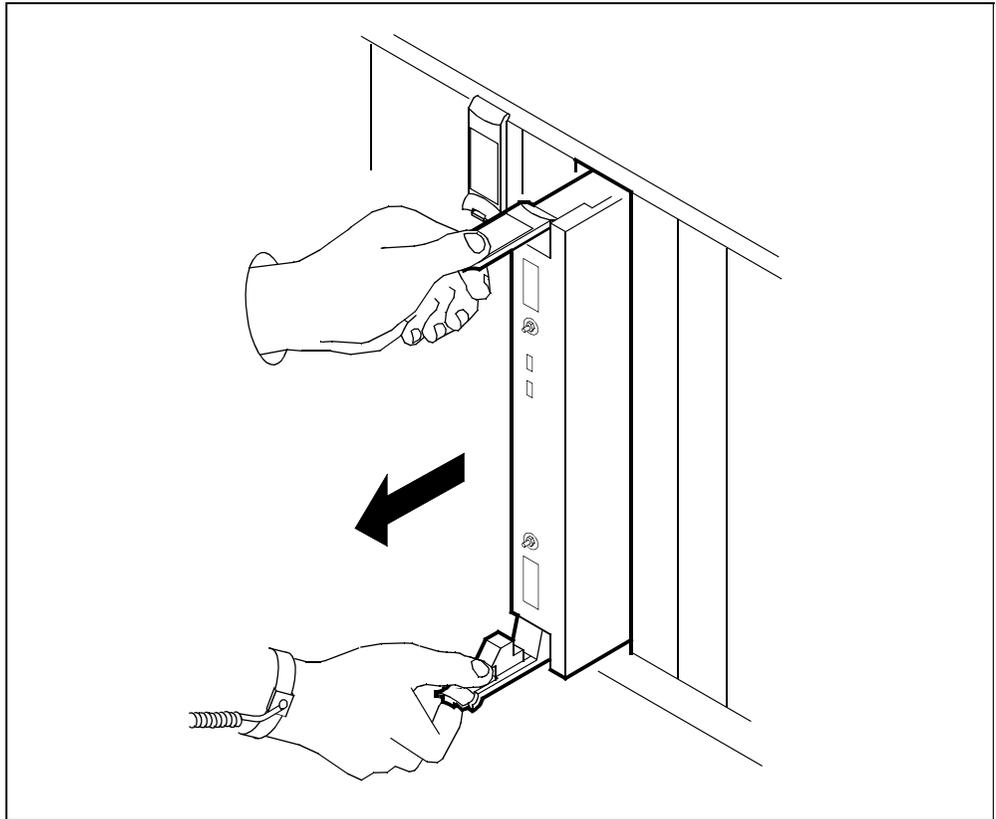
12 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.
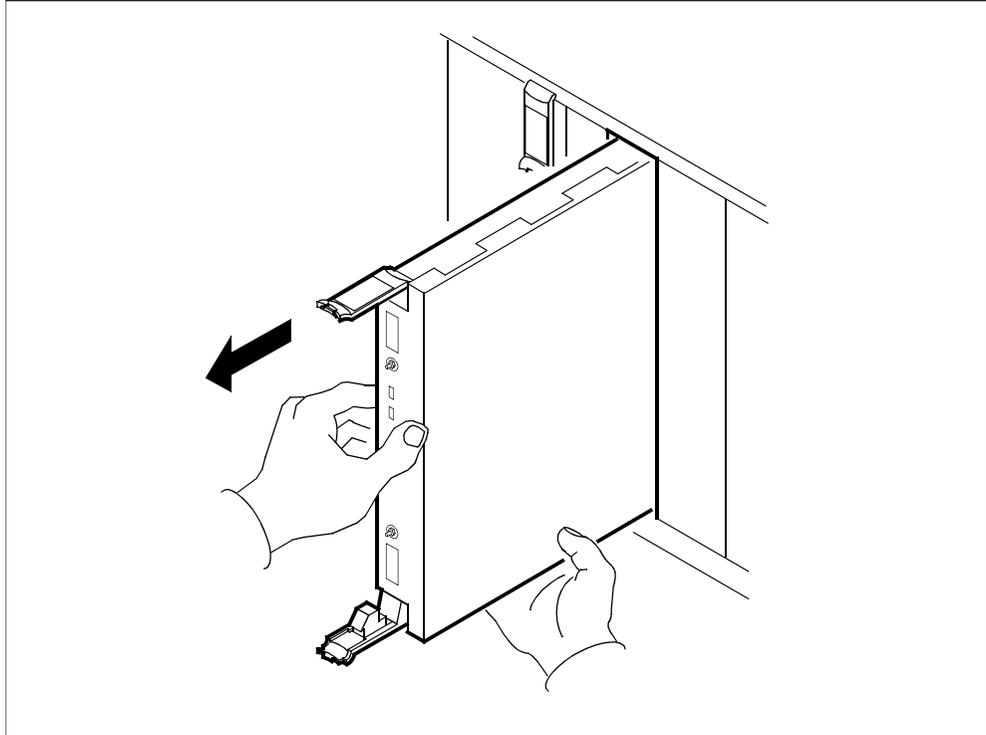
13 Place the module you have removed in an ESD protective container.

14 Insert the replacement module into the CS 2000 Core Manager shelf.

15 Gently slide the module into the shelf until it is fully inserted.
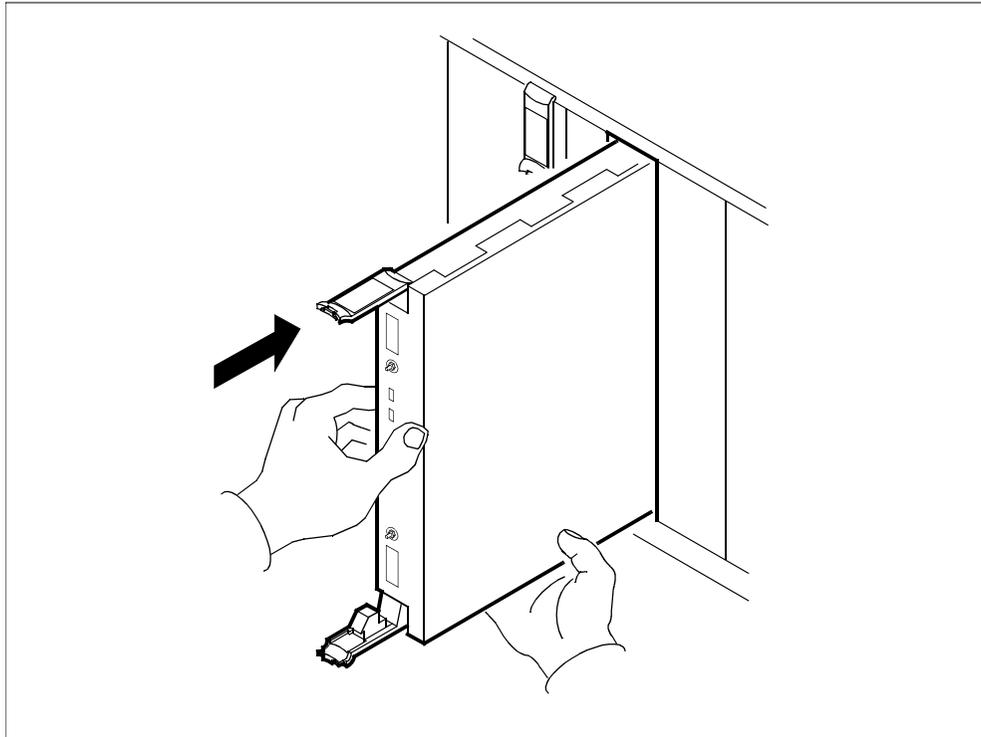
16   Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.

Micro switch
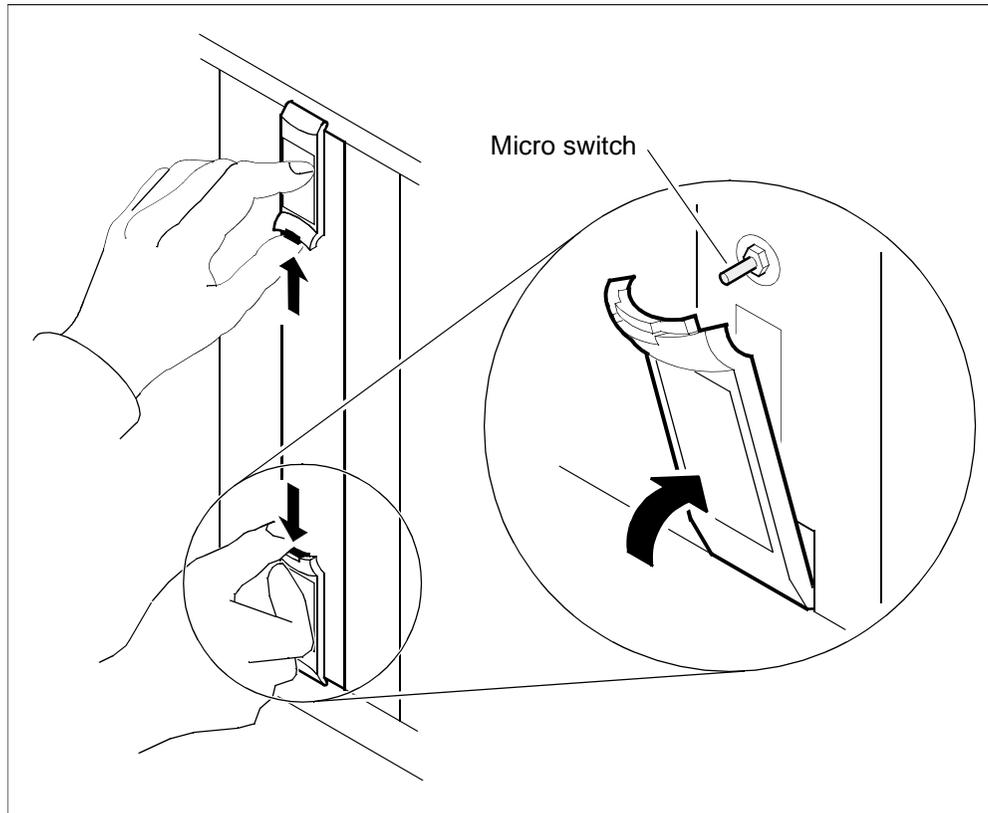
At the local or remote VT100 console

17   Return the X.25 controller module to service by typing

```
> rts n X25
```

and pressing the Enter key.

where

> **n**
> > is the SDM domain number (0 or 1) of the X.25 controller module you replaced in step 5.

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 CS 2000 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).

18   You have completed this procedure.

176

Replacing a standalone X.25 personality module

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 CS 2000 Core Manager.

Nortel PEC	Name
NTRX50FZ	X.25 SYNC personality module

Action

The following flowchart is only 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

```
                              ▽1
  ┌──────────────┐        ┌──────────────┐       ┌──────────────────────────┐
  │ Obtain the   │        │ Replace X.25 │       │ This flowchart summarizes │
  │ replacement  │        │ personality  │       │ the procedure.            │
  │ module       │        │ module       │       │                           │
  └──────┬───────┘        └──────┬───────┘       │ Use the instructions in   │
         │                       │               │ the procedure that follows│
         ▼                       ▼               │ this flowchart to perform  │
  ┌──────────────┐        ┌──────────────┐       │ the procedure.            │
  │ Log in to the│        │ Seat the X.25│       └──────────────────────────┘
  │ CS 2000 Core │        │ controller   │
  │ Manager.     │        │ module       │
  └──────┬───────┘        └──────┬───────┘
         │                       │
         ▼                       ▼
  ┌──────────────┐        ┌──────────────┐
  │ Access the   │        │ Return the   │
  │ hardware     │        │ X.25         │
  │ level        │        │ controller   │
  └──────┬───────┘        │ to service   │
         │                └──────┬───────┘
         ▼                       │
  ┌──────────────┐               ▼
  │ Manually busy│        ┌──────────────┐
  │ the X.25     │        │ End          │
  │ controller   │        │              │
  │ module       │        │              │
  └──────┬───────┘        └──────────────┘
         │
         ▼
  ┌──────────────┐
  │ Unseat the   │
  │ X.25 control-│
  │ ler module   │
  └──────┬───────┘
         │
         ▼
  ┌──────────────┐
  │ Remove the   │
  │ X.25         │
  │ personality  │
  │ module       │
  └──────┬───────┘
         ▽1
```

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 written at the top of the module.

At the local or remote VT100 console

2   Log into the CS 2000 Core Manager as the root or maintenance user.

3   Access the maintenance interface by typing

 # sdmmtc

and pressing the Enter key.

4   Access the hardware (Hw) level by typing

> hw

and pressing the Enter key.

5   Busy the X.25 controller module by typing

> bsy <n> X25

and pressing the Enter key.

where

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

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 slots 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 slots 9 to 16 on the expansion chassis

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")
```

6   Confirm the Bsy command by typing

> **y**

and pressing the Enter key.

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*.

Response:

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

> *Note:* At the hardware menu level of the CS 2000 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 CS 2000 Core Manager

7

> **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.

8

> ⚠️ **CAUTION**
> **Potential service interruption**
> Unseat only the X.25 controller module that you busied in step 5, and not the corresponding X.25 controller module in the other domain. The in-service LED on the module busied in step 5 is off, and the out-of-service LED is on (red).

Unseat the correct X.25 controller module.

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

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

At the back of the CS 2000 Core Manager

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

> *Note:* The thumbscrews are the captive type, and cannot be removed from the module.

12   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.

13 While grasping the thumbscrews, gently pull the X.25 personality module towards you until it protrudes about 2 in. (5.1 cm) from the CS 2000 Core Manager shelf.
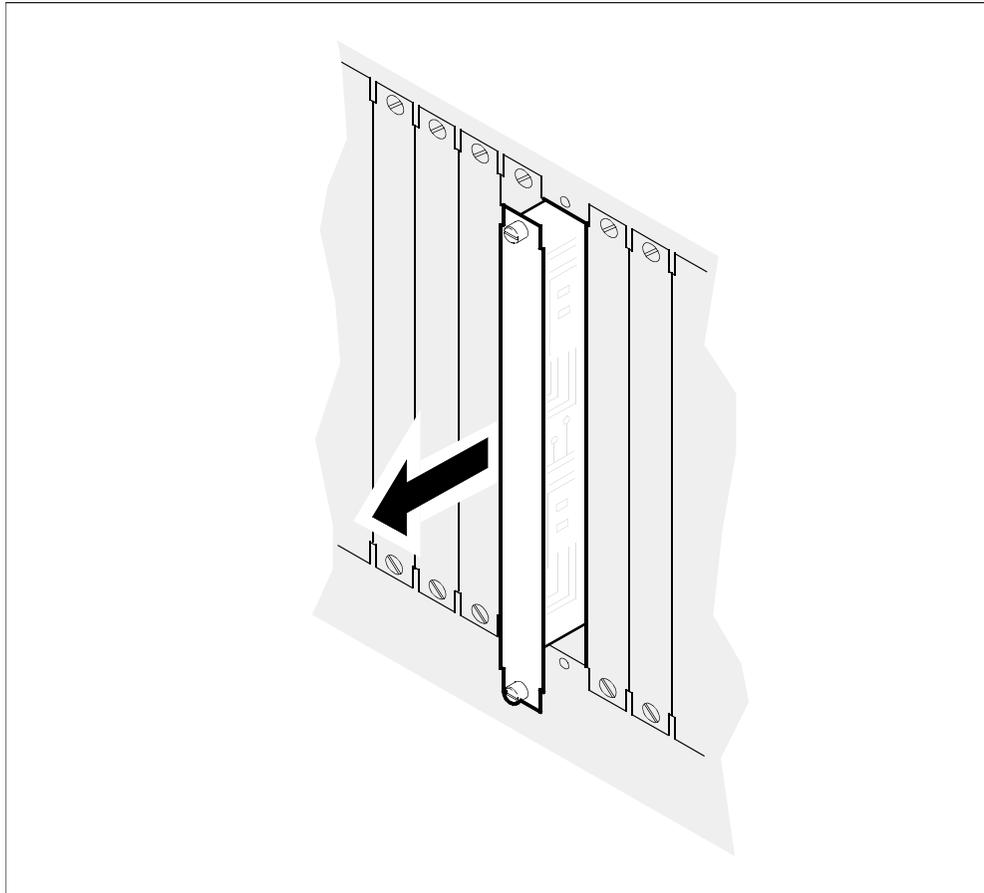
14   Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the X.25 personality module toward you until it clears the shelf.
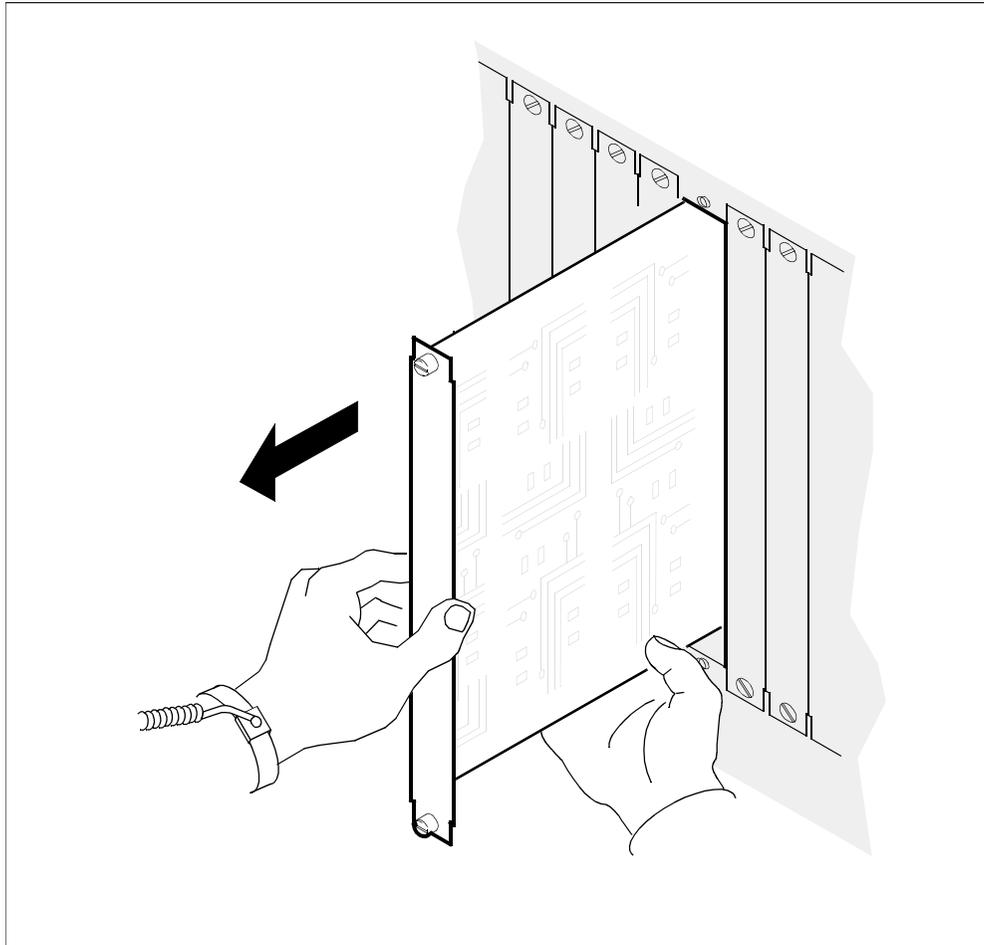
15   Place the X.25 personality module you have removed in an ESD protective container.

16   Insert the replacement X.25 personality module into the CS 2000 Core Manager shelf.

17   Gently slide the X.25 personality module into the shelf until it is fully inserted.
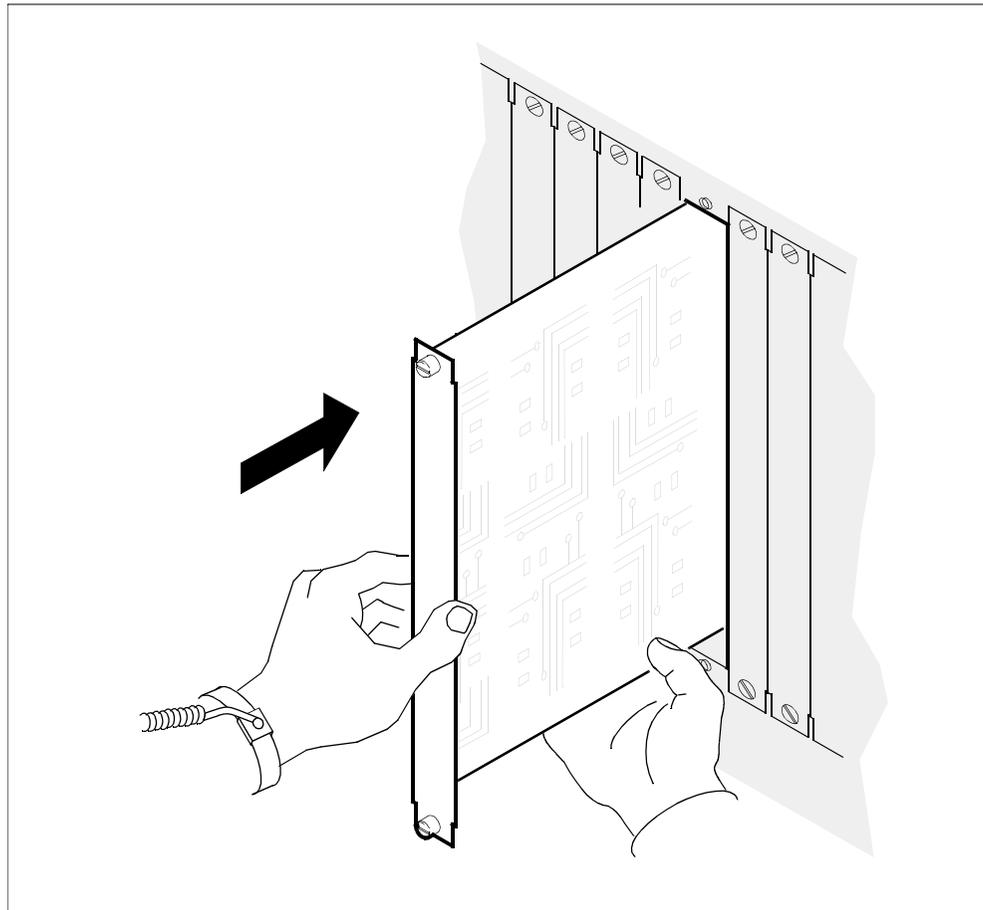
18   Tighten the thumbscrews at the top and the bottom of the X.25 personality module.

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

At the front of the CS 2000 Core Manager

20 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.

Micro switch
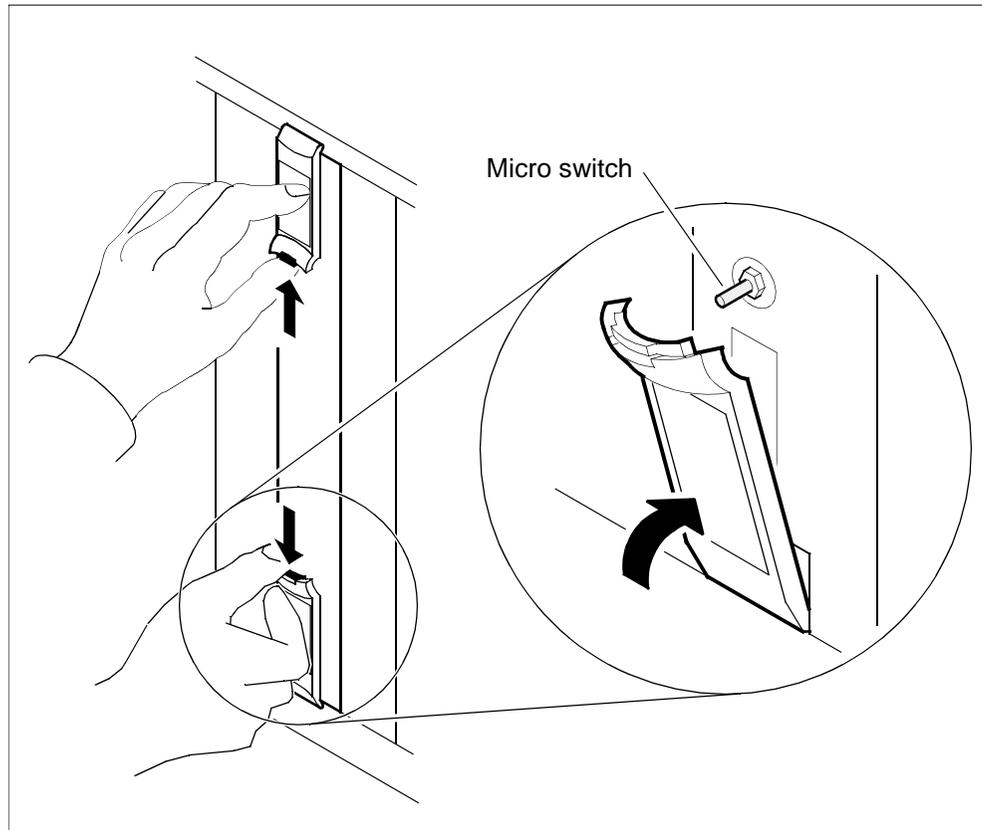
At the local or remote VT100 console

21   Return the X.25 controller module to service by typing

> `> rts <n> X25`

and pressing the Enter key.

where

> **n**
> is the SDM domain number (0 or 1) of the X.25 controller module you replaced. (See step 5.)

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 CS 2000 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).

22   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 only 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
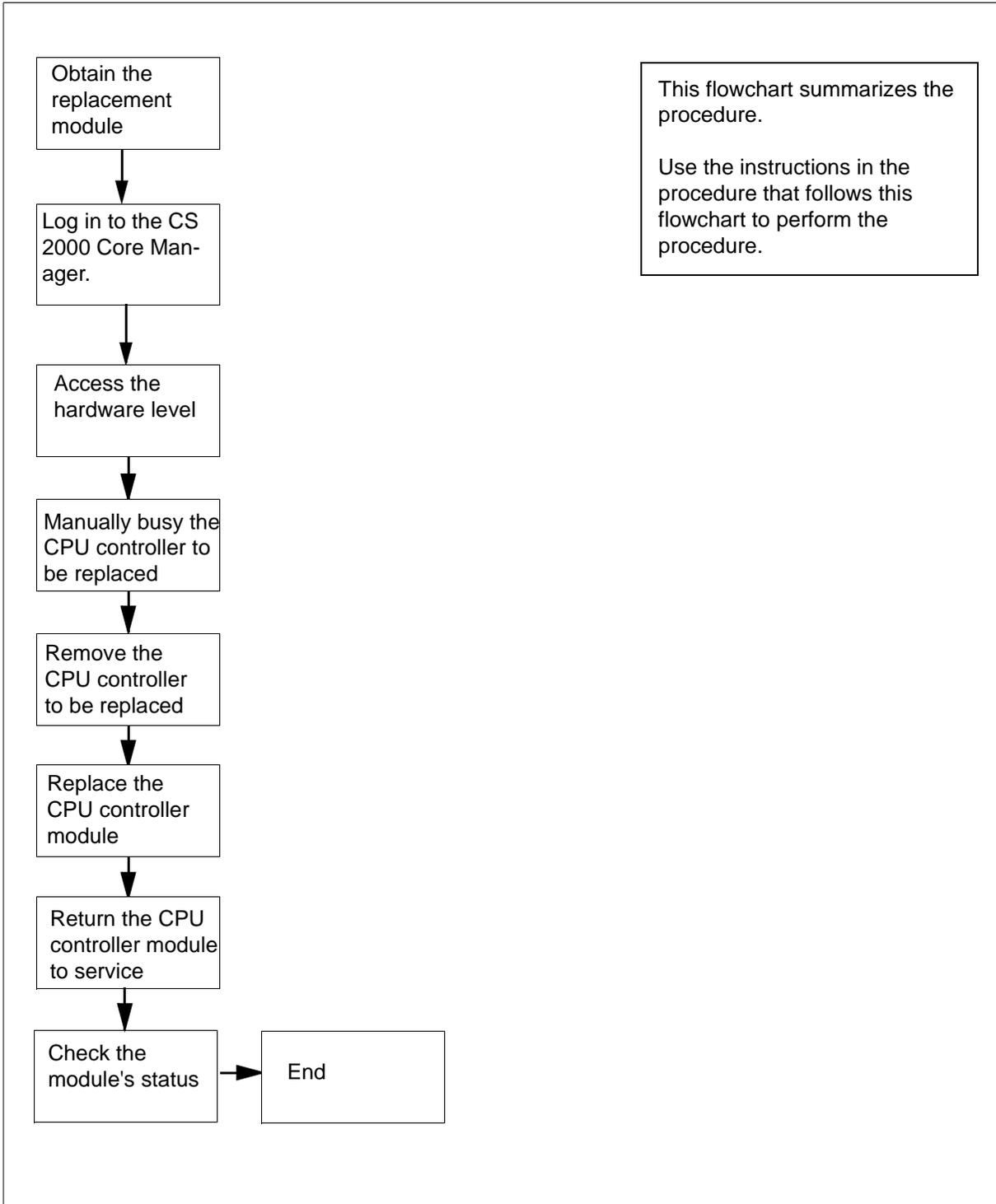
```
┌─────────────────┐
│ Obtain the      │
│ replacement     │
│ module          │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Log in to the CS│
│ 2000 Core Man-  │
│ ager.           │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Access the      │
│ hardware level  │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Manually busy the│
│ CPU controller to│
│ be replaced      │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Remove the      │
│ CPU controller  │
│ to be replaced  │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Replace the     │
│ CPU controller  │
│ module          │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Return the CPU  │
│ controller module│
│ to service      │
└────────┬────────┘
         │
         ▼
┌─────────────────┐      ┌─────────────┐
│ Check the       │─────▶│ End         │
│ module's status │      │             │
└─────────────────┘      └─────────────┘
```

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

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 written on the module's top locking lever.

At the local or remote VT100 console

2 Log into the CS 2000 Core Manager as the root or maintenance user.

3 Access the maintenance interface by typing

```
# sdmmtc
```

and pressing the Enter key.

4 Access the hardware (Hw) level by typing

```
> hw
```

and pressing the Enter key.

5 Busy the CPU controller module you want to replace by typing

```
> bsy <n> cpu
```

and pressing the Enter key.

where

> **n**
>> 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, and 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 CS 2000 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 CS 2000 Core Manager shuts down and an automatic reboot occurs.

When a CPU controller module is pulled from the CS 2000 Core Manager, automatic message accounting (AMA) may go into backup, depending on the scenario:

*   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 CS 2000 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 min.) is longer than the SuperNode Billing

Application (SBA) tolerance to waiting for acknowledgement for storage of billing data.

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

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

7 Depress the tips of the locking levers on the face of the CPU controller module.
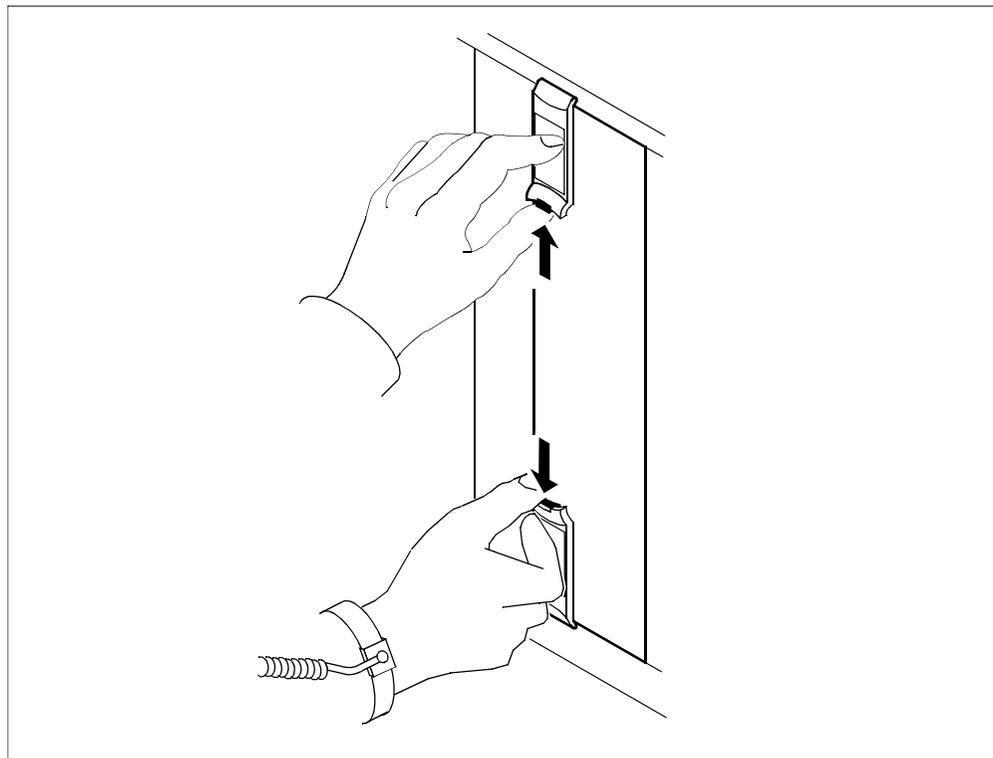
8 Open the locking levers on the face of the module by moving the levers outwards.
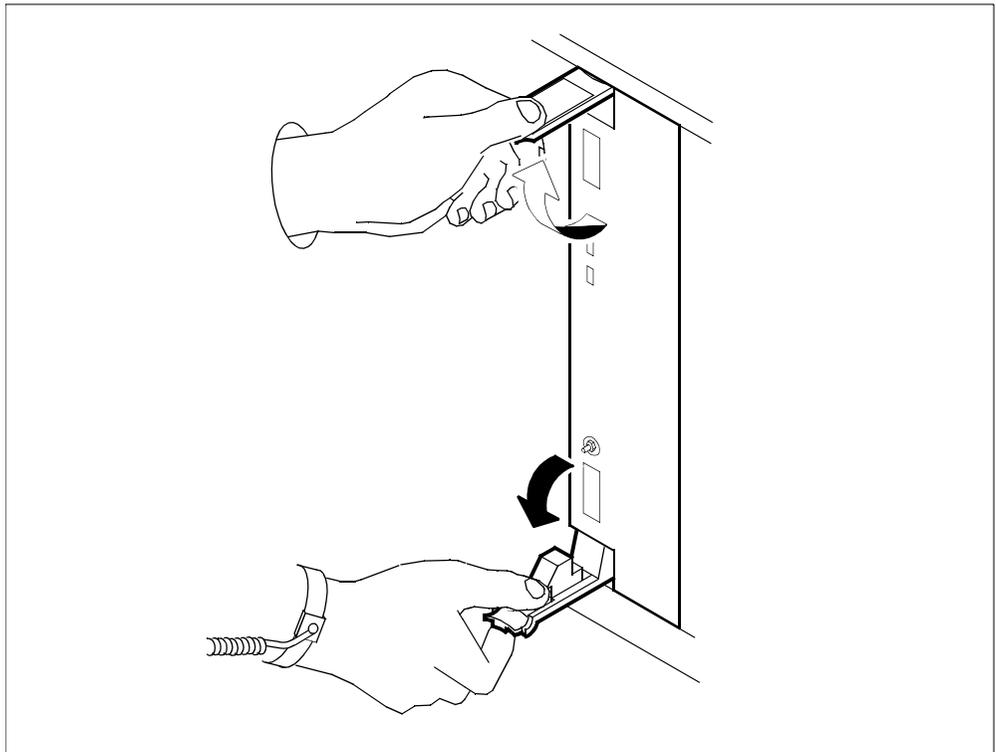
9 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the CS 2000 Core Manager shelf.
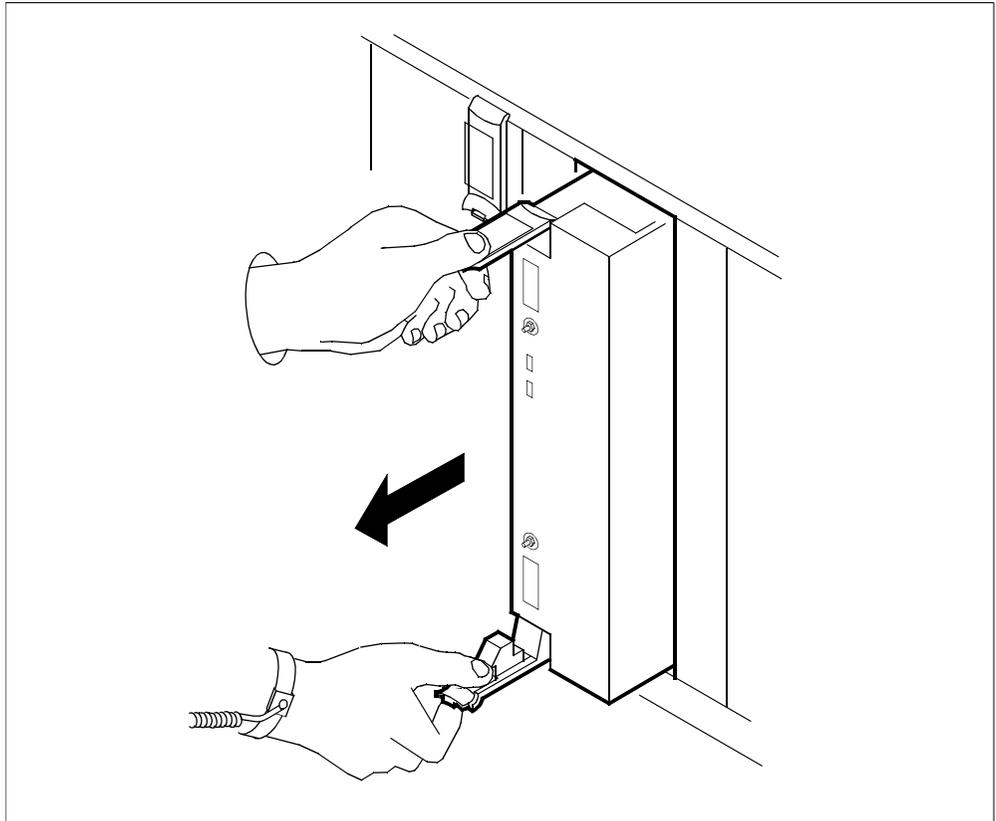
10 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.
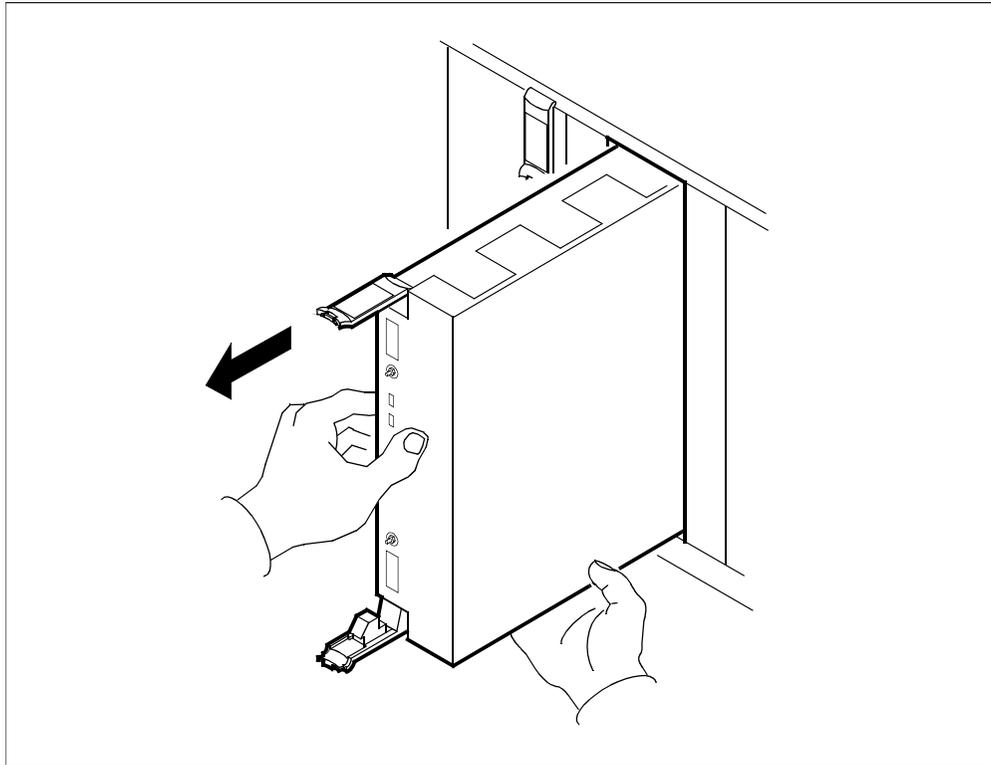
11 Place the module you have removed in an ESD protective container.

12 Insert the replacement module into the CS 2000 Core Manager shelf.

13 Gently slide the module into the shelf until it is fully inserted.
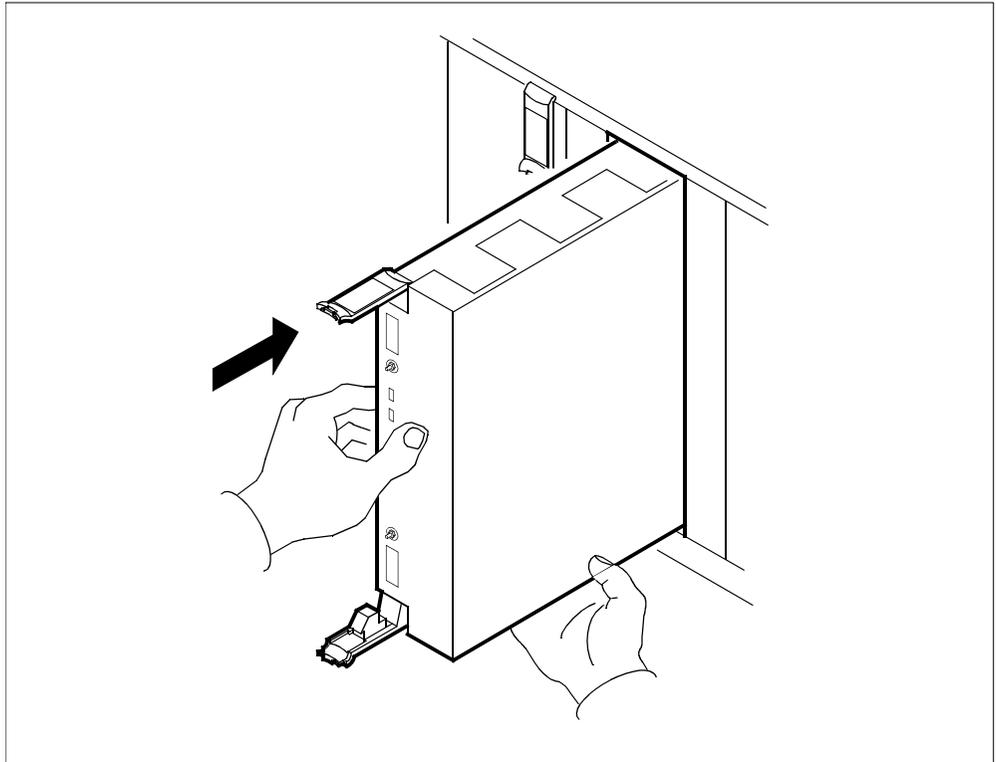
14   Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.
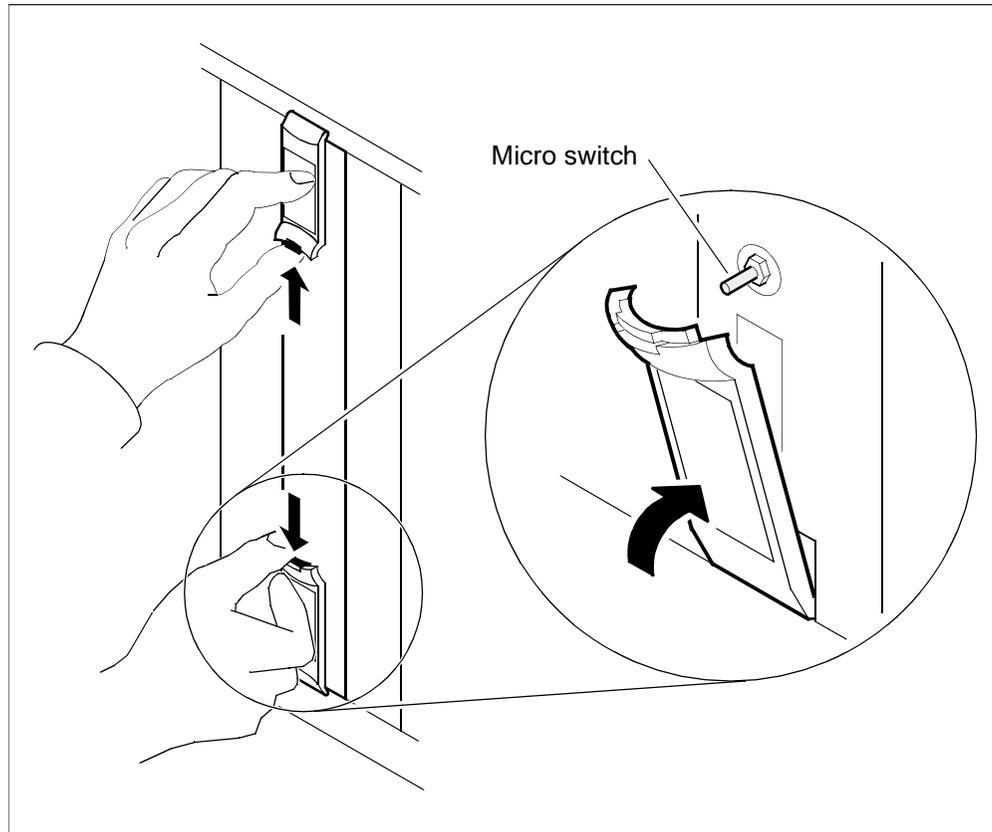
15   Tighten the thumbscrews on the module.

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

16   Return the CPU controller module to service by typing

    `> rts <n> cpu`

and pressing the Enter key.

where

> **n**
> 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, and 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 min. for the CPU controller module to complete reintegration and return to service.

17   Use the following table to determine your next step.

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

200

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
NTRX50FU	I/O controller module with 2-Gbyte disk drive, digital audio tape (DAT) and Ethernet
NTRX50GN	I/O controller module with 4-Gbyte disk drive, DAT and Ethernet
NTRX50GP	I/O controller module with two 4-Gbyte disk drives and Ethernet
NTRX50GX	I/O controller module with increased buffer memory (16-Kbyte per link)
NTRX50NC	I/O controller module with two 9-Gbyte disk drives and Ethernet
NTRX50ND	I/O controller module with 9-Gbyte disk drive, DAT and Ethernet

Action

The following flowchart is only 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

```
                                    ▽1
                                     │
                                     ▼
  ┌─────────────────┐       ┌─────────────────┐     ┌──────────────────────────┐
  │ Obtain the      │       │ Eject the tape, │     │ This flowchart summarizes │
  │ replacement     │       │ if required     │     │ the procedure.            │
  │ module          │       └─────────────────┘     │                           │
  └─────────────────┘                │              │ Use the instructions in   │
           │                         ▼              │ the procedure that follows│
           ▼                ┌─────────────────┐     │ this flowchart to perform │
  ┌─────────────────┐       │ Remove the      │     │ the procedure.            │
  │ Log into the CS │       │ I/O controller  │     └──────────────────────────┘
  │ 2000 Core Man-  │       │ module          │
  │ ager.           │       └─────────────────┘
  └─────────────────┘                │
           │                         ▼
           ▼                ┌─────────────────┐
  ┌─────────────────┐       │ Replace the     │
  │ Access the      │       │ I/O controller  │
  │ storage level.  │       │ module          │
  └─────────────────┘       └─────────────────┘
           │                         │
           ▼                         ▼
  ┌─────────────────┐       ┌─────────────────┐
  │ Determine the   │       │ Return the I/O  │
  │ state of disk   │       │ controller module│
  │ mirroring       │       │ to service      │
  └─────────────────┘       └─────────────────┘
           │                         │
           ▼                         ▼
  ┌─────────────────┐       ┌─────────────────┐
  │ Allow           │       │ Access the      │
  │ reintegration,  │       │ storage level.  │
  │ if required     │       └─────────────────┘
  └─────────────────┘                │
           │                         ▼
           ▼                ┌─────────────────┐
  ┌─────────────────┐       │ Monitor disk    │
  │ Access          │       │ mirroring       │
  │ hardware level. │       │ status          │
  └─────────────────┘       └─────────────────┘
           │                         │
           ▼                         ▼
  ┌─────────────────┐       ┌─────────────────┐
  │ Manually busy   │       │ Reinsert the    │
  │ the I/O controller│     │ tape, if        │
  │ module          │       │ required        │
  └─────────────────┘       └─────────────────┘
           ▽1                        │
                                     ▼
                            ┌─────────────────┐
                            │ End             │
                            │                 │
                            └─────────────────┘
```

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 written on the module's top locking lever.

At the local or remote VT100 console

2 Log into the CS 2000 Core Manager as the root or maintenance user.

3 Access the maintenance interface by typing

 # sdmmtc

and pressing the Enter key.

4 Access the storage level by typing

> storage

and pressing the Enter key.

5 Use the following table to determine your next step.

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 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 min. for each Gbyte. The actual time required varies

depending 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 by typing

> **hw**

and pressing the Enter key.

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 by typing

> **bsy *<domain>* dsk**

and pressing the Enter key.

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 by typing

`> y`

and pressing the Enter key.

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 CS 2000 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 <u>8</u>. 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 CS 2000 Core Manager. If you remove the in-service NTRX50FQ module, you will also cause an automatic reboot of the CS 2000 Core Manager.
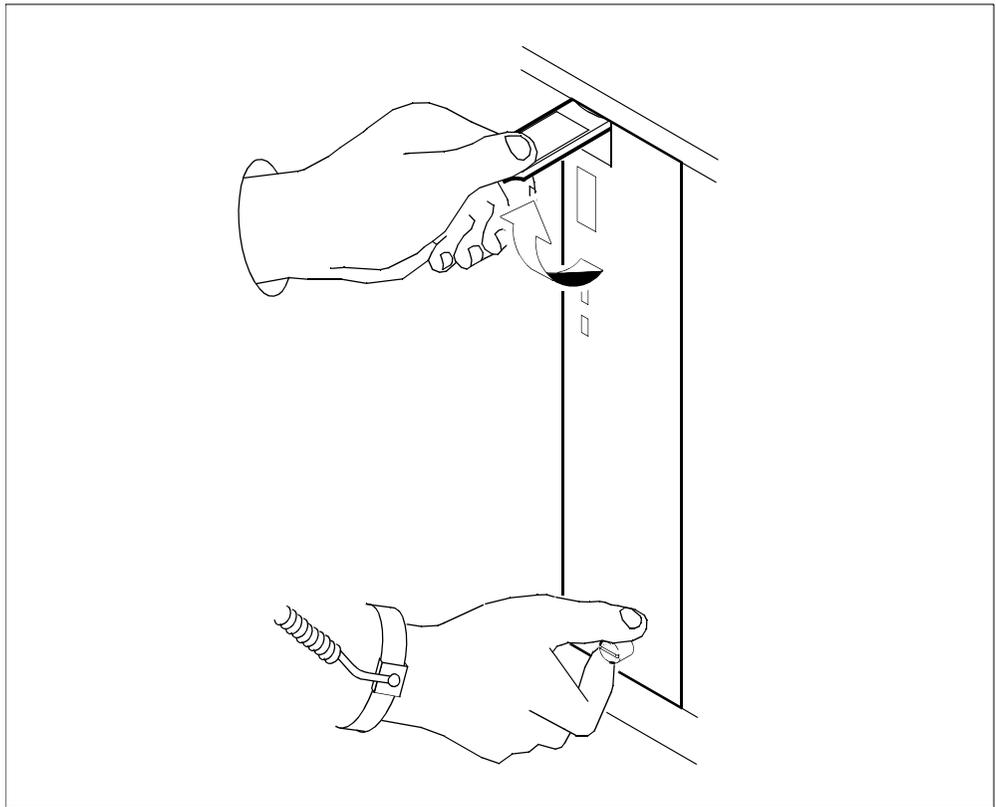
Undo the thumbscrews located on the top and the bottom of the I/O controller module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.
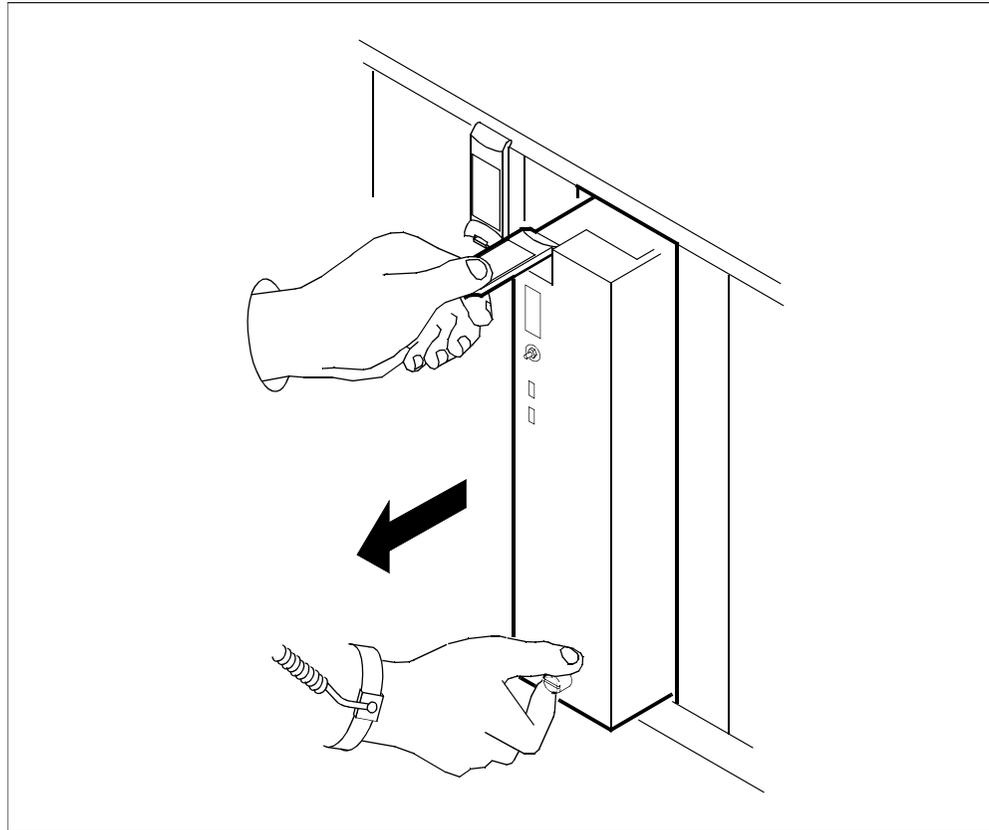
12 Depress the tip of the locking lever on the face of the I/O controller module.
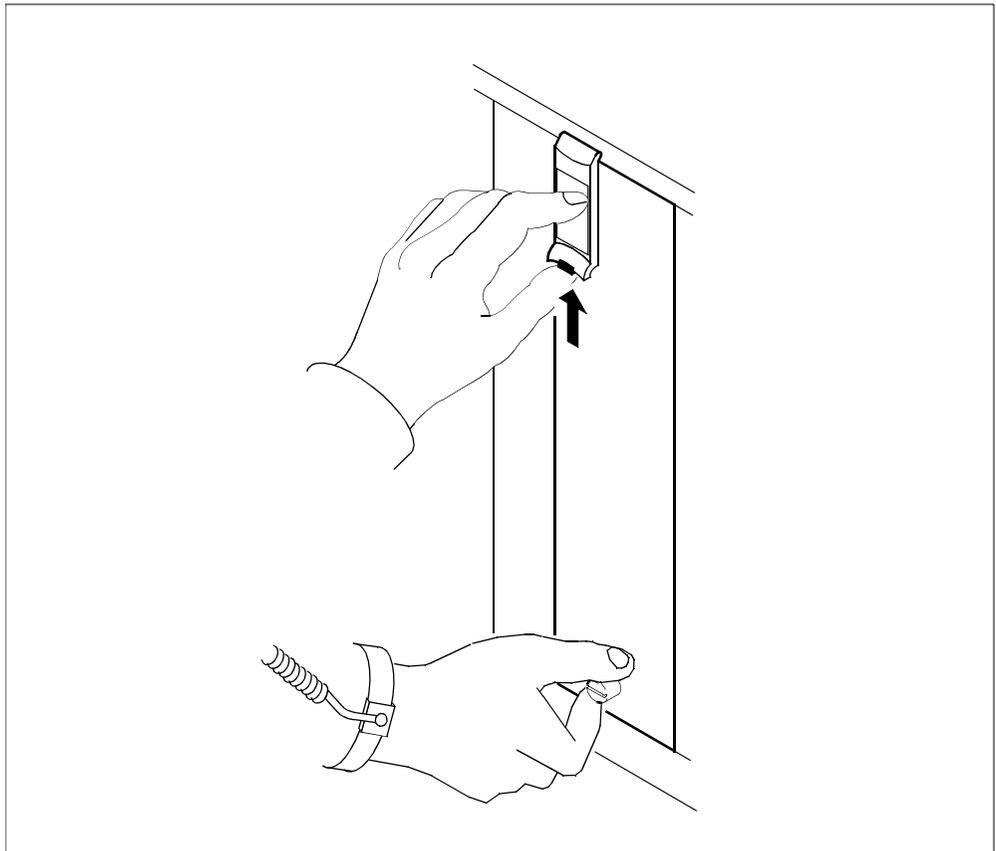
13　　Open the locking lever on the face of the module by moving the lever outwards.

14 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the CS 2000 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.
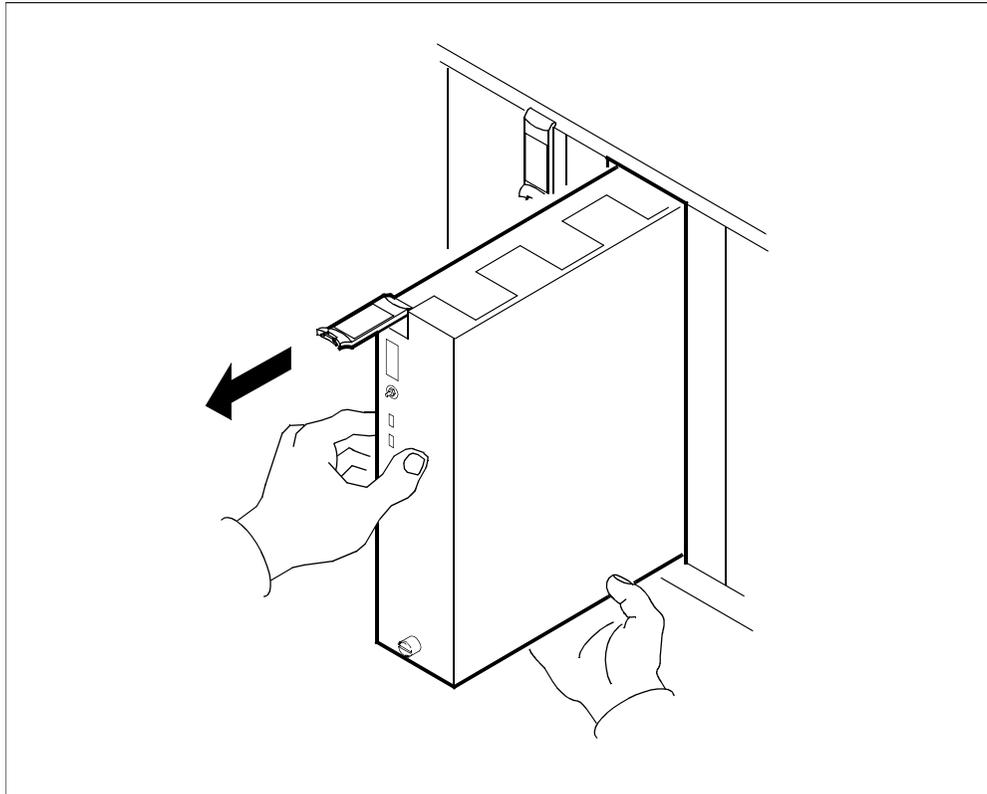
16   Place the module you have removed in an ESD protective container.

17   Insert the replacement module into the CS 2000 Core Manager shelf.

18 Gently slide the module into the shelf until it is fully inserted.
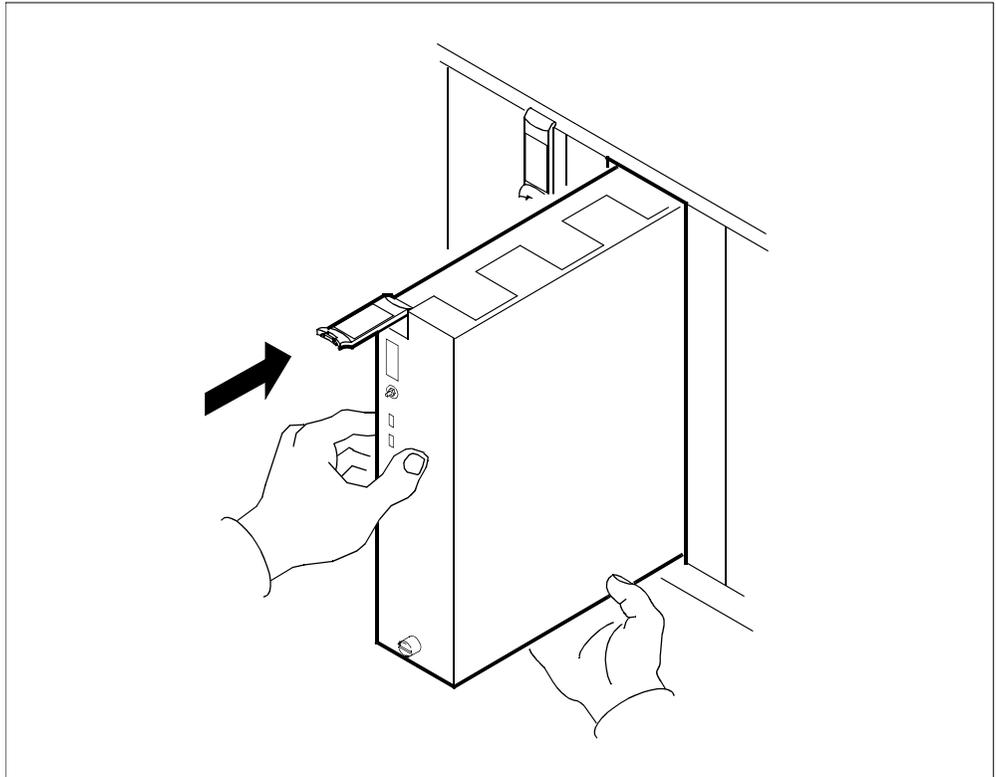
19 Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.

Micro switch
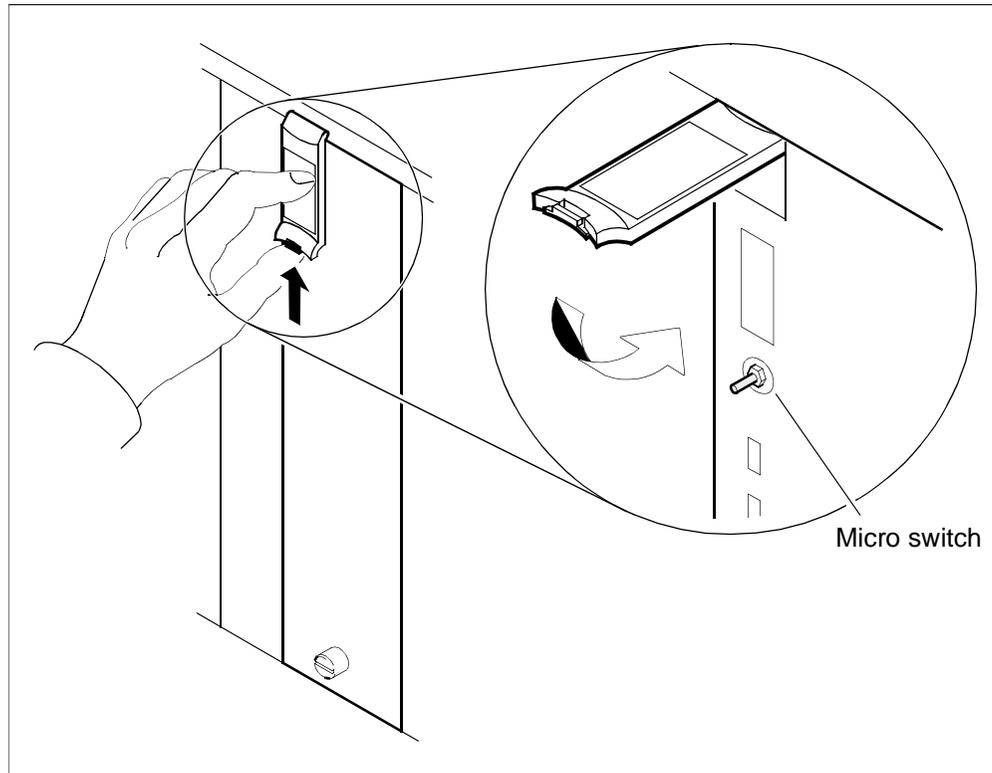
20 Tighten the thumbscrews on the module.

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 by typing

> **rts <*domain*> dsk**

and pressing the Enter key.

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 by typing

> **storage**

and pressing the Enter key.

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 min.
for each Gbyte. The actual time varies depending 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

Application

Use this procedure to replace the DS512 controller module, located at the front of the main chassis (slots 1 and 12) of the CS 2000 Core Manager.

Nortel PEC	Name
NTRX50GA	DS512 controller module

Action

The following flowchart is only 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

Obtain the replacement module

↓

Access the MAP display

↓

Display the MS port modules

↓

Access the MS level of the MAP display

↓

Access the shelf level

↓

Access the MS port module level

↓

Manually busy the DS512 links

↓

Access the hardware level

▽ 1

▽ 1

Manually busy the DS512 controller module

↓

Replace the DS512 controller module

↓

Return the DS512 controller module to service

↓

Return the DS512 links to service

↓

End

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.
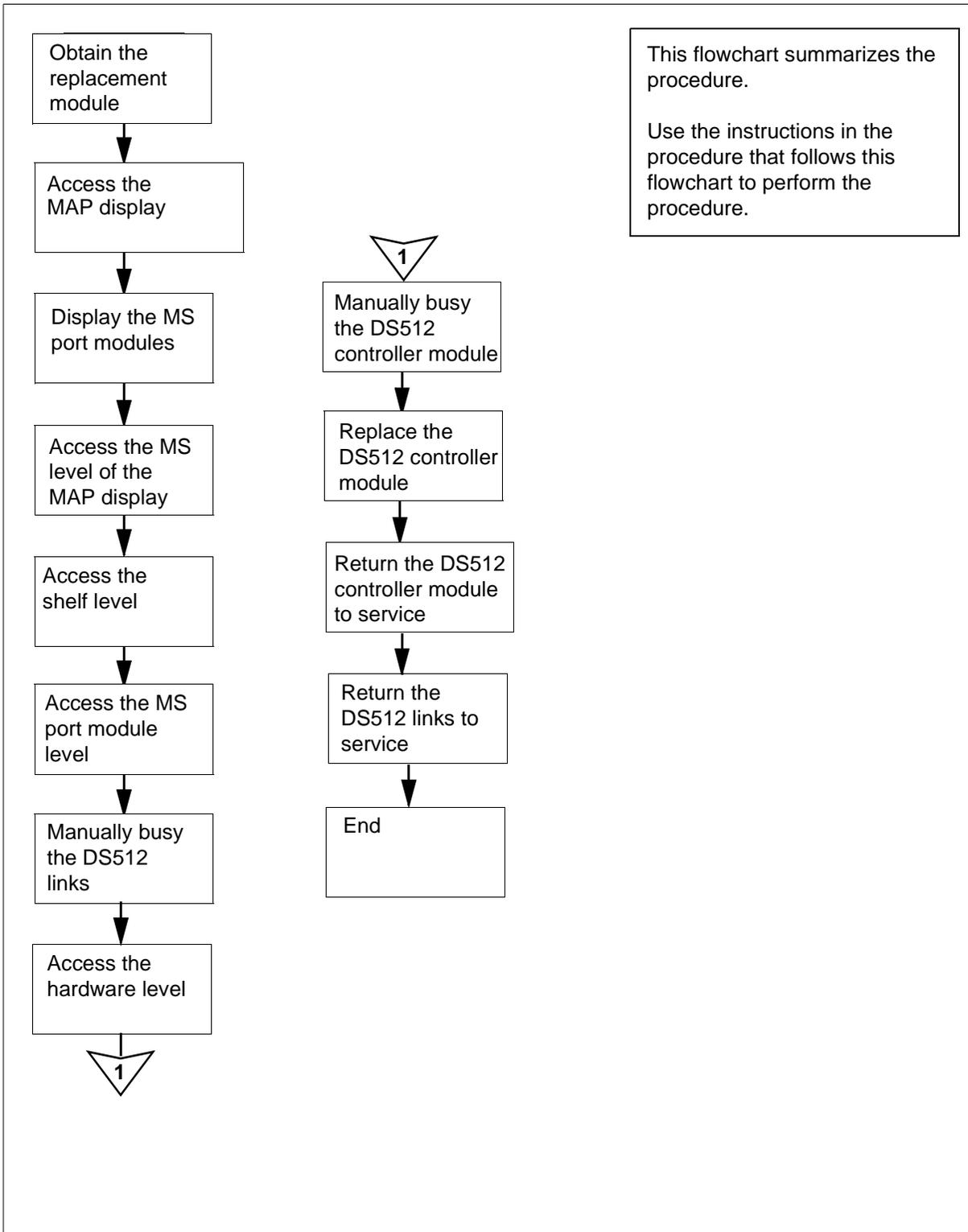
Replacing a DS512 controller module

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 written on the module's top locking lever.

At the MAP display

2   Access the SDM level by typing

> **mapci;mtc;appl;sdm**

and pressing the Enter key.

3   Display the message (MS) port modules which provide the DS512 links to the CS 2000 Core Manager by typing

> **trnsl**

and pressing the Enter key.

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 CS 2000 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 by typing

> **ms**

and pressing the Enter key.

6   Access the shelf level by typing

> **shelf 0**

and pressing the Enter key.

7 Access the MS chain level that is associated with the CS 2000 Core Manager DS512 links by typing

> **chain <*cardno*>**

and pressing the Enter key.

where

> **cardno**
> is the MS card number recorded in step 4

8 Busy the DS512 link between MS plane 0 and the CS 2000 Core Manager DS512 controller module you want to replace by typing

> **bsy 0 link <*link number*>**

and pressing the Enter key.

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: 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 CS 2000 Core Manager DS512 controller module you want to replace by typing

> **> bsy 1 link <*link number*>**

and pressing the Enter key.

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 CS 2000 Core Manager as the root or maint user.

11   Access the maintenance interface by typing

> **# sdmmtc**

and pressing the Enter key.

12   Access the hardware (Hw) level by typing

> **> hw**

and pressing the Enter key.

13 Busy the DS512 controller module by typing

> **> bsy <*n*> 512**

and pressing the Enter key.

where

> **n**
>> 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 by typing

> **> y**

and pressing the Enter key.

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 CS 2000 Core Manager maintenance interface, the state of the DS512 controller module changes to "M".

At the front of the CS 2000 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 CS 2000 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 cannot be removed from the
module.

17   Depress the tips of the locking levers on the face of the DS512 controller module.
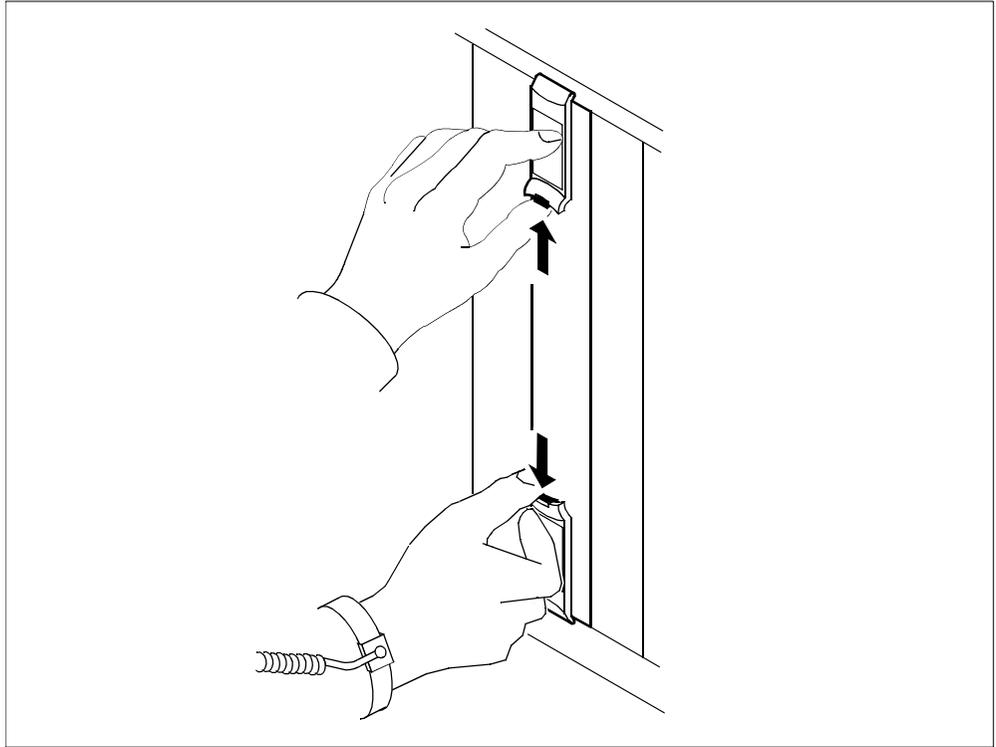
18 Open the locking levers on the face of the module by moving the levers outward.
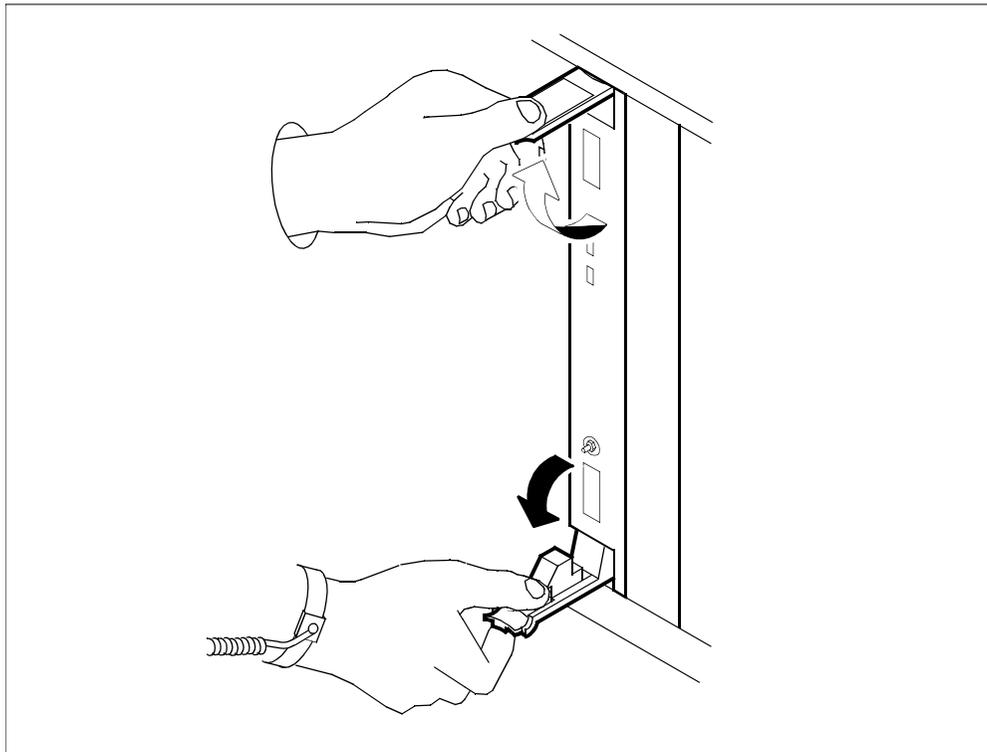
19 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the CS 2000 Core Manager shelf.
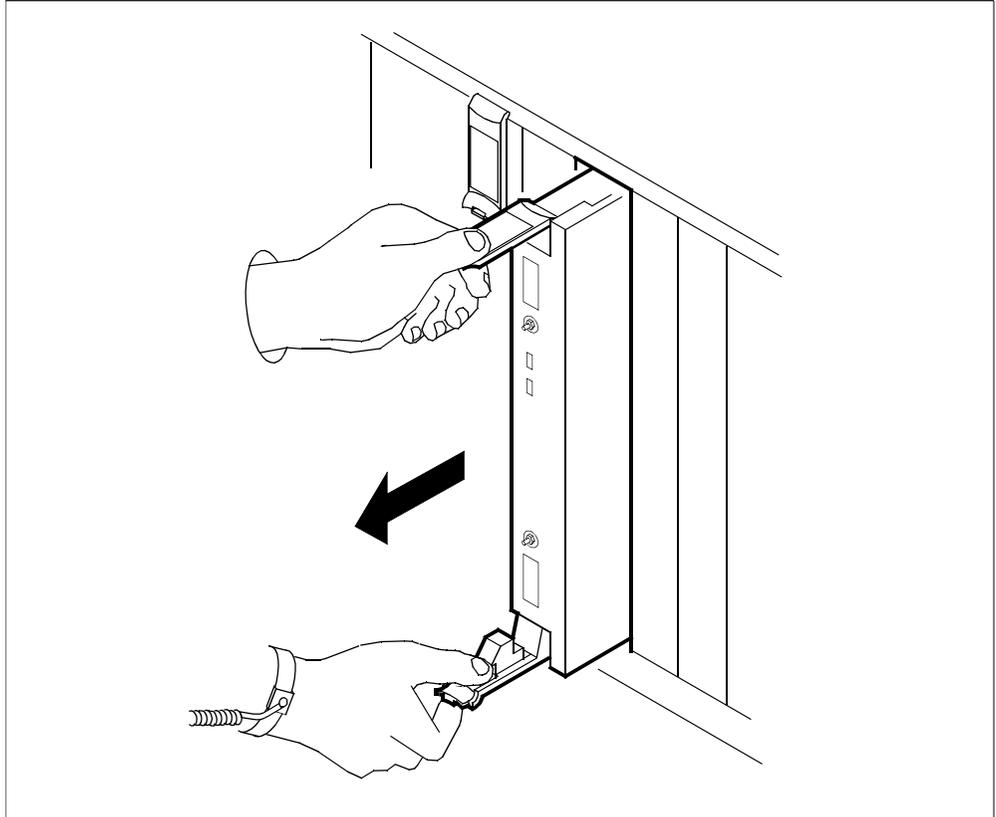
20   Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.
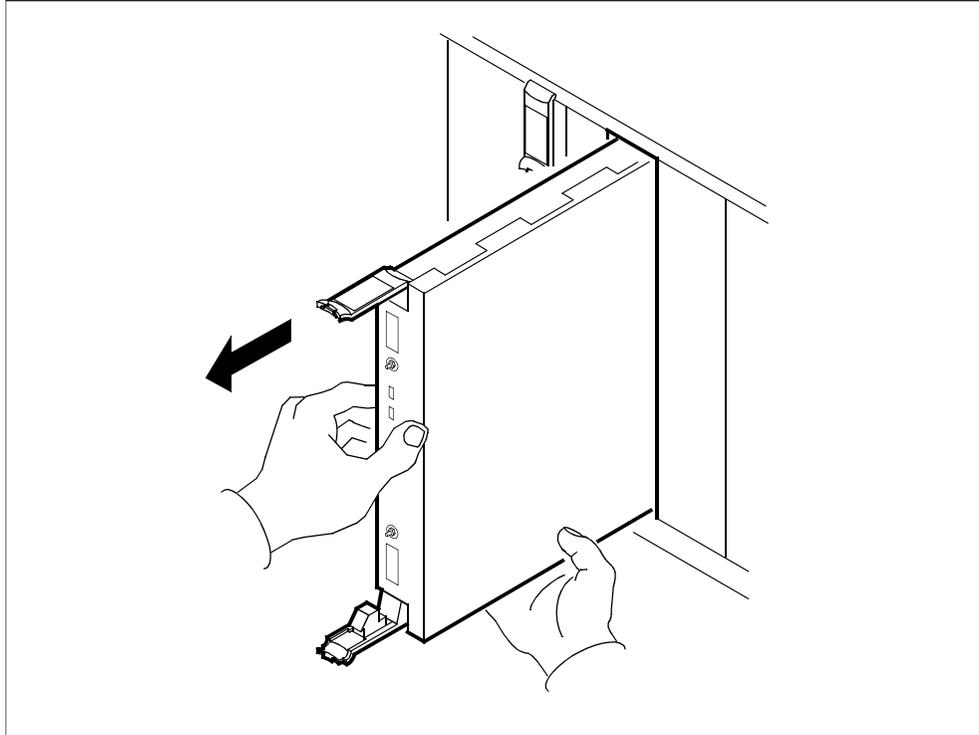
21   Place the module you have removed in an ESD protective container.

22   Insert the replacement module into the CS 2000 Core Manager shelf.

23 Gently slide the module into the shelf until it is fully inserted.
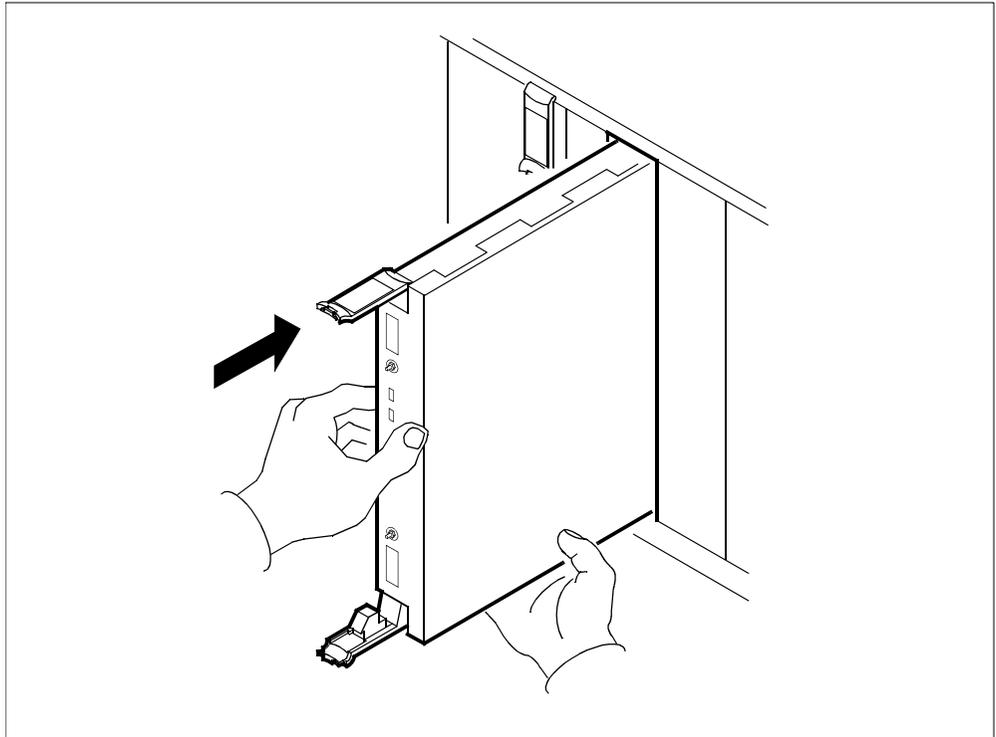
24   Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.

Micro switch
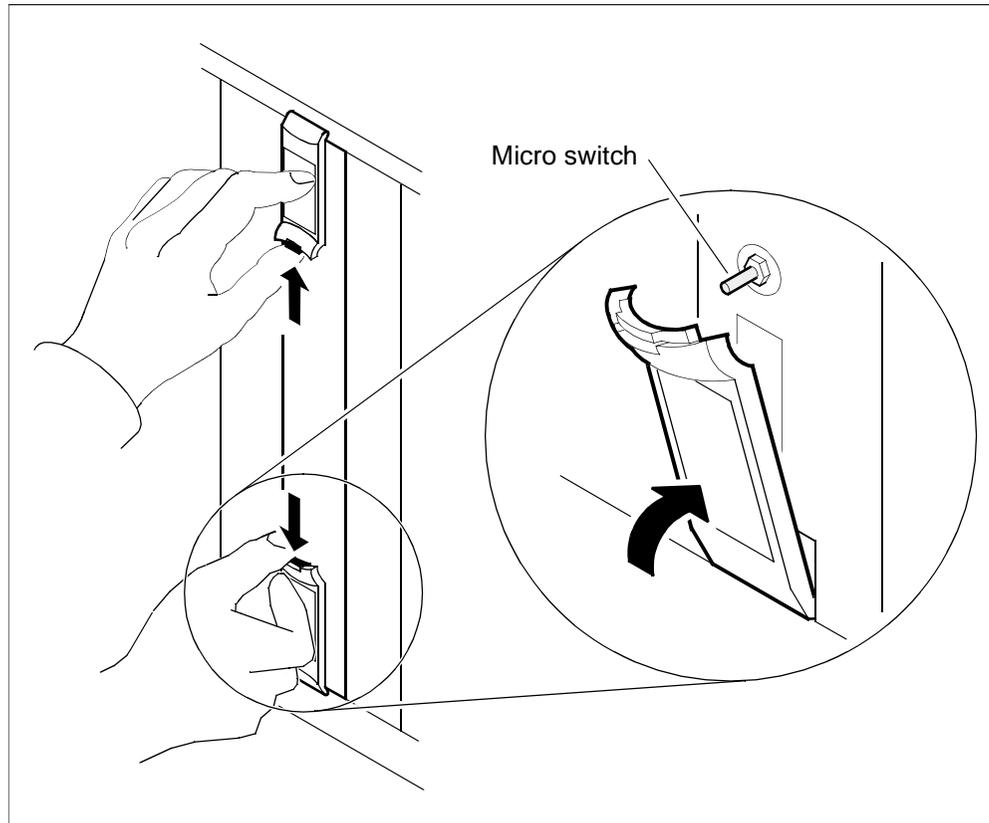
25   Tighten the thumbscrews on the module.

At the local or remote VT100 console

26 Return the DS512 controller module to service by typing

```
> rts <n> 512
```

and pressing the Enter key.

where

> **n**
>> 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 CS 2000 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 you replaced by typing

> **> rts 0 link <*link number*>**

and pressing the Enter key.

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 CS 2000 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 by typing

> **> rts 1 link <*link number*>**

and pressing the Enter key.

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 CS 2000 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

Application

Use this procedure to replace the DS512 personality module, located at the rear of the main chassis (slots 1 and 12) of the CS 2000 Core Manager.

Nortel PEC	Name
NTRX50GH	DS512 personality module

Action

The following flowchart is only 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

Obtain the replacement module

↓

Access the MAP display

↓

Display the MS port modules

↓

Access the MS level of the MAP display

↓

Access the shelf level

↓

Access the MS port module level

↓

Manually busy the DS512 links

↓

Access the hardware level

▽ 1

▽ 1

Manually busy the DS512 controller module

↓

Unseat the DS512 controller module

↓

Remove DS512 personality module

↓

Replace DS512 personality module

↓

Seat the DS512 controller module

↓

Return the DS512 controller to service

↓

Return the DS512 links to service

↓

End

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.
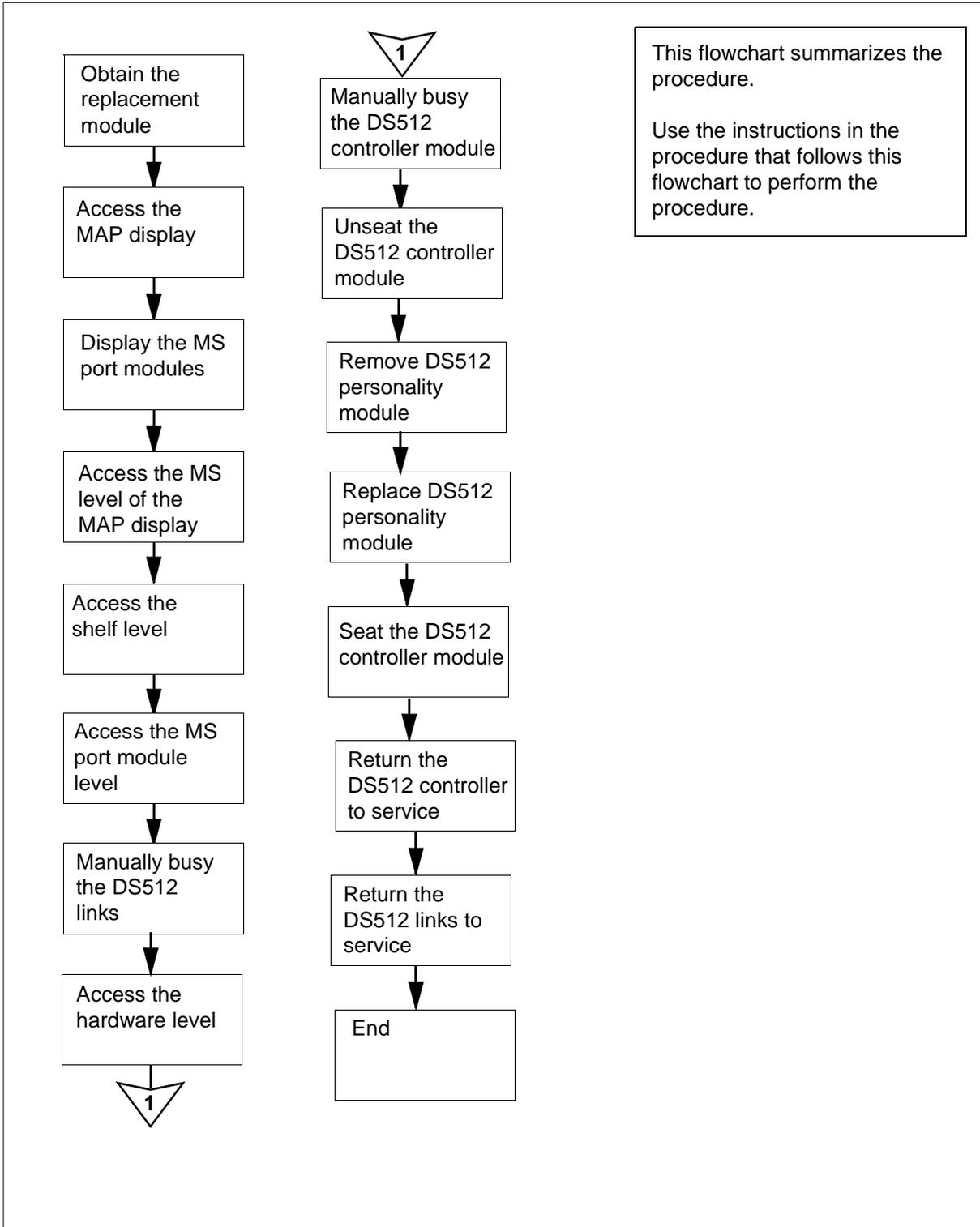
Replacing a DS512 personality module

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 written at the top of the module.

At the MAP display

2   Access the SDM level by typing

      > mapci;mtc;appl;sdm

      and pressing the Enter key.

3   Display the message (MS) port modules which provide the DS512 links to the CS 2000 Core Manager by typing

      > trnsl

      and pressing the Enter key.

      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 CS 2000 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 by typing

      > ms

      and pressing the Enter key.

6   Access the shelf level by typing

      > shelf 0

      and pressing the Enter key.

7 Access the MS chain level associated with the CS 2000 Core Manager DS512 links by typing

> **chain *<cardno>***

and pressing the Enter key.

where

> ***cardno***
> is the MS card number recorded in step 4

8 Busy the DS512 link between MS plane 0 and the CS 2000 Core Manager DS512 personality module you wish to replace by typing

> **bsy 0 link *<link number>***

and pressing the Enter key.

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 CS 2000 Core Manager DS512 personality module you want to replace by typing

> **bsy 1 link <*link number*>**

and pressing the Enter key.

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 CS 2000 Core Manager as the root or maint user.

11 Access the maintenance interface by typing

sdmmtc

and pressing the Enter key.

12 Access the hardware (Hw) level by typing

> **hw**

and pressing the Enter key.

13   Busy the DS512 controller module by typing

```
> bsy <n> 512
```

and pressing the Enter key.

where

> **n**
>> is the domain number (0 or 1) of the DS512 personality module 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 by typing

```
> y
```

and pressing the Enter key.

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*.

Response:

```
Hardware Bsy : Domain 0 Device 512 - Command
complete.
```

> *Note:* At the hardware menu level of the CS 2000 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 CS 2000 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 CS 2000 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 the captive type, and cannot be removed from the module.

17 Depress the tips of the locking levers on the face of the DS512 controller module.
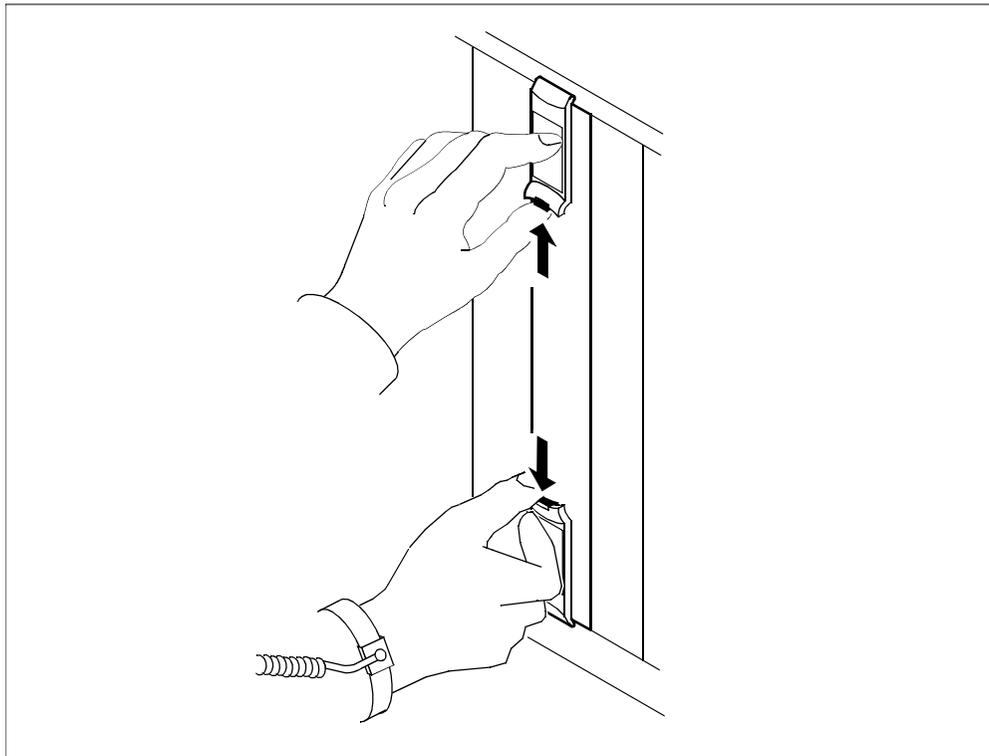
18   Open the locking levers on the face of the DS512 controller module by moving the levers outwards.
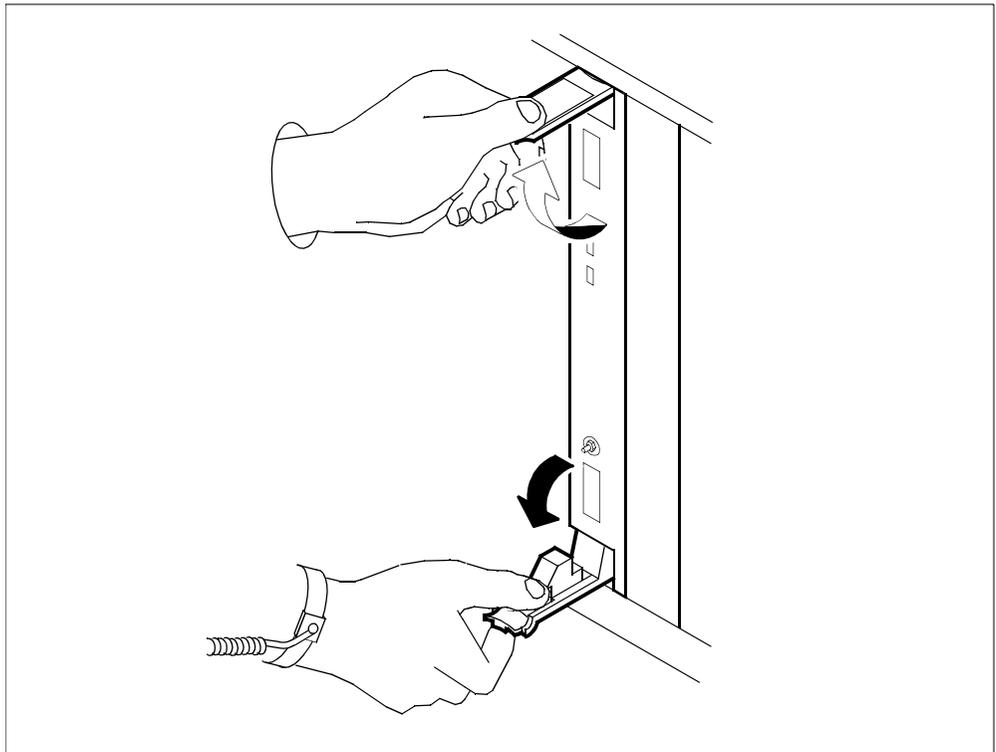
At the back of the CS 2000 Core Manager

19   Loosen the two thumbscrews located at the top and the bottom of the DS512 personality module.

> *Note:* The thumbscrews are the captive type, 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. If you have not already done so, 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 a 1/4 turn to the left.

21   While grasping the thumbscrews, gently pull the DS512 personality module toward you until it protrudes about 2 in. (5.1 cm) from the CS 2000 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.
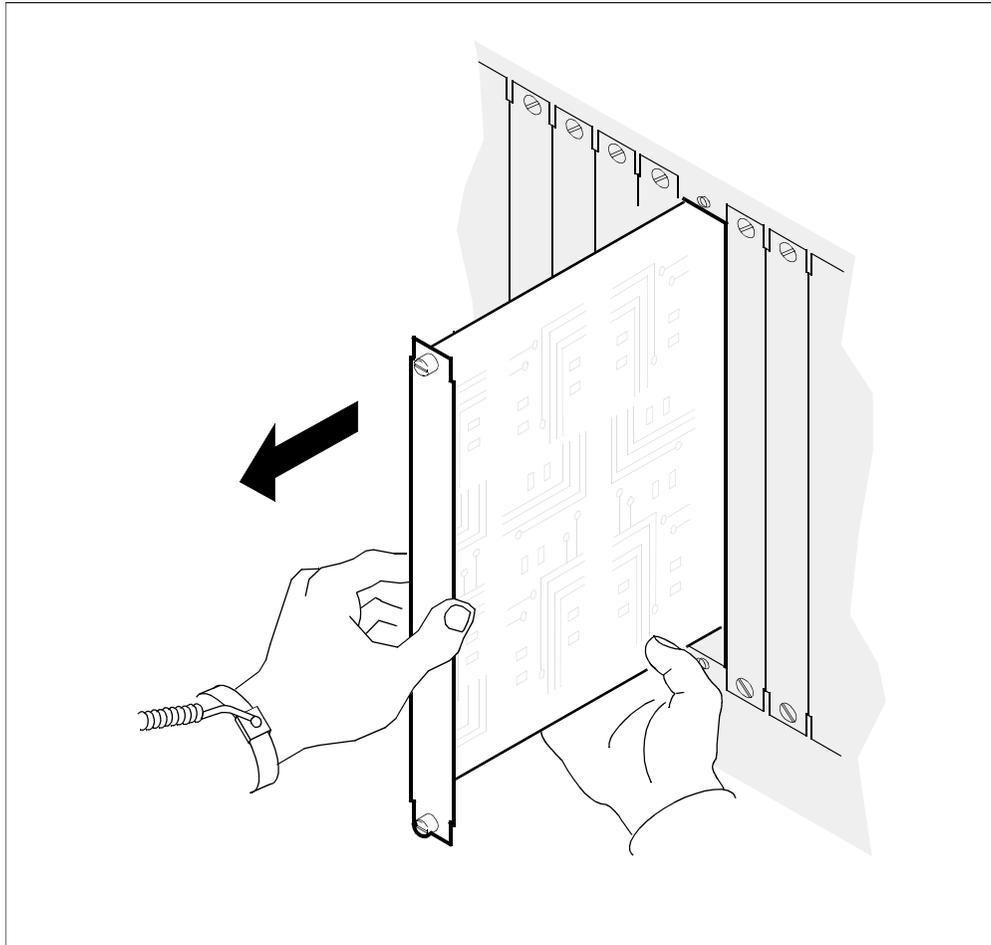
23   Place the DS512 personality module you have removed in an ESD protective container.

24   Insert the replacement DS512 personality module into the CS 2000 Core Manager shelf.

25   Gently slide the DS512 personality module into the shelf until it is fully inserted.
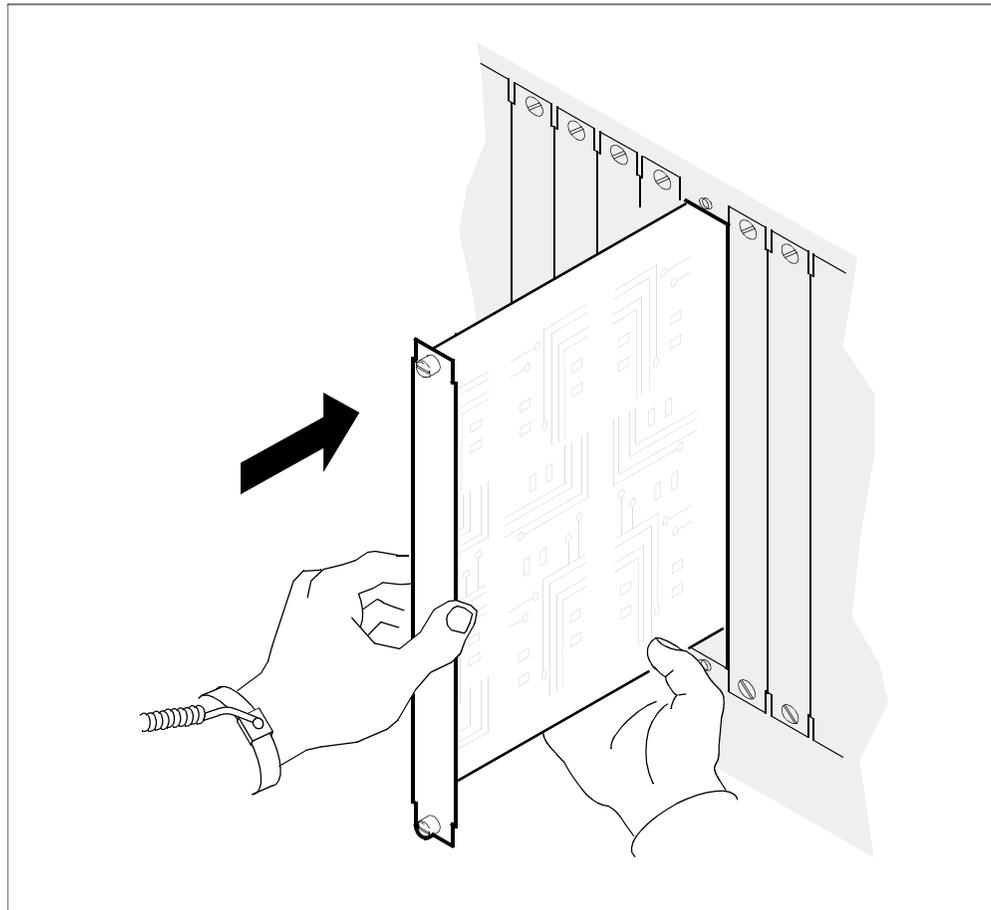
26   Tighten the thumbscrews at the top and the bottom of the DS512 personality module.

27
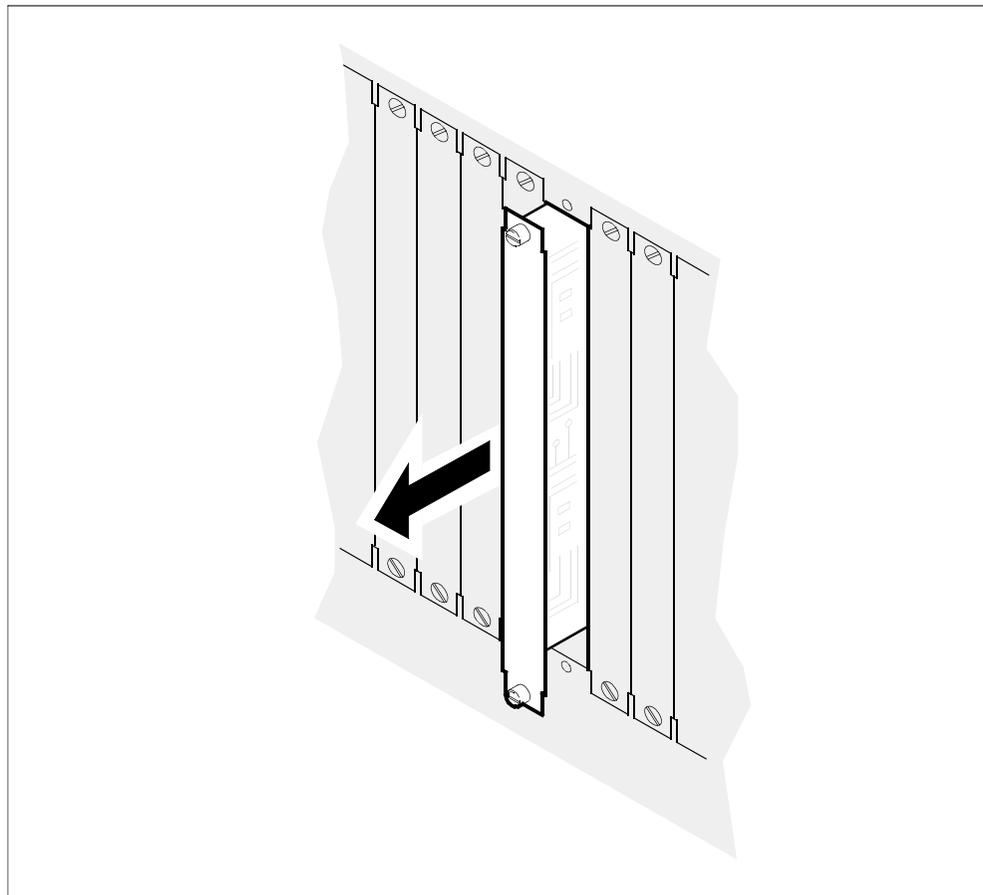
> **CAUTION**
> **Reconnecting transmit and receive cables**
> Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the right.

At the front of the CS 2000 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.
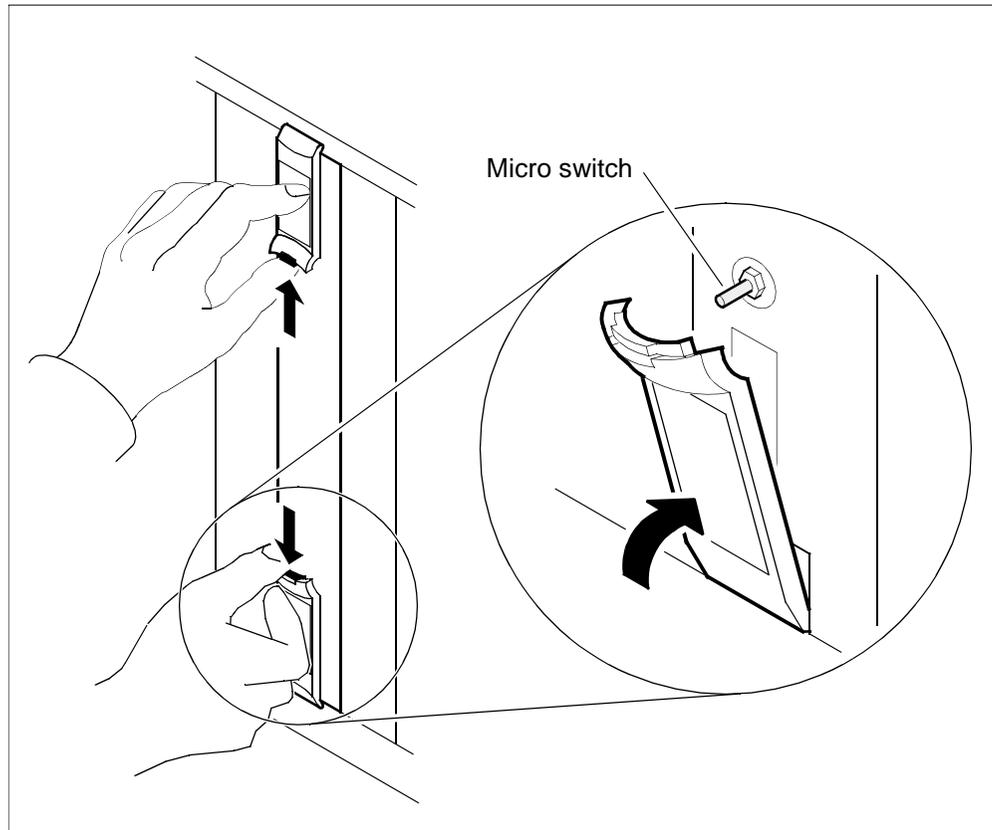
29   Tighten the thumbscrews on the DS512 controller module.

At the local or remote VT100 console

30   Return the DS512 controller module to service by typing

> **> rts <n> 512**

and pressing the Enter key.

where

> **n**
>> 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 CS 2000 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 by typing

> **> rts 0 link <*link number*>**

and pressing the Enter key.

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 CS 2000 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 by typing

> **> rts 1 link <*link number*>**

and pressing the Enter key.

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 CS 2000 Core Manager DS512 link is in-service. Otherwise, the state for DS512 link changes to a "P".

33   You have completed this procedure.

246

Retrieving and viewing log records

This procedure provides instructions on how to retrieve and view CM and CS 2000 Core Manager log records using the CS 2000 Core Manager log query tool.

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

Retrieving and viewing logs

At a terminal or terminal session connected to the CS 2000 Core Manager

1 Log into the CS 2000 Core Manager.

2 Start the log query tool using the default settings by typing

 # logquery

and pressing the Enter key.

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 by typing

> logquery -help

and pressing the Enter key.

4 Enter the your selected command, and press the Enter key.

5 When you are finished, exit the log query tool by typing

> quit

6 You have completed this procedure.

Saving current alarm state information

Complete the following procedure to save the current alarm state information in the snapshot file.

WARNING

Existing snapshot file will be replaced

If the file "snapshot.txt" already exists on the CS 2000 Core Manager hard disk, completing this procedure will cause the old file to be overwritten, destroying its data. If you want to save the data in an existing snapshot file, you must copy the existing snapshot file to a new rfile before completing this procedure. If necessary, refer to Copying a snapshot file in the Fault Management section, before completing this procedure.

Saving current alarm state information

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Save the current alarm state information by typing

      `# snapshot`

      and press the Enter key to save the current alarm state information to the file "snapshot.txt". The CS 2000 Core Manager will display the following response:

```
Taking 'snapshot' of stored alarms

SOCKET call successful
CONNECT call successful
     now connected to Alarm Conduit socket

Sending FILE_WRITE_REQUEST_MSG

Snapshot request accepted

maint:
```

3   You have completed this procedure.

Saving the current display view

Use the following procedure to save a maintenance interface or MAP display view to a text file.

Saving the current maintenance interface or MAP display view

At any workstation or console

1   Use ETA to access the CS 2000 Core Manager or Core.

2   From the File menu in the SDM or CI/MAP Session window, select the Save current view... menu item.

The Set a text file name window appears.

Set a text file name
Filter
/bnr/users/guest/tmp/Attempt.*

Directories	Files
.	ETAmap.12021545
.	ETAmap.12031031
.endoscope	

Selection

/bnr/users/guest/tmp/ETAmap.12040919

[OK]   [Filter]   [Cancel]
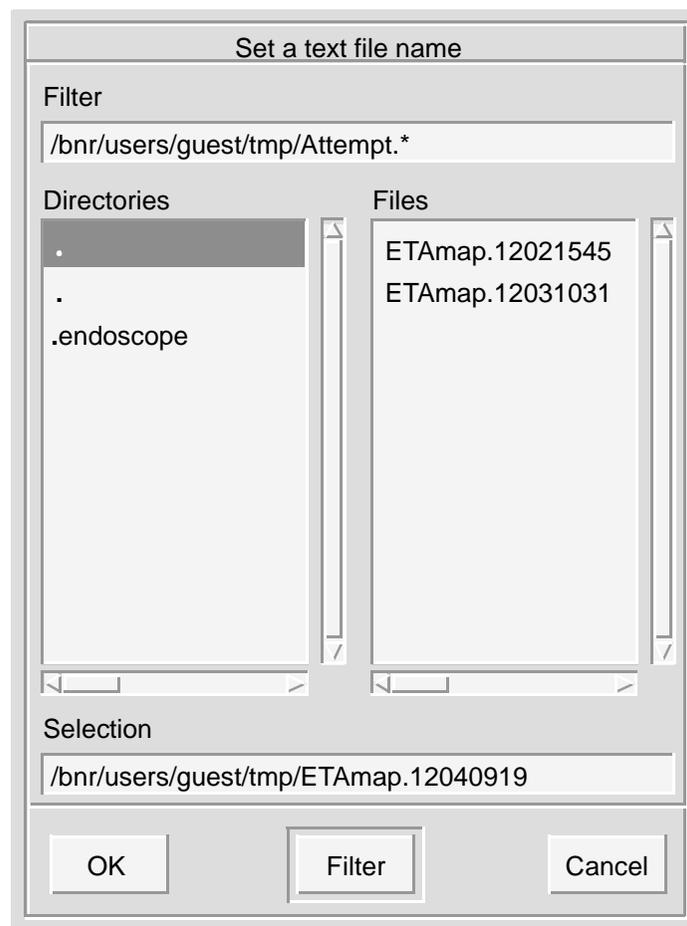
Note: When you select a name for the maintenance interface or MAP display view file, you are prompted for the file name. Nortel Networks recommends that you accept the default file name in the current directory. In the example in step 2, the

default file name is 12021545. 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 4
specify a new file name	step 5

3   Select the default file name by clicking on OK.

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

Note: In the example in step 2, Logging to file /bnr/users/guest/tmp/ETAlog.12040919 indicates that users/guest is the directory where the file is located, ETAlog is the file prefix, and 12040919 is the file extension. The file extension indicates that the file was opened on December 4 (1204), at 9:19 a.m. (0919).

Go to step 6.

4   Select an existing file name by clicking on a file name displayed under the Files heading. Click on OK.

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

Go to step 6.

5   Type a new file name in the Selection heading area of the Set a text file name window. Position the cursor on the default file name extension mmddhhmm and backspace to erase. Go to step 6.

6　　Close the current ETA session window.

If you are in	Do
a CS 2000 Core Manager session	step 7
a CI/MAP session	step 8

7　　Exit the CI/MAP session by typing

> logout

8　　Exit the CS 2000 Core Manager session by typing

 # exit

9　　You have completed this procedure.

Searching for a text string in a snapshot file

Complete the following procedure to search for a text string in an existing snapshot file. If the text string is broken up by white spaces, the string must be enclosed by double quotes.

Searching for a text string in a snapshot file

At any workstation or console

1 Log in to the CS 2000 Core Manager.

2 Search for the text string by typing

 # gacf <text_string> <source_file>

and pressing the Enter key.

where

<text_string> is the string of text to search for

<source_file> is the simple filename of the file to search in

Example response:

```
Trunk,Critical,GC  ,TTT        ,Tue Mar 9  16:13:45  2000

. . .

snapshot.txt:    END
maint:
```

Note: A simple filename does not contain the complete pathname of the file.

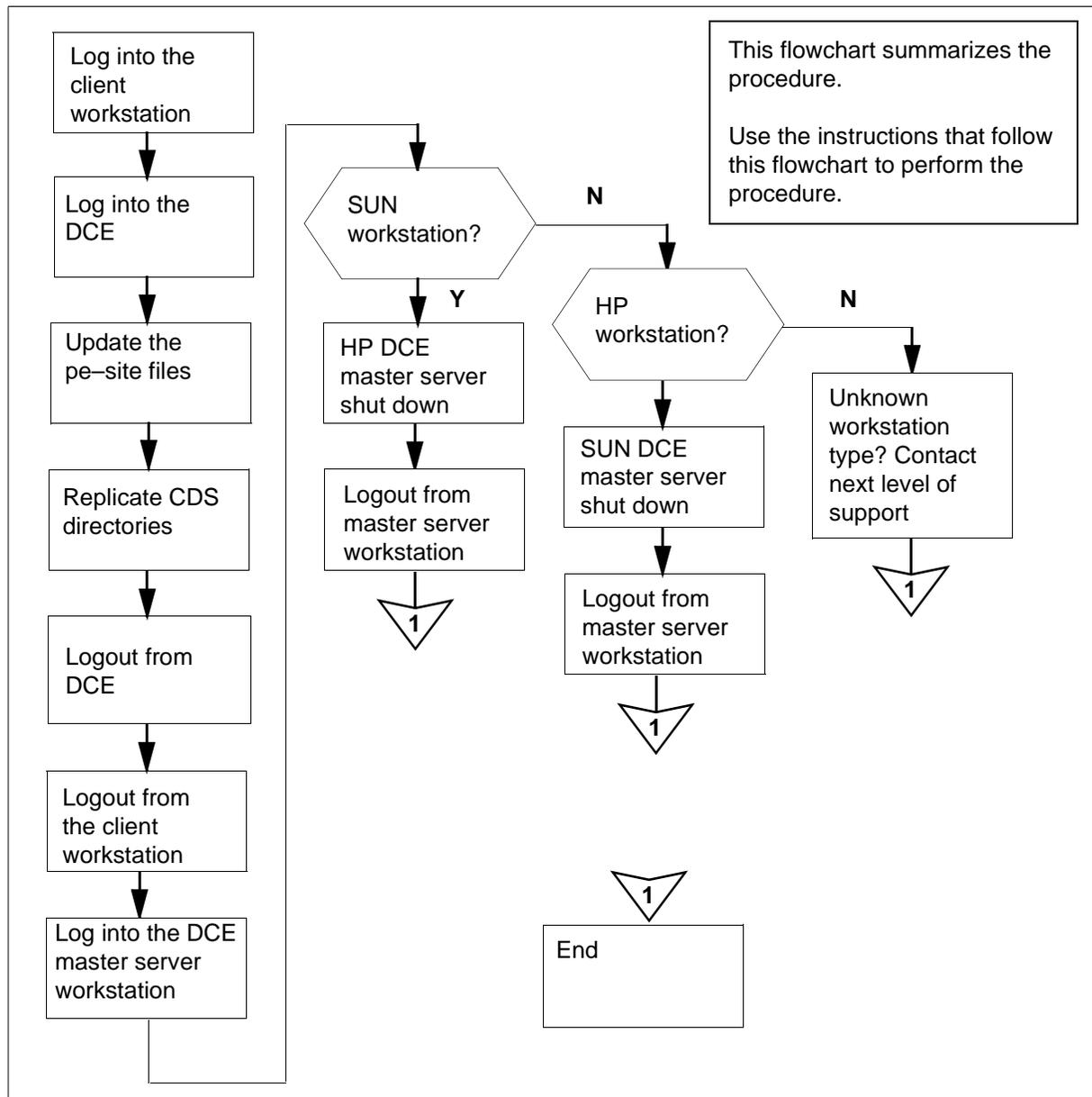**3** You have completed this procedure.

Shutting down the master server

Application

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 that follows the flowchart to perform the task.

Summary of shutting down the master server

```
┌───────────────┐                                    ┌──────────────────────────┐
│ Log into the  │                                    │ This flowchart summarizes│
│ client        │                                    │ the procedure.           │
│ workstation   │                                    │                          │
└───────┬───────┘                                    │ Use the instructions that│
        │                                            │ follow this flowchart to │
        ▼                                            │ perform the procedure.   │
┌───────────────┐                                    └──────────────────────────┘
│ Log into the  │         ⬡ SUN              N
│ DCE           │        workstation? ──────────────┐
└───────┬───────┘              │                     │
        │                      │ Y                   ▼
        ▼                      ▼              ⬡ HP           N
┌───────────────┐      ┌──────────────┐      workstation? ──────────┐
│ Update the    │      │ HP DCE       │           │                 │
│ pe–site files │      │ master server│           │                 ▼
└───────┬───────┘      │ shut down    │           ▼          ┌──────────────┐
        │              └──────┬───────┘    ┌──────────────┐  │ Unknown      │
        ▼                     │            │ SUN DCE      │  │ workstation  │
┌───────────────┐             ▼            │ master server│  │ type? Contact│
│ Replicate CDS │      ┌──────────────┐    │ shut down    │  │ next level of│
│ directories   │      │ Logout from  │    └──────┬───────┘  │ support      │
└───────┬───────┘      │ master server│           │          └──────┬───────┘
        │              │ workstation  │           ▼                 │
        ▼              └──────┬───────┘    ┌──────────────┐         ▼
┌───────────────┐            │            │ Logout from  │         ▽ 1
│ Logout from   │            ▽ 1          │ master server│
│ DCE           │                         │ workstation  │
└───────┬───────┘                         └──────┬───────┘
        │                                        │
        ▼                                        ▽ 1
┌───────────────┐
│ Logout from   │
│ the client    │
│ workstation   │                                ▽ 1
└───────┬───────┘                         ┌──────────────┐
        │                                 │ End          │
        ▼                                 └──────────────┘
┌───────────────┐
│ Log into the  │
│ DCE master    │
│ server        │
│ workstation   │
└───────────────┘
```

Shutting down the master DCE server

┌───┐
| **ATTENTION**
| This procedure must be performed by a trained Distributed
| Computing Environment (DCE) system administrator who knows
| DCE administration procedures.
└───┘

At the CS 2000 Core Manager client workstation

1   Log into the client workstation.

2   Log into DCE by typing

> **> dce_login <administrator name>**

and pressing the Enter key.

where

> **administrator name**
> is the userID of the administrator.

3   Enter the administrator password, and press the Enter key.

4   Access the /sdm/bin directory by typing

> **> cd /sdm/bin**

and pressing the Enter key.

5   Update the pe_site file by typing

> **> ./update_pe_site**

and pressing the Enter key.

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 by typing

> **> y**

and pressing the Enter key.

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 by typing

> **> ./replicate_cds_dirs**

and pressing the Enter key.

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 by typing

> y

and pressing the Enter key.

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 by typing

> exit

and pressing the Enter key.

10   Log out of the client workstation by typing

> exit

and pressing the Enter key.

11   Log into the DCE master server workstation as the root user.

12   Determine the operating system by typing

> uname

and pressing the Enter key.

Example response:

```
HP-UX
```

13   Use the following table to determine your next step.

If the O/S you are running is	Do
HP-UX	step 14, 15, and 19
SunOS	step 16, 17, and 19
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 by typing

> `> exit`

and pressing the Enter key.

Go to step 19.

16   Follow the SUN vendor's DCE configuration instructions to shut down the master server.

17   Log out of the master server workstation by typing

> `> exit`

and pressing the Enter key.

Go to step 19

18   For this type of operating system, contact your next level of support.

19   You have completed this procedure.

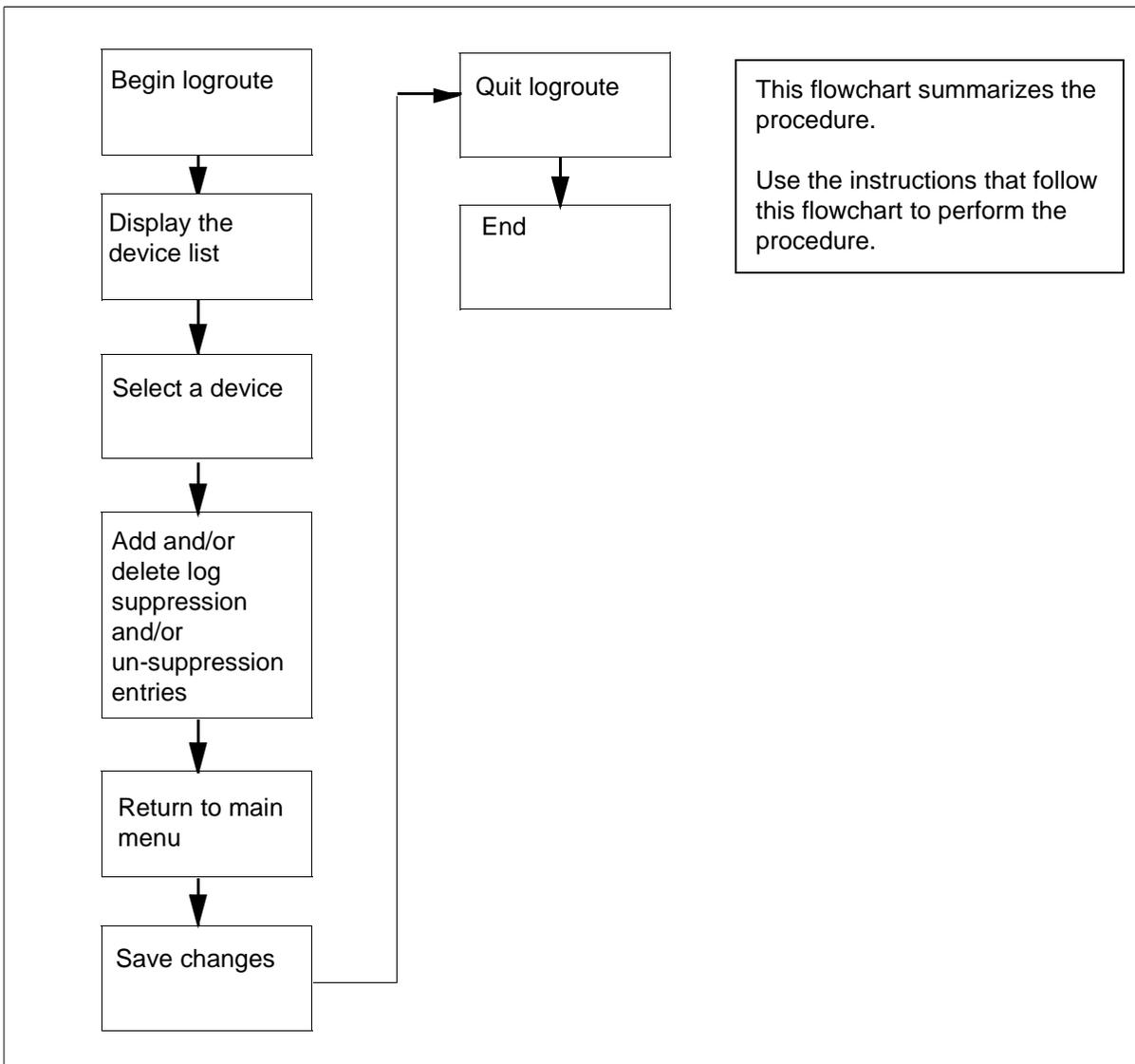## Specifying the logs delivered to a device

Application

Use this procedure to add or remove entries that suppress or un-suppress logs for a specific device. The rules you enter for each device only accommodate the set of logs defined in the procedure [Changing the set of logs sent from the CM](#) in the Fault Management section. Logs that are being suppressed at the CM cannot be unsuppressed for a specific device.

Action

The following flowchart provides a description of the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of specifying the logs delivered to a specific device

```
┌──────────────┐        ┌──────────────┐        ┌────────────────────────┐
│ Begin logroute│   ┌──▶│ Quit logroute │        │ This flowchart summarizes│
│              │   │    │              │        │ the procedure.          │
└──────┬───────┘   │    └──────┬───────┘        │                         │
       │           │           │                │ Use the instructions    │
       ▼           │           ▼                │ that follow this        │
┌──────────────┐   │    ┌──────────────┐        │ flowchart to perform    │
│ Display the  │   │    │     End      │        │ the procedure.          │
│ device list  │   │    │              │        │                         │
└──────┬───────┘   │    └──────────────┘        └────────────────────────┘
       │           │
       ▼           │
┌──────────────┐   │
│ Select a device│ │
│              │   │
└──────┬───────┘   │
       │           │
       ▼           │
┌──────────────┐   │
│ Add and/or   │   │
│ delete log   │   │
│ suppression  │   │
│ and/or       │   │
│ un-suppression│  │
│ entries      │   │
└──────┬───────┘   │
       │           │
       ▼           │
┌──────────────┐   │
│ Return to main│  │
│ menu         │   │
└──────┬───────┘   │
       │           │
       ▼           │
┌──────────────┐   │
│ Save changes │───┘
│              │
└──────────────┘
```

Specifying the logs delivered to a specific device

At the CS 2000 Core Manager

1 Log in to the CS 2000 Core Manager.

2 Begin the logroute application by typing

   # logroute

   and pressing the Enter key.

   The Logroute Main Menu screen appears.

At the logroute application screen

3   Change the parameters of an item in the logroute menu by typing

```
> c
```

and pressing the Enter key.

Response:

```
Enter number of main menu option ==>
```

4   Display the device list by typing

```
> 1
```

and pressing the Enter key.

The Device List screen appears.

5   Change a device by typing

```
> c
```

and pressing the Enter key.

Response:

```
Enter number of device to change ==>
```

6   Enter the device number for which you want to add or delete a routing entry and press the Enter key. The screen for that device will appear. An example of a TCP device screen (the second device listed on the screen capture in step 4) appears below.

Example response:

```
                        TCP Device

Device Parameters
                    1 – HOST IP          :47.208.11.123
                    2 – PORT             :1024
                    3 – FORMAT           :SCC2

Log Routing




c:change parameter, a:add log routing, d:delete log routing
f:forward, b:back, q:quit, h:help, p:previous menu, m:main menu

Enter command ==>
```

7 Use the following table to determine your next step.

If you want to	Do
add an entry	step 8
delete an entry	step 14

8 Add a log routing entry by typing

`> a`

and pressing the Enter key.

Response:

`Enter - a:addrep or d:delrep ==>`

> **Note:** The maximum number of log routing entries you can enter is 30 entries. If you have 30 entries, and you want to add another entry, you must replace one of the existing entries to add the new entry.

9 Use the following table to determine your next step.

If you want to	Do
suppress logs	step 10
un-suppress logs	step 12

10 Add a routing entry that suppresses logs (causes them not to be routed to the device) by typing

`> d`

and pressing the Enter key.

Response:

`Enter log identifier ("log_type", or "log_type`
`log_number") ==>`

11 Enter a log type or a combination of log type and log number and press the Enter key. The new entry is added to the log routing list on the screen.

> *Note 1:* An example of a log type is type "PM." This entry will suppress all logs of type PM.

> *Note 2:* An example of a combined log type and log number is type "PM 181." This entry will suppress the PM181 log but leave the routing of other PM logs unchanged.

If you	Do
want to make further changes	step 7
do not want to make further changes	step 16

12 Add a routing entry that un-suppresses logs (causes them to be routed to the CS 2000 Core Manager) by typing

```
> a
```

and pressing the Enter key.

Response:

```
Enter log identifier ("log_type", or "log_type
log_number") ==>
```

13 Enter a log type or a combination of log type and log number and press the Enter key. The new entry is added to the log routing list on the screen.

> *Note 1:* An example of a log type is type "PM." This entry will suppress all logs of type PM.

> *Note 2:* An example of a combined log type and log number is type "PM 181." This entry will suppress the PM181 log but leave the routing of other PM logs unchanged.

If you	Do
want to make further changes	step 7
do not want to make further changes	step 16

14 Delete a log routing entry by typing

> **d**

and pressing the Enter key.

Response:

```
Enter log routing number to delete ==>
```

15 Type the number of the entry you want to delete from the log routing list on the screen, and press the Enter key. The entry you specified will be deleted from the log routing list.

> *Note:* Use caution when deleting entries in the log routing list because the order of the log routing list is very important. Each entry impacts the entries following it in the log routing list. Therefore, deleting an entry may change the effect of any following entries.

If you	Do
want to make further changes	step 7
do not want to make further changes	step 16

16 Return to the main menu by typing

> **m**

and pressing the Enter key.

17 Save the changes you have made by typing

> **s**

and pressing the Enter key.

Response:

```
Warning: Some log devices will be restarted. Do
you wish to proceed?
```

18 Confirm the save command by typing

> **y**

and pressing the Enter key.

Response:

```
Save data completed -- press return to continue
```

19 Press the Enter key to continue.

20   Quit the logroute application by typing

> `> q`

and pressing the Enter key.

21   You have completed the procedure.

270

Starting the ETA server on the CS 2000 Core Manager

The ATA and ETA clients run on any remote workstation that is configured in the DCE cell. Along with the ETA server on the CS 2000 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.

Note: 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 Configuration Management section.

Starting the ETA server on theCS 2000 Core Manager

At the local or remote VT100 console

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

2   Access the maintenance interface by typing

`maint: sdmmtc`

and pressing the Enter key.

3   Access the application (Appl) level by typing

`> appl`

and pressing the Enter key.

4   The application menu lists the software packages installed on the CS 2000 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 by typing

`> bsy <n>`

and pressing the Enter key.

where

> **n**
> is the number next to the Enhanced Terminal Access application.

6 Start the ETA application by typing

`> rts <n>`

and pressing the Enter key.

where

> **n**
> is the number next to the ETA application.

Note: The state of Enhanced Terminal Access shown at the application level must be InSv. The Enhanced Terminal Access application is dependent on the DCE service on the CS 2000 Core Manager. If DCE is not in service, then Enhanced Terminal Access will be off-line.

7 You have completed this procedure.

Transferring a snapshot file using FTP

To move an alarm conduit snapshot file to another machine using FTP, the following information is required:

- the name of the snapshot file
- the IP address of the FTP host
- a valid user ID and password on the FTP host

Complete the following procedure to transfer a snapshot file to another machine.

Transferring a snapshot file using FTP

At the CS 2000 Core Manager

1   Type

> **> ftpacf <ip_address>**

and press Enter to start the FTP session.

where

<ip_address> is the IP address of the FTP host

The system prompts you for your login and password.

2   Enter your login and password for the destination host.

Response:

```
rftp>
```

3   Type

> **> bin**

and press the Enter key to change the transfer mode to binary.

4   If it is necessary to change the desired target directory, type

> **> cd <path_name>**

and press Enter.

where

<path_name> is the desired target directory on the destination host.

5   Type

> **put <source_file>**

and press the Enter key to copy the snapshot file to the
destination host.

where

<source_file> is the simple filename of the file to FTP.

```
200 PORT command successful.
150 Opening ASCII mode data connection for filename.
226 Transfer complete.
number bytes sent in time (bytes/s)
rftp>
```

> *Note:* A simple filename does not contain the complete
> pathname of the file. In the preceding example, the CS 2000
> Core Manager displays the response.

6   Type

> **quit**

and press the Enter key to exit the FTP session.

The CS 2000 Core Manager displays the file to be deleted.

7   You have completed this procedure.

Troubleshooting DCE

> **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's DCE version 2.0 did contain these executables. IBM documentation explains this change in "Chapter 26. Interoperation with Network Time Protocol" of the "IBM DCE Version 3.1 for AIX and Solaris: Administration Guide--Core Components," at http://www-4.ibm.com/software/network/dce/library/publications/dce31aix.html.
>
> 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.
>
> Be aware that CS 2000 Core Manager applications requiring DCE will not successfully configure into a 3.1 cell without the dts_ntp_provider or dts_null_provider binaries present. In their absence, DCE applications will be inoperable. You may contract with Nortel Global Professional services to install and configure the DCE cell. Their installation includes the proper configuration for the required time-provider executables.

The DCE troubleshooting procedures provide information for solving operational DCE administration problems. It defines the cause of the problem, and offers solutions. These procedures should be used by qualified DCE administrators only.

The problems are grouped into four categories as follows:

1. problems pertaining to DCE Security Service (SEC)
2. problems pertaining to DCE Cell Directory Service (CDS)

3. problems pertaining to DCE Distributed Time Service (DTS)

4. miscellaneous (MISC)

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 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

   This records the events which indicate an unexpected error occurred.

- /opt/dcelocal/var/svc/fatal.log.

   This records the events which indicate an unrecoverable error occurred.

- /opt/dcelocal/var/svc/warning.log

   This records the events which indicate an error that was corrected automatically.

DCE Security Service (SEC) 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: dce_login with valid DCE principal name and password.

SEC004: Failure of dce_login on CS 2000 Core Manager

Symptom: On the CS 2000 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: dce_login with valid DCE principal name and password

SEC005: Failure of dce_login on HP or SUN

Symptom: On HP, or CS 2000 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're trying to log in 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 CS 2000 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 in directory /opt/dcelocal/var/security/creds. Perhaps the disk partition is full. The directory may also not be writable.

If on SUN, you can run dce_login under truss as follows:

truss -f dce login

This will identify 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. Then, restart it with the following command:

secd - locksmith fooBar -lockpw

This command results in the following actions:

1. You will be prompted for a password for account fooBar. FooBar is the locksmith account.
2. Secd will restart normally but will not drop into the background

3. Locksmith mode will arrange for fooBar's account to be valid.

4. FooBar will be granted 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 cell_admin's 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" 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. Then enter the following command:

```
dce_login hosts/hostname/self -k /krb5/v4srvtab
```

where

hostname
    is the name of the local workstation.

You must be in root to enter this command. Replace the word "hostname" with the hostname for your local client workstation. The dce_login command will attempt to login as hosts/*hostname*/self using the keytab /krb5/v5srvtab of the client workstation.

If dce_login is successful, the secval should start. Stop and restart the DCE.

If dce_login fails, then go to the dce_login 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

CDS001: DCE startup script hangs with two cdsadv processes running

Symptom: On the CS 2000 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:

1. the cache file on disk is corrupted because the system crashed when a previous cdsadv process was writing to it

2. the cdsadv process underwent "kill -9" while it was saving to disk

3. /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 cdsadv process

3. remove the faulty line in /etc/hosts file

4. ensure 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 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 may be occurring because your system IPC resources are used up. Perhaps the semaphores have not been unlocked by other software. Also, the kernel parameters may have been set too small 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.

You may need to 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 should be set to the same value as seminfo_semmni.

It is recommended that the following lines be added 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

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.

If you need to configure more DTS servers, configure them.

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 will only persist until dtsd is stopped. The command must be reissued each time dtsd is restarted.

DTS002: Undetermined drift

Symptom: DCE is ISTb on the CS 2000 Core Manager. The log indicates the following message.

```
DTS Clock not synchronized, undetermined drift.
```

Possible Cause: The following reasons may be causing the problem:

1. The lan-profile name of the CS 2000 Core Manager is not correct.

2. 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.

- If the lan-profile name is not correct, then re-commission DCE with the correct LAN profile.

- If the number of dts servers is less than the value of the minservers attribute, change the default value of minservers attribute. 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 talk to a remote DTS server. The server is not responding, or the local machine's LAN profile is missing or empty.

Solution: Refer to the solutions offered for problem numbers DTS001: Too few dts servers and DTS002: Undetermined drift.

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 for more information on configuring your IPC resources.

DTS005: DCE configuration fails

Symptom: On CS 2000 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 such a situation.

Solution: Create a /var/locks directory with world-writable permission, and restart the DTS daemon.

DTS006: DCE configuration on the CS 2000 Core Manager failed on *start DTS daemon*

Symptom: After the hot removal or insertion on the CS 2000 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: Type 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.

Miscellaneous (MISC) Problems

MISC001: Failure of "dcecp hostdata" commands

Symptom: On HP, CS 2000 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 CS 2000 Core Manager, HP or SUN:

1. On CS 2000 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 may not be 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 the hosts. On DCE client hosts, you should see dced and cdsadv daemons. You may also see one or more cdsclerk and dtsd daemons. On DCE servers, you should see the dced and dtsd daemons. 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 particular machine, check the DCE configuration file. Then 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 should be running the dced daemon. Check the processes running on the workstation

to confirm that the dced daemon is running. Also, 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. On 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. If the file has a line that says *SECD=0*, the secd daemon is not running on the workstation.

- On the CS 2000 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 may hang also when at attempt is made to start DCE on CS 2000 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:

1. DCE was stopped and immediately restarted. The operating system will wait three minutes before marking TCP port 135 as available for use again.

2. Another process is using port 135.

Solution: If DCE was immediately stopped and restarted, the DCE startup script will hang for a few minutes. TCP port 135 will then be available again.

There should not be any other process off port 135.

> **Note:** llbd may 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 will fail 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 may have been talking to and all 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 CS 2000 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 CS 2000 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 CS 2000 Core Manager. Refer to the procedure "Configuring the CS 2000 Core Manager in a DCE cell" in the Configuration Management section.

Troubleshooting Log Delivery problems

This section describes fault conditions affecting Log Delivery operation and how to isolate and clear them. Use the procedure to

- troubleshoot why the state of the log delivery application is ISTb
- change the state of the log delivery application from ISTb to InSv

Fault conditions affecting Log Delivery

Lost logs

Lost logs can be detected by examining the sequence numbers of the logs at a client output device and determining if they are sequential. If they are not sequential, logs are likely being lost. To clear the problem, access the Log Delivery commissioning tool, select the Global Parameters menu, and increase the buffer size.

No logs being received at a Log Delivery client

If no logs are being received at a Log Delivery client, check the following Log Delivery commissioning parameters:

- At the Device List menu of the Log Delivery commissioning tool, verify that the client is defined, and that the log stream for the client is defined.

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 or SCC2).
- At the Global Parameters menu, check that the parameters for start and end of line, and start and end of log, are set correctly.

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 may be 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 follows:

```
* SDM303
  Package: SDM_BASE.logs
  Process: start_sdmlaq
  Trouble condition asserted
  Reason: No available CM log devices
  Mon Feb 5 04:09:14 2001
```

The 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.
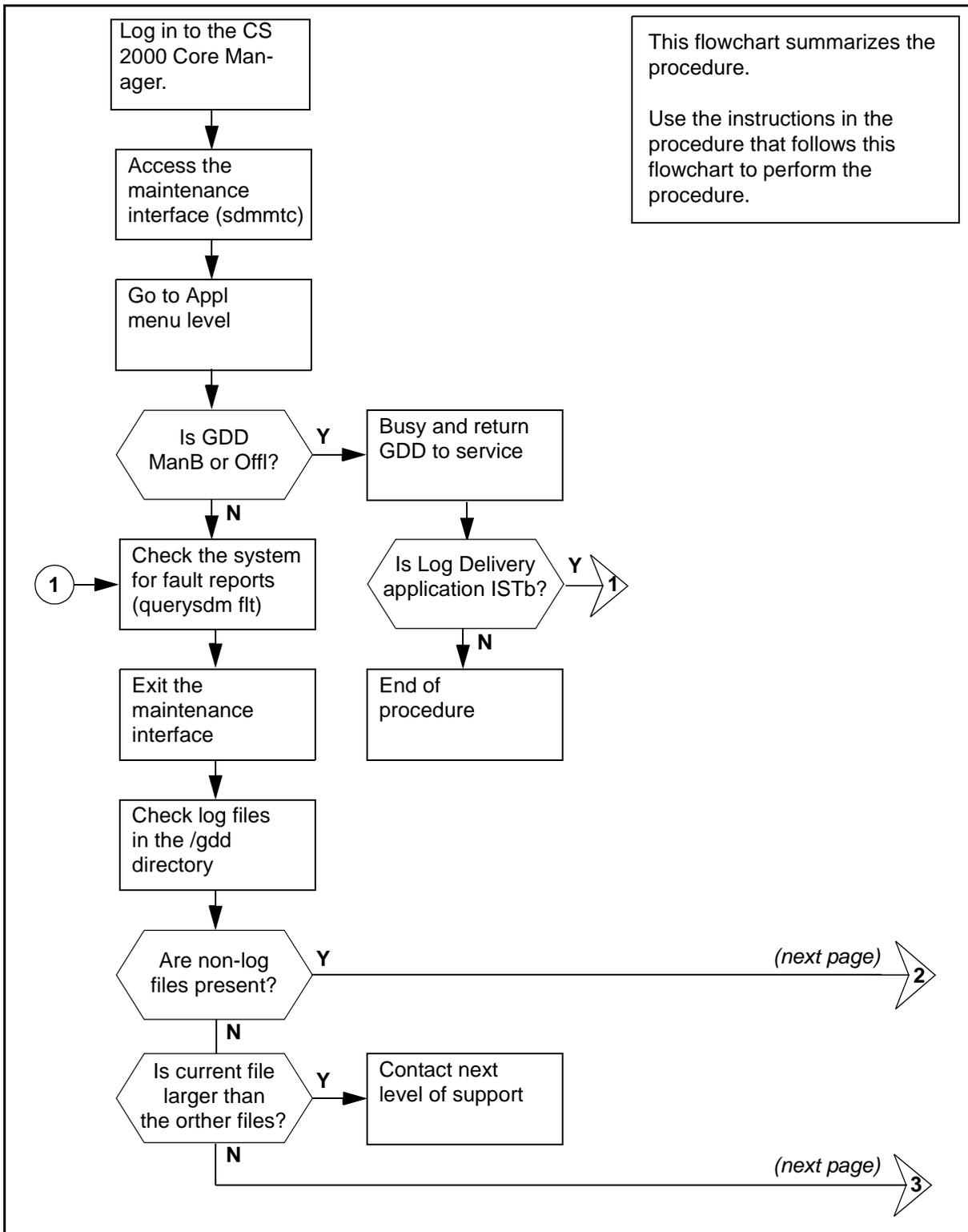
Interval

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 procedure.

Summary of troubleshooting the Log Delivery application when its node state is ISTb *(page 1 of 2)*

Log in to the CS 2000 Core Manager.

↓

Access the maintenance interface (sdmmtc)

↓

Go to Appl menu level

↓

Is GDD ManB or Offl? —**Y**→ Busy and return GDD to service

N ↓

(1) → Check the system for fault reports (querysdm flt)

↓

Exit the maintenance interface

↓

Check log files in the /gdd directory

↓

Are non-log files present? —**Y**→ *(next page)* 2

N ↓

Is current file larger than the orther files? —**Y**→ Contact next level of support

N ↓

(next page) 3

Busy and return GDD to service ↓ Is Log Delivery application ISTb? —**Y**→ 1

N ↓

End of procedure

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

Summary of troubleshooting the Log Delivery application when its node state is ISTb *(page 2 of 2)*

```
(2) → [ Delete non-log
        files from shell ]
            │
            ▼
     [ Check Appl level
       of maintenance
       interface ]
            │
            ▼
    < Is Log Delivery      Y    [ Exit maintenance
      application ISTb? > ─────→   interface and go
            │                      to /gdd directory ]
            │ N                          │
            │                            ▼
            │                   < Is current file    Y   [ Contact next
            │                     larger than the  ─────→   level of support ]
            │                     other files? >
            │                            │ N
            │                            ▼
            │          (3) →    [ Access the
            │                     maintenance
            │                     interface ]
            │                            │
            │                            ▼
            │                   [ At storage level
            │                     increase size of
            │                     /gdd file system ]
            │                            │
            │                            ▼
            │                   [ Busy and return
            │                     Log Delivery appl.
            │                     to service ]
            │                            │
            │                            ▼
            │                   < Is Log Delivery     Y   [ Contact next
            │                     application ISTb? ─────→   level of support ]
            │                            │
            │                            │ N
            │                            ▼
            └───────────────→   [ End of
                                  procedure ]
```

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

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 by typing

  # sdmmtc

  and pressing the Enter key.

3   Access the application level (Appl) by typing

  > appl

  and pressing the Enter key.

4   Use the following table to determine your next step.

If GDD is	Do
Offl	step 5
ManB	step 6
InSv	step 8

5   Busy the GDD application by typing

  > bsy <fileset_number>

  and pressing the Enter key.

  where

    fileset_number
      is the number next to the GDD application

6   Return the GDD application to service by typing

  > rts <fileset_number>

  and pressing the Enter key.

  where

    fileset_number
      is the number next to the GDD application on the screen.

    Note: Wait at least 1 min. for the ISTb state to change to InSv.

7   Use the following table to determine your next step.

If the Log Delivery application	Do
remains ISTb	step 8
goes InSv	you have completed this procedure

8   Check the CS 2000 Core Manager for any faults by typing

> **`querysdm flt`**

and pressing the Enter key.

9   Use the following table to determine your next step.

If	Do
a fault report indicates "log file is circulating (losing logs)"	step 10
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 25

10   Exit the maintenance interface by typing

> **`quit all`**

and pressing the Enter key.

11   Access the /gdd directory by typing

`cd /gdd`

and pressing the Enter key.

> *Note:* You must be a root user of the CS 2000 Core Manager to continue with the procedure.

12   Check all log files by typing

`ls -l`

and pressing the Enter key.

13   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 14
all files start with LOGS.recorddata	step 20

14   Delete files that are not log files by typing

 # rm <*file*>

and pressing the Enter key.

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.

15   Return to the maintenance interface by typing

 # sdmmtc

and pressing the Enter key.

16   Access the application level (Appl) by typing

> appl

and pressing the Enter key.

17   Determine if the state of the log delivery application is ISTb. Wait at least 1 min. to for the ISTb state to change to InSv.

If the Log Delivery application	Do
remains ISTb	step 18
goes InSv	you have completed this procedure

18   Exit the maintenance interface by typing

> quit all

and pressing the Enter key.

19   Access the /gdd directory by typing

```
# cd /gdd
```

and pressing the Enter key.

20   Check the log files by typing

```
# ls -l
```

and pressing the Enter key.

21   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 22

22   Return to the maintenance interface by typing

```
# sdmmtc
```

and pressing the Enter key.

23   Access the storage level by typing

```
> storage
```

and pressing the Enter key.

24   Increase the size of the /gdd file system by typing

```
> change lv /gdd <Mbytes>
```

and pressing the Enter key.

where

> **Mbytes**
> is the number of megabytes you want to increase the current size of the /gdd file system by

Note: Nortel Networks recommends that you set the size of the /gdd file system to be equal to the required capacity for 12 hours of log files, multiplied by 2 (to get a 24 hour file size) then multiplied by 50 days. This should provide 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 the average size of a 12 hour log file in the /gdd file system

25 Busy the Log Delivery application by typing

```
> bsy <fileset_number>
```

and pressing the Enter key.

where

> **fileset_number**
> is the number next to the GDD application

26 Return the Log Delivery application to service by typing

```
> rts <fileset_number.
```

and pressing the Enter key.

where

> **fileset_number**
> is the number next to the GDD application

27 Determine if the state of the log delivery application is still ISTb. Wait at least 1 min. 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

28 You have completed this procedure.

302

Viewing the dcemonitor status file

Application

The CS 2000 Core Manager detects common DCE failure conditions, reports them to the CS 2000 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 CS 2000 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) script that is continuously executed by a DCE control program (dcecp) running in the CS 2000 Core Manager platform. Dcemonitor dumps its current status, problems found, and the recovery action in a file that is regularly rewritten. By viewing the contents of the status file, you can determine what caused the DCE state change.

This procedure assists you 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 CS 2000 Core Manager hostname is changed
- the CS 2000 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 that follows the flowchart to perform the task.

Summary of viewing the dcemonitor status file

```
┌─────────────────┐
│ Log in to the CS│
│ 2000 Core Man-  │
│ ager.           │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Go to           │
│ dcemonitor      │
│ directory       │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ Determine       │
│ when file was   │
│ written         │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ View contents   │
│ of the file     │
│                 │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ End             │
│                 │
│                 │
└─────────────────┘
```
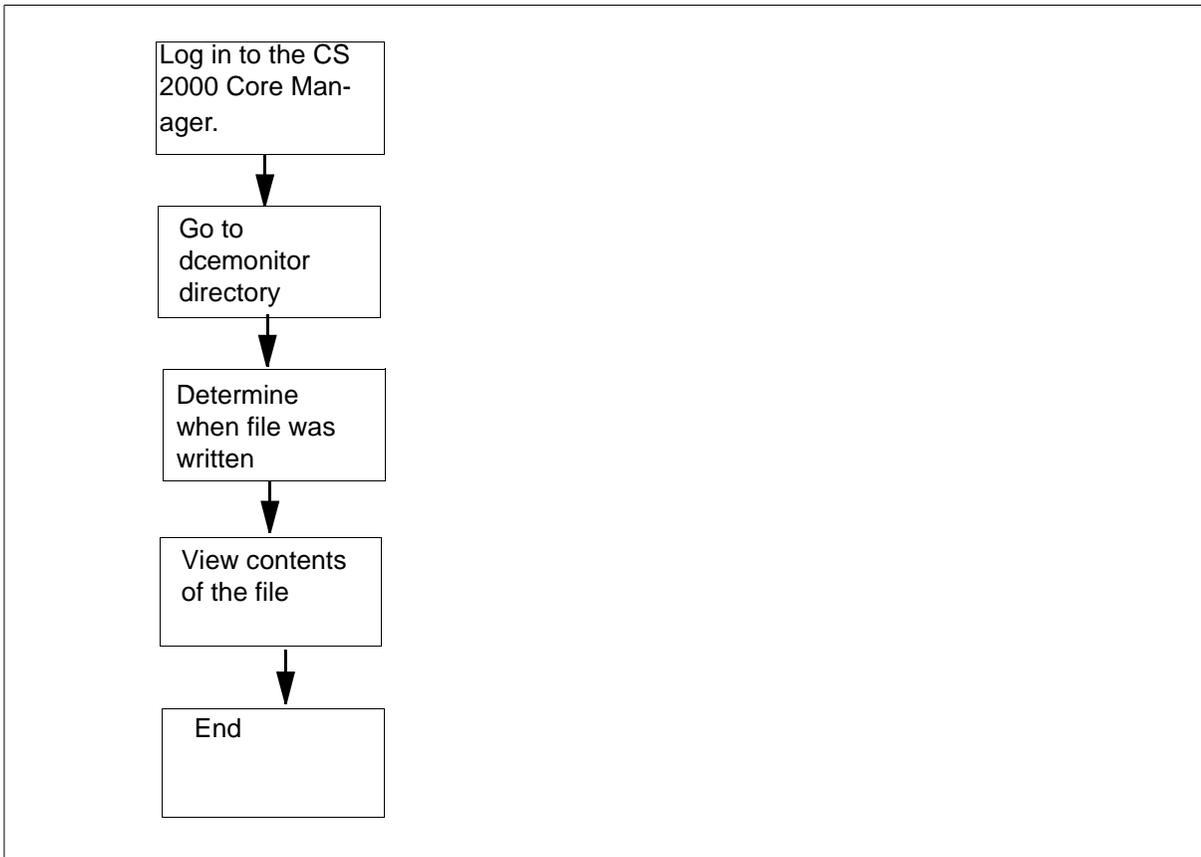
Viewing the dcemonitor status file

> **ATTENTION**
> This procedure must be performed by a trained Distributed
> Computing Environment (DCE) system administrator who knows
> DCE administration procedures.

At the local VT100 console or remote client workstation

1 Log in to the CS 2000 Core Manager as the root user.

2 Access the dcemonitor data directory by typing

> **# cd /sdm/configdata/dce**

and pressing the Enter key.

3 Determine when the file was last written by typing

> **# ls -l dce_mon_status**

and pressing the Enter key.

4   View the contents of the status file by typing

        `# cat dce_mon_status`

        and pressing the Enter key.

5   You have completed this procedure.

306

Viewing the contents of a snapshot file

Complete the following procedure to view the contents of a snapshot file.

Viewing the contents of a snapshot file

At the CS 2000 Core Manager prompt

1　　Type

　　　> vacf <source_file>

　　　and press the Enter key.

　　　where

　　　<source_file> is the simple filename of the file to view

```
Trunk,Critical,GC  ,TTT       ,Tue Mar 9  16:13:45  2000

. . .

snapshot.txt:    END
maint:
```

　　　Note: A simple filename does not contain the complete pathname of the file. In the preceding example, the CS 2000 Core Manager displays the contents of the file.

2　　You can scroll forward through the file until you reach the end. To scroll one line at a time, press the Enter key. To scroll one page at a time, press the Space bar.

3　　You have completed this procedure.

Clearing an AFT alarm

Application

The AFT alarm is generated by the Automatic File Transfer (AFT) application. Use the following procedures to clear AFT alarms that are specific to the SuperNode Billing Application (SBA).

Indication

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

Meaning

An AFT alarm is generate under the conditions in the following table.

AFT alarms

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

Impact

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

Action

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

Clearing critical alarms

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

- Delete the tuple from the automaticFileTransferTable table.

- Manually clear the alarm through the Alarm command at the AFT level of the BILLMTC remote maintenance interface (RMI).

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

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

- Restart the session using the Start the command available at the AFT level of the BILLMTC RMI.

- Delete the tuple from the automaticFileTransferTable table.

- Manually clear the alarm through the Alarm command available at the AT level of the BILLMTC RMI.

Action

Use the following procedure to clear an AFT alarm manually.

Clearing an AFT alarm

At the CS 2000 Core Manager

1   Access the BILLMTC level by typing

> **billmtc**

and pressing the Enter key.

2   Access the Application (APPL) level by typing

> **appl**

and pressing the Enter key.

3   Access the Automatic File Transfer (AFT) level by typing

> **aft**

and pressing the Enter key.

4   Clear the alarm by typing

> **alarm cancel <session_name>**

and pressing the Enter key.

where:

<session_name> = 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, type

> **> yes**

and press the Enter key.

Example response:

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

6   You have completed this procedure.

Deleting a tuple from automaticFileTransferTable

> **CAUTION**
>
> When an AFT tuple is deleted, billing files are no longer being transferred downstream. *Note that an AFT tuple must be stopped before it can be deleted.*

At the CS 2000 Core Manager

1   Access the BILLMTC level by typing

> **> billmtc**

and pressing the Enter key.

2   Access the APPL level by typing

> **> appl**

and pressing the Enter key.

3   Access the AFT level by typing

> **> aft**

and pressing the Enter key.

4   Access the AFTCONFIG level by typing

> **> aftconfg**

and pressing the Enter key.

5   Delete the tuple from the automaticFileTransferTable by typing

> `delete <session_name>`

where:

   <session_name> = 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), type

> `yes`

and press the Enter key.

Example response:

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

7   You have completed this procedure.

Restarting an AFT session

At the CS 2000 Core Manager

1   Access the BILLMTC level by typing

> `billmtc`

and pressing the Enter key.

2   Access the APPL level by typing

> `appl`

and pressing the Enter key.

3   Access the AFT level by typing

> `aft`

and pressing the Enter key.

4   Restart the AFT session that generated the alarm by typing

`> start <session_name>`

where:

<session_name> = 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

Indication

The "SDM System Audit Status" under the system (SYS) level of SDMMTC 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](#) in the Fault section. 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 will re-appear on the next execution of the system audit.

Refer to "System audit overview" in the Basics section for more information on the system audit.

At the CS 2000 Core Manager

1   Log in to the CS 2000 Core Manager.

2   Access the system level by typing

`# sdmmtc sys`

and pressing the Enter key

3   Clear the system audit alarm by typing

`> audit clear`

and pressing the Enter key

4   When prompted, confirm the command by typing

`> y`

and pressing the Enter key.

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 CS 2000 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 CS 2000 Core Manager is sending system busy status to the CM because it is out of service, or the CM has designated the CS 2000 Core Manager as system busy because it is unable to communicate with the CS 2000 Core Manager.

Impact

If the CS 2000 Core Manager is out of service, all CS 2000 Core Manager applications are unavailable.

If the CM is unable to communicate with the CS 2000 Core Manager, the local state and operating condition of the CS 2000 Core Manager are unknown to the CM. MAP commands requesting state changes to the CS 2000 Core Manager are not sent to the CS 2000 Core Manager, and MAP requests for information from the CS 2000 Core Manager cannot be completed. The CS 2000 Core Manager maintenance interface can be used to change the local state of the CS 2000 Core Manager, or obtain information about the CS 2000 Core Manager, when the CM-CS 2000 Core Manager link is not functioning. When communications are restored, the CS 2000 Core Manager local state aligns itself to the CM view of its state.

Action

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

Summary of clearing a critical APPL alarm
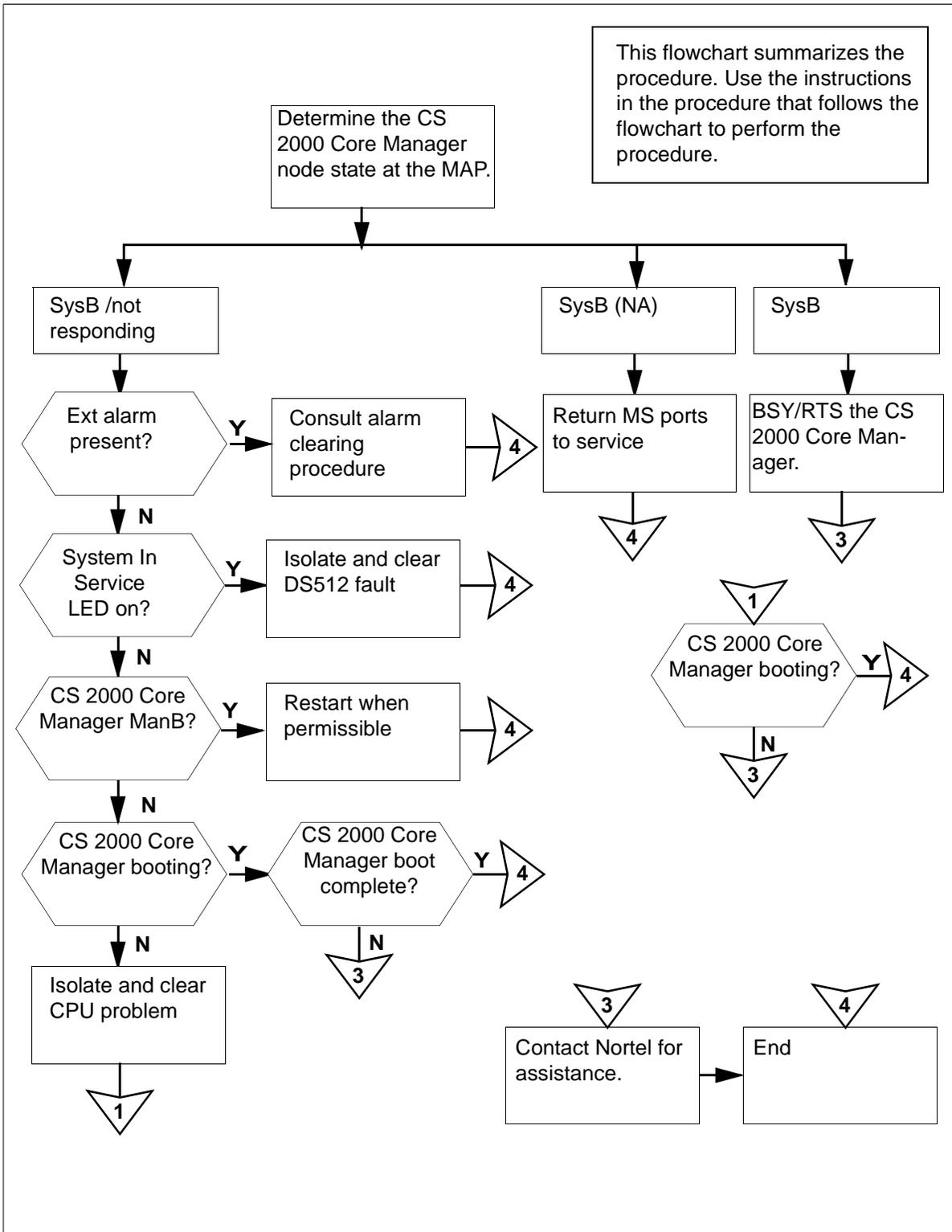
Clearing critical APPL alarm

At the MAP display

1   Access the SDM level of the MAP display by typing

> **> mapci;mtc;appl;sdm**

and pressing the **Enter** key.

Example response:

```
SDM    SysB(NA)    Links_OOS: 4
```

2   Determine the state of the CS 2000 Core Manager.

If the state is	Do
SysB (NA)	step 4
SysB/ the CS 2000 Core Manager is not responding	step 3
SysB/CS 2000 Core Manager online upgrade in progress but not responding	contact your next level of support
SysB	step 66

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 CS 2000 Core Manager by typing

> **> trnsl**

and pressing the **Enter** key.

> *Note:* The CM has designated the CS 2000 Core Manager as system busy (SysB) because all four message switch (MS) ports that provide the DS512 links to the CS 2000 Core Manager are unavailable. The CS 2000 Core Manager may

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 CS 2000 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 by typing

> **> ms**

and pressing the **Enter** key.

7   Access the shelf level by typing

> **> shelf 0**

and pressing the **Enter** key.

8   Access the MS port card level that is associated with the CS 2000 Core Manager DS512 links by typing

> **> card *<cardno>***

and pressing the **Enter** key.

> *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 procedure.

11   Access the EXT level of the MAP display by typing

> **> ext**

and pressing the **Enter** key.

12 List all major EXT alarms by typing

> **`> list maj`**

and pressing the **Enter** key.

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

13 Determine if the CS 2000 Core Manager has triggered an FSP frame fail alarm for the equipment aisle containing the CS 2000 Core Manager.

If a CS 2000 Core Manager -related FSP alarm is	Do
present	step 14
not present	step 16

> *Note:* An EXT FSP major alarm triggered by the CS 2000 Core Manager indicates that one or both -48V dc power inputs to the CS 2000 Core Manager have failed, or that the CS 2000 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 in the Fault Management section.

15 You have completed this procedure.

At the front of the CS 2000 Core Manager

16   At the front of the CS 2000 Core Manager, determine if the
System in Service light is on (green).
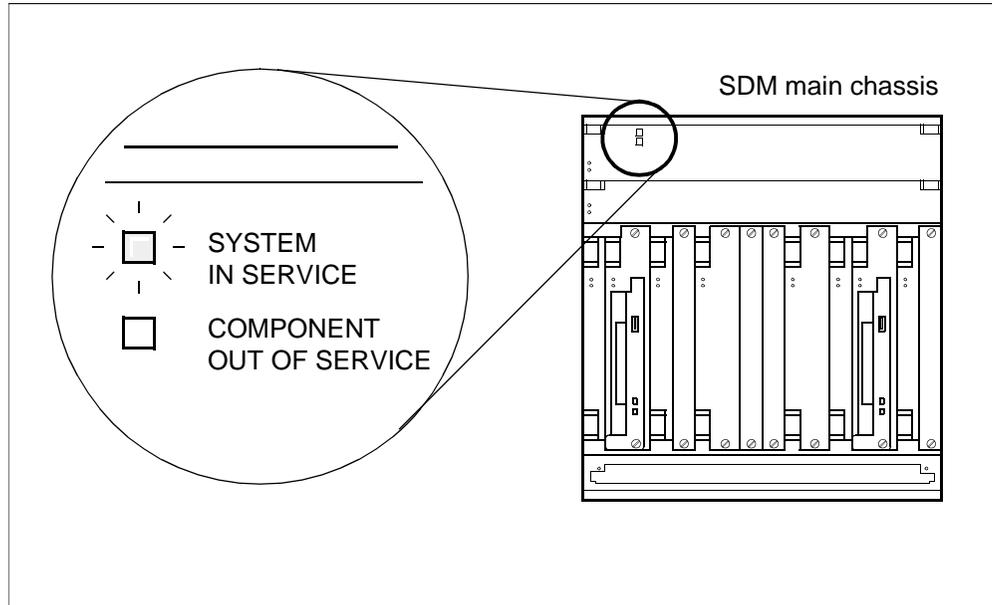
Note: If the System in Service light is off, but power is
available to the system and it has not shut down because of
thermal failure (overheating), one or more of the following
conditions is present or has occurred:

*   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 43
off	step 17

17   Determine from office records or other personnel if the CS 2000 Core Manager was manually shut down.

If the system was	Do
manually shut down	step 21
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 CS 2000 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 CS 2000 Core Manager by turning the modular supervisory panel (MSP) breakers off and on. The MSP breakers supply power to the CS 2000 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 min.

If the boot process	Do
does not start	step 23
starts, but does not complete (returns to the FX-Bug prompt)	step 34
completes normally, and the login prompt is displayed	step 32

At the front of the CS 2000 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). Determine if either CPU controller module was accidentally unseated or removed. (This scenario may have occurred 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 28
a CPU controller module was removed or unseated	step 24

24

> **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

25 Determine whether the system has begun to boot.

If the system is	Do
booting	step 27
not booting, or the boot has failed	step 26

At the front of the MSP

26 Cycle power to the CS 2000 Core Manager by turning the MSP breakers off and on. The MSP breakers supply power to the CS 2000 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

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

If the boot process	Do
does not start	step 28
starts, but does not complete (returns to the FX-Bug prompt)	step 34
completes normally, and the login prompt is displayed	step 32

At the front of the CS 2000 Core Manager

28

> ⚠️ **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.

29 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 30
both CPU controller modules fail their self tests	contact your next level of support
both CPU controller modules pass their self tests	step 31

30 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 CS 2000 Core Manager hardware replacement procedures.

At the local VT100 console

31 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 34
completes normally, and the login prompt is displayed	step 32

32 Access the maintenance interface by typing

`# sdmmtc`

and pressing the **Enter** key.

> *Note:* Monitor the alarm banner at the top level of the SDM maintenance interface. Wait at least 10 min. for the CS 2000 Core Manager to recover (until all items on the alarm banner display a dot).

33 Go to step 42

At the front of the CS 2000 Core Manager

34 Physically verify that the I/O controller modules which 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 scenario may have occurred 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 37
an I/O controller module was removed or unseated	step 35

35 Reinsert the I/O controller module that was removed in error.

36 Go to step 38.

37 Unseat and reseat both I/O controller modules in slots 2 and 3, and 13 and 14. Ensure that they are seated firmly and that the latches are closed snugly.

At the front of the MSP

38 Cycle power to the CS 2000 Core Manager by turning the MSP breakers off and on. The MSP breakers supply power to the CS 2000 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

39 Monitor the boot process at the local VT100 console.

If the boot process	Do
does not start	step 40
completes normally, and the login prompt is displayed	step 42

40 Perform a system software reinstall using the procedure "Performing a full restore of the software load from S-tape" in the Security and Administration section. Ensure that you reboot the system as indicated in that procedure.

41 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 42

42 Complete the remainder of the procedure "Performing a full restore of the software from S-tape" in the Security and Administration section.

At the local or remote VT100 console

43   Log in to the CS 2000 Core Manager as the root, or a maint class user.

44   Access the maintenance interface by typing

 # sdmmtc

and pressing the **Enter** key.

45   Access the maintenance (Mtc) level by typing

> mtc

and pressing the **Enter** key.

46   Access the connectivity (Con) level by typing

> con

and pressing the **Enter** key.

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
```

47   Continue according to state of the DS512 links.

If	Do
all four links are failed	step 54
any of the links are closed	step 48

48   Note the I/O domain number and port number of each closed link.

At the back of the CS 2000 Core Manager

49 Physically inspect the fiber link connections to the CS 2000 Core Manager DS512 personality modules.

If the fibre links	Do
require reconnecting or replacement	step 50
appear undamaged, and are correctly connected	step 52

50

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

51 Monitor the link status at the connectivity (Con) level.

If	Do
any of the links are closed	step 52
all four links are open	you have completed this procedure
two links are open, and two links are failed	step 54

Note: Allow 5 min. for the CS 2000 Core Manager link status to update if one or more fibers were reconnected or replaced.

At the MAP display

52 At the MAP display, determine the MS hardware that provides the DS512 links to the CS 2000 Core Manager by typing

> **trnsl**

and pressing the **Enter** key.

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
```

53 Record the MS port card number associated with the system-busy DS512 links identified in step 51.

Note: In the example response shown in step 52, the port card number is 15.

At the local VT100 console

54 Access the hardware (Hw) menu level of the SDM maintenance interface by typing

>**hw**

and pressing the **Enter** key.

55 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 56
both DS512 controller modules have failed (indicated by an F)	step 59
one DS512 controller module failed, and the other is in service (indicated by a dot)	step 58
both DS512 controller modules are in service	contact your next level of support

56   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 by typing

```
> rts <n> 512
```

and pressing the **Enter** key.

where

> **n**
>> 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".

Response:

```
Hardware RTS : Domain 0 Device 512 - Command
submitted.
```

57   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

58   Return the failed DS512 controller module to service using the procedure [Clearing a minor or major APPL SDM alarm](#).

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 CS 2000 Core Manager

59 Physically verify that the two DS512 controller modules (NTRX50GA, front slots 1 and 12) are present in the main chassis. 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.)

If	Do
both DS512 modules are present	step 64
one DS512 controller module was removed or unseated	step 60

> **Note:** If both LEDs on the DS512 controller module are off, the module is not seated correctly.

60 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

61 Return the DS512 controller module to service by typing

> **`> rts <domain> 512`**

and pressing the **Enter** key.

where

> **domain**
>   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".

Response:

```
Hardware RTS : Domain 0 Device 512 - Command
submitted.
```

62   Check the status of the DS512 controller modules, indicated under the "512" header.

If	Do
both DS512 modules have failed (indicated by an F)	step 64
one DS512 controller module is in service, and one has failed	step 63

63   Return the system-busy DS512 controller module to service using the procedure Clearing a minor or major APPL SDM alarm.

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 CS 2000 Core Manager

64   Replace the failed DS512 controller module at the front of the CS 2000 Core Manager using the procedure Replacing the DS512 personality module.

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.

65   Go to step 68.

At the MAP display

66   The CS 2000 Core Manager state SysB at the MAP display with no additional qualifier (NA or / not responding) indicates that the CS 2000 Core Manager is communicating successfully with the CM. However, all CS 2000 Core Manager applications have

failed., on other internal CS 2000 Core Manager problem exists. Manually busy the CS 2000 Core Manager by typing

> **bsy**

and pressing the **Enter** key.

Response:

```
SDM Bsy initiated.
SDM Bsy completed.
```

67 Return the CS 2000 Core Manager to service by typing

> **rts**

and pressing the **Enter** key.

Response:

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

68 Determine the next step using the table below.

If the CS 2000 Core Manager	Do
recovers	you have completed this procedure
does not recover	step 69

69 Busy the CS 2000 Core Manager at the MAPCI;MTC;APPL;SDM level by typing.

> **bsy**

and pressing the **Enter** key.

70 Reboot the CS 2000 Core Manager by typing

> **rebootsdm**

and pressing the **Enter** key.

> *Note:* Wait for the */Reboot SDM in progress* message to disappear from the screen before you continue with the procedure.

71   Return the CS 2000 Core Manager to service by typing

> `> RTS`

and pressing the **Enter** key.

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

Application

Use this procedure to clear an APPL SDM minor or major MAP alarm that has been triggered by the CS 2000 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 CS 2000 Core Manager is in manual-busy (ManB) or in-service trouble (ISTb) state.

Impact

If the CS 2000 Core Manager state at the MAP display is ManB, the CS 2000 Core Manager was set to that state by the MAP command.

If the CS 2000 Core Manager state at the MAP display is ISTb, the computing module (CM) is receiving ISTb status from the CS 2000 Core Manager. One or more of the following conditions exist:

- One or more CS 2000 Core Manager applications have failed, but at least one application has not failed.

- A system software resource has exceeded its alarm threshold.

- The CS 2000 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 CS 2000 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 CS 2000 Core Manager.

    Note: If all CS 2000 Core Manager applications fail, the CS 2000 Core Manager node state is system busy (SysB). The system generates an APPL SDM critical or APPL SysB critical alarm.

Action

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

Summary of clearing a minor or major APPL SDM alarm
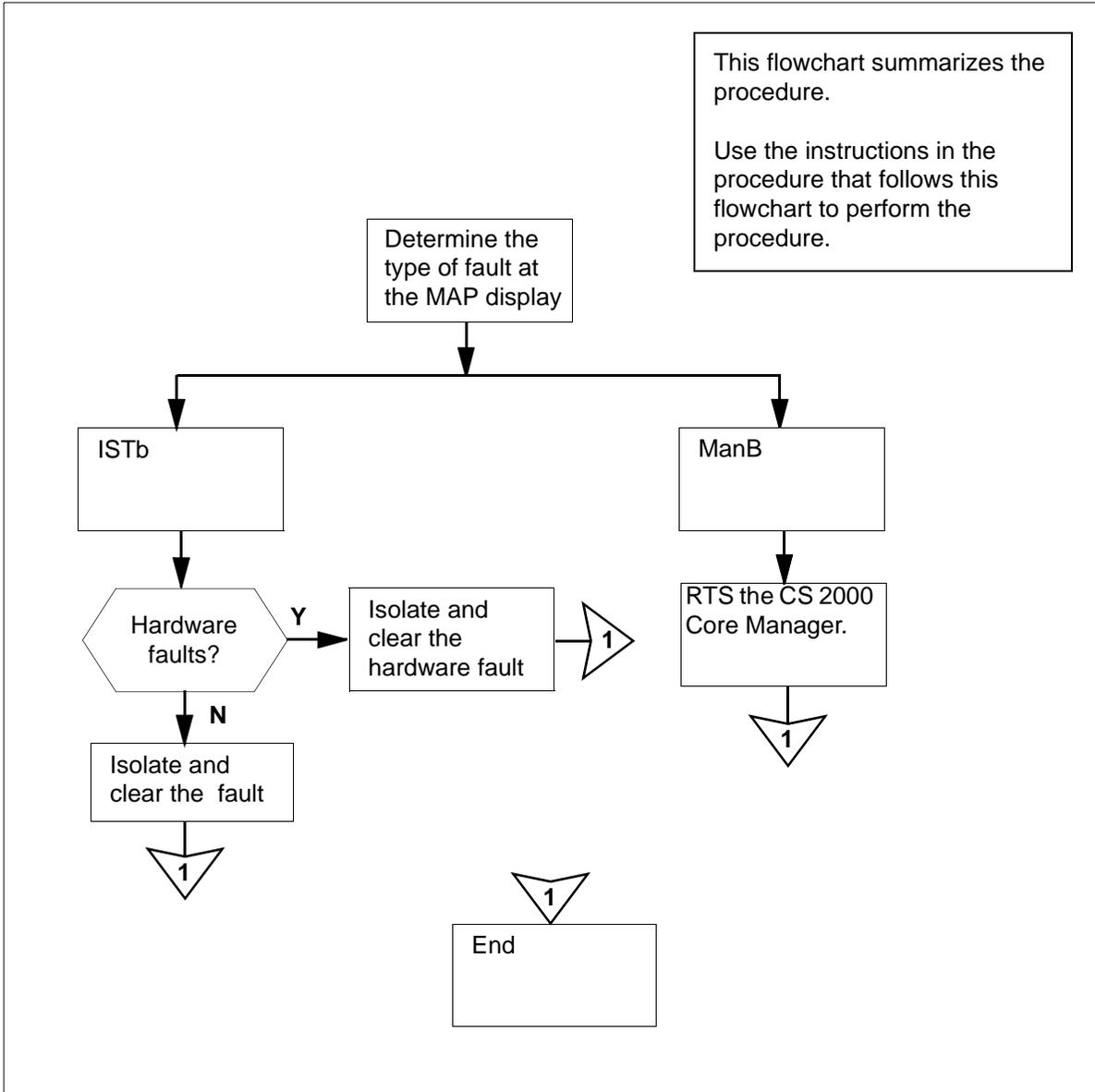
Clearing a minor or major APPL SDM alarm

At the MAP display

1   Access the SDM level at the MAP display by typing

> **> mapci;mtc;appl;sdm**

and pressing the **Enter** key.

Example response:

```
SDM 0 ISTb LINKS_OOS: .
```

2   Check the node state of the CS 2000 Core Manager at the MAP display.

If the state is	Do
ManB	step 3
ISTb	step 5

3   If applicable, determine from office records or other personnel why the CS 2000 Core Manager was set to manual busy state. When permissible, return the CS 2000 Core Manager to service by typing

> **> rts**

and pressing the **Enter** key.

Response:

```
SDM RTS initiated.

SDM RTS completed.
```

4   Use the following table to determine your next step.

If the CS 2000 Core Manager	Do
returns to service	you have completed this procedure
does not return to service	step 5

5   Obtain fault status information from the CS 2000 Core Manager by typing

> **> querysdm flt**

and pressing the **Enter** key.

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
```

6   Use the table below 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.	SDM 321	Split-system upgrade in progress
		Status: <spmdstatus>
		   spmdstatus = started
		      SwAct started
		      SwAct completed
		     SwAct started for
		         fallback
		     Completed

7 Proceed according to the type of fault.

If the fault is	Do
a connectivity problem with fault type CM (300)	step 28
a connectivity problem with fault type LAN	step 55
a logical volume problem (301)	step 15
an exceeded resource threshold (302)	step 8
a hardware device fault (309)	step 67
a DCE problem (317)	have your system administrator isolate and clear the problem
an application problem (321)	step 18

At the local or remote VT100 console

8 Log into the CS 2000 Core Manager as a maint class user, or root user, and access the maintenance interface by typing

```
# sdmmtc
```

and pressing the **Enter** key.

9 Access the maintenance level by typing

```
> mtc
```

and pressing the **Enter** key.

10   Obtain fault status information from the CS 2000 Core Manager by typing

> **`> querysdm flt`**

and pressing the Enter key.

From the response, determine the type of system resource that has exceeded its alarm threshold.

If the resource exceeded is	Do
swap space	step 11
number of processes	step 11
number of swap queue entries	step 11
number of zombie processes	step 11
CPU (number of run queue entries)	step 11
logical volume	step 13

11   Access the System (Sys) level by typing

> **`> sys`**

and pressing the **Enter** key.

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
```

12   Check the current level of the software resource by locating the resource identified in step 10.

> *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 11, 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 CS 2000 Core Manager. When you reboot the CS 2000 Core Manager, the CS 2000 Core Manager remains out of service for approximately 15 min.

13

> **CAUTION**
> **Potential Service Interruption**
> A logical volume on the CS 2000 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 for assistance.

Access the storage level by typing

> **> storage**

and pressing the **Enter** key.

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 particular
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 CS 2000 Core Manager from the status field in log SDM301.

If the status is	Do
integrating	step 16
not mirrored	step 17
I/O error detected while writing to %s, possibly due to double disk fault	step 17

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 min. to complete. The processing time depends on the amount of data (in the affected volume group) the CS 2000 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

17 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
due to out-of-service hardware	step 68

At the local or remote VT100 console

18   Log into the CS 2000 Core Manager as a maint class user, or root user, and access the maintenance level by typing

 # sdmmtc

and pressing the **Enter** key.

19   Access the application (Appl) menu level of the RMI by typing

> 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              ManB
5 Enhanced Terminal Access          ISTb
6 Exception Reporting               ISTb
                    Applications showing: 1 to 6
of 6
```

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

21 Proceed depending on the state of the application.

If the application is	Do
ManB	step 22
ISTb	step 23
SysB	step 24
Fail	step 25

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

```
> rts <n>
```

and pressing the Enter key.

where

> **n**
> is the key number next to the application you want to return to service

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 returns to service	step 21

23 This state can result from a recent change of state, or if this application is dependent on another application that has not completed initialization. If you suspect either situation to be true, wait 10 min. for the 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

24 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

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

- The system cannot restart the package.

- The application has restarted and failed three times within10 min.

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

> bsy *key*

and pressing the **Enter** key.

where

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

Response:

```
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.
```

26   Return the application to service by typing

> **> rts *key***

and pressing the **Enter** key.

where

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

Response:

```
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.
```

27   Proceed depending on the state of the application.

If the application	Do
remains in a Fail state	refer to the configuration or installation information modules in the Configuration or Upgrades section, specific to that application
changes to InsV state	you have completed this procedure

28   Determine if the response indicates an IP address mismatch.

If the QUERYSDM FLT response indicates	Do
an SDM IP address mismatch	step 29
a CM IP address mismatch	step 32
anything else	contact your next level of support

At the MAP display

29   Access table SDMINV by typing

> **> table sdminv; list all**

and pressing the **Enter** key.

30   Record the datafill value for the CS 2000 Core Manager CM-side IP address (field IPADDR).

31   Go to step 34

At the MAP display

32   Access table IPNETWRK by typing

> ```
> table ipnetwrk; list all
> ```

and pressing the **Enter** key.

33   Record the datafill value for the CM IP address (field CMIPADDR).

34   Check the address from step 30 and step 33 against office records.

If	Do
both addresses are correct	step 29
neither address is correct	contact your next level of support

At the local or remote VT100 console

35   Access the connectivity (Con) level by typing

> ```
> con
> ```

and pressing the **Enter** key.

36   Determine how the CM IP, SDM IP, and CM/SDM netmask addresses are commissioned on the CS 2000 Core Manager by typing

> ```
> querysdm
> ```

and pressing the **Enter** key.

Example response:

```
CM IP Address:            47.105.155.1
SDM IP Address:           47.105.155.6
CM/SDM Netmask:           255.255.255.248
```

37   Record the CM IP, SDM IP, and CM/SDM netmask addresses.

At the MAP display

38   Busy the CS 2000 Core Manager by typing

> **> bsy**

and pressing the **Enter** key.

Response:

```
SDM Bsy initiated.
SDM Bsy completed.
```

At the local or remote VT100 console

39   Access the change editor for the CM side IP parameters by typing

> **> change**

and pressing the **Enter** key.

> *Note:* Only the root user can access the editor.

40   Access the change editor for the CM side IP parameters by typing

> **> change <n>**

and pressing the **Enter** key.

where

> **n**
>   is the numeric key for the hostname entry, shown under the "#"header

> *Note:* Only the root user can perform this step.

41

DANGER
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.

42   Confirm your request by typing

> **> yes**

and pressing the **Enter** key.

43   Compare the CM IP address from step 33 to the CM IP address from step 36.

If the values are	Do
identical	step 45
not identical	step 44

44   Type the CM IP address from step 33 (include dots; example 47.105.155.6) and press the **Enter** key.

Example response

```
CM IP address: 47.105.155.6
```

45   Press the **Enter** key.

46   Compare the SDM IP address from step 30 to the SDM CM-side IP address from step 36.

If the values are	Do
identical	step 48
not identical	step 47

47   Type the SDM CM-side IP address from step 33 (include dots; example 47.105.155.6) and press the **Enter** key.

48   Press the **Enter** key.

49   Determine if the displayed values are correct.

If the values are	Do
incorrect	step 50
correct	step 52

50   At the local or remote VT100 console, edit the values by typing

```
> e
```

and pressing the **Enter** key.

51   Go to step 43.

52   Save the change and exit the change editor by typing

> **> y**

and pressing the **Enter** key.

Response:

```
Change CM Connectivity command initiated.
Please wait ...
```

At the MAP display

53   At the SDM level return the CS 2000 Core Manager to service by typing

> **> rts**

and pressing the **Enter** key.

Response:

```
SDM RTS initiated.
```

```
SDM RTS completed.
```

54   Go to

At the local or remote VT100 console

55   Contact your LAN network administrator to determine whether the communications problem is external to the CS 2000 Core Manager. If external to the CS 2000 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 56
on the operating company LAN	you have completed this procedure

56   Log into the CS 2000 Core Manager as a maint class user or root user, and access the maintenance interface by typing

> **# sdmmtc**

and pressing the **Enter** key.

57 Access the NET level by typing

> **net**

and pressing the **Enter** key.

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
```

58 Determine if the IP address shown for the affected LAN hostname is correct.

If the IP address is	Do
incorrect	step 40
correct	contact your next level of support

59 Access the change editor by typing

> **change <*n*>**

and pressing the **Enter** key.

where

> **n**
> is the numeric key for the hostname entry, shown under the "#" header

60 Each editable parameter is displayed in turn. Keep pressing the **Enter** key until the IP address is displayed.

61 Type the correct IP address for the LAN node, and press the **Enter** key.

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
```

62 Determine if the displayed values are correct.

If the displayed values are	Do
correct	step 63
incorrect	step 65

63 Save the change and exit the change editor by typing

> **y**

and pressing the **Enter** key.

> *Note:* The node state changes to InSv within 2 min.

64 Go to step 96.

65 Edit the values by typing

> **e**

and pressing the **Enter** key.

66 Go to step 41.

At the local or remote VT100 console

67 Obtain fault status information from the CS 2000 Core Manager by typing

> **querysdm flt**

and pressing the **Enter** key.

68 From the fault status response, determine the affected device type and its state.

If the device state is	Do
ManB	step 69
Fail	step 73

69 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

70 Access the Platform level under the SDM level.

71 Return the device to service by typing

> **`> rts <n> <device>`**

and pressing the **Enter** key.

where

> **n**
> > 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.
```

72 Go to step 96.

73 Determine if the QuerySDM FLT response indicates an interconnect module (ICM) failure.

If an ICM failure is	Do
indicated	step 74
not indicated	step 81

74 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 75
the ICM power feed is OK	step 88

Note: If the CS 2000 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

75 From the SDM level, enter the Platform level.

76 Have qualified power maintenance personnel restore the power feed to the ICM.

77 Access the hardware level of the RMI by typing

> **hw**

and pressing the **Enter** key.

78 Return the main chassis ICM (that has failed due to loss of power) to service by typing

> **rts <*domain*> icm**

and pressing the **Enter** key.

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 CS 2000 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 min. The actual amount of time may*

vary depending on the amount of data stored on the disks, and the current processor load.

79   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.

80   Go to step 96.

81   Determine the fault in the CS 2000 Core Manager from the QuerySDM FLT response and go to the appropriate steps indicated below.

If	Do
one of the CPUs is shown Fail	step 82
the Ethernet device is the only faulty device on an MFIO (usually indicates a cable fault)	step 85
a fan is faulty	step 88
a disk is faulty	step 88
a dat is faulty	step 88
a DS512 card is faulty	step 90

At the MAP display

82   Access the hardware level of the RMI by typing

> **hw**

and pressing the **Enter** key.

83   Return the out-of-service CPU to service and start CPU reintegration by typing

> **> rts <*domain*> cpu**

and pressing the **Enter** key.

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 min. to complete. The actual time may vary depending on the processor load. When reintegration is complete, the CPU status changes to in-service, indicated by a dot (.).

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

If the action is	Do
successful	you have completed this procedure
not successful	step 88

At the local or remote VT100 console

85   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 86
appears undamaged and correctly connected	contact your next level of support

86 Reconnect, repair, or replace the cable as appropriate.

> *Note:* If this is not successful, replace the MFIO.

87 Go to step 96

88 Replace the failed device using the appropriate hardware replacement procedure.

89 Go to step 96.

90 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 94
DS512 controller module	step 91

91 Check the LEDs on the affected card.

If the LEDs are	Do
on	step 93
off	step 92

92 Reseat the card.

At the MAP display

93 Try to bring the card back into service by typing

> **rts** *<domain number> 512*

and pressing the **Enter** key.

where

domain number
is either 0 or 1

If the system	Do
recovers	you have completed this procedure
does not recover	step 95

94 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 95

95 Replace the affected card using the appropriate hardware replacement procedure.

96 You have completed this procedure.

Clearing a BAK50 alarm

Indication

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

Note: The term "XAC16" is used in this document to mean an XA-Core system based on CSP16 or later. To determine if this applies to your system, run the IMAGENAME command on your CM. If the first line of the response begins with "XA", you are on a XA-Core system. If the line that begins "LAYER: TL" indicates 16 or higher, then "XAC16" notes apply to your 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 set to `on`, the alarm is minor. If the stream is set to `both`, no alarm occurs.

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.

The CS 2000 Core Manager generates the SDMB820 log report when this alarm is raised.

Impact

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

Procedure

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

BAK50 alarm clearing flowchart

```
                      ╭─────────╮
                      │  Start  │
                      ╰────┬────╯
                           │
                           ▼
                 ┌───────────────────┐
                 │ Receive BAK50     │
                 │ alarm             │
                 └─────────┬─────────┘
                           │
                           ▼
                 ┌───────────────────┐
                 │ Access the SDMBIL │
                 │ level             │
                 └─────────┬─────────┘
                           │
                           ▼
                 ┌───────────────────┐
                 │ Find out why system│
                 │ is in backup mode │
                 └─────────┬─────────┘
                           │
                           ▼
                 ┌───────────────────┐
                 │ Run a manual audit│
                 └─────────┬─────────┘
                           │
                           ▼
                      ╭─────────╮
                      │   End   │
                      ╰─────────╯
```
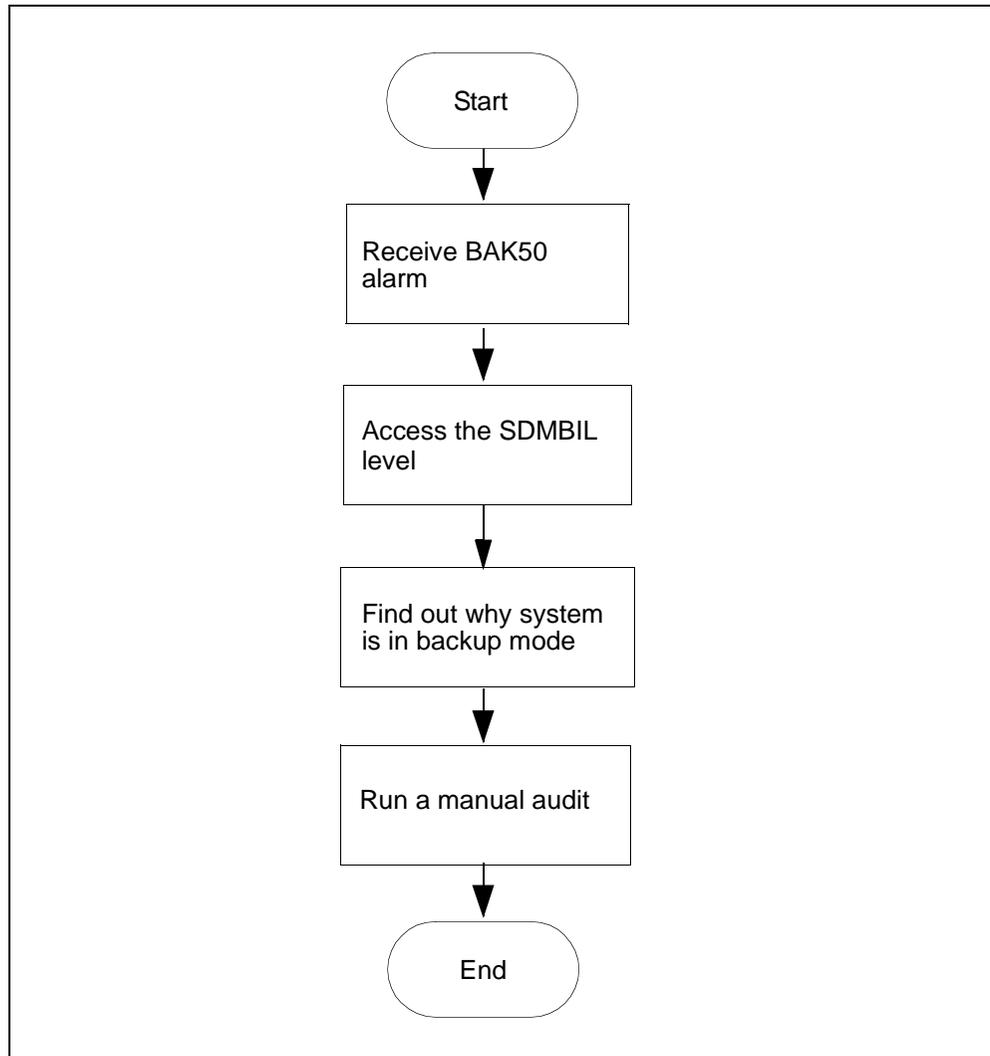
Clearing a BAK50 alarm

At the MAP

1   Post the billing stream by typing

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

and pressing the Enter key.

Where

<x> is the name of the billing stream.

2   Determine why the system is in backup mode and check the
system node state.

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

If the SBA is	Do
SysB	refer to Clearing a DSKWR alarm, Clearing a NOCOM alarm, Clearing a major SBACP alarm, Clearing a minor SBACP alarm (depending on why you are receiving alarm)
ManB	determine if you still have sufficient space in the backup volume, continue with step 4
RBsy	refer to Clearing a major SBACP alarm

4   Display the names of the backup volumes by typing

> **`> conf view <x>`**

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

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

> **`> diskut;lv s00d<xxxx>`**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

> *Note:* This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D), or if the backup volumes are on IOP disks (their names start with F02L or F17L). If the volume information starts with D000 or D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

6   Display the size of the second volume and its number of free blocks by typing

```
> diskut;lv s01d<xxxx>
```

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

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

If the volumes	Do
have enough disk space	you have completed this procedure
do not have enough disk space	refer to procedure "Configuring IOP disk drive backup volumes" in the Accounting section, if you are on XA-core. Otherwise, refer to procedures "Configuring SLM disk drive backup volumes" and "Configuring DDU disk drive backup volumes" in the Accounting section. You must use IOP volumes on XAC16 systems.

8   Use Audit to clear the alarm. If the alarm does not clear, contact your next level of support.

Clearing a BAK70 alarm

Indication

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

Note: The term "XAC16" is used in this document to mean an XA-Core system based on CSP16 or later. To determine if this applies to your system, run the IMAGENAME command on your CM. If the first line of the response begins with "XA", you are on a XA-Core system. If the line that begins "LAYER: TL" indicates 16 or higher, then "XAC16" notes apply to your system.

Meaning

The backup system is using more than 70 percent of the total space on backup volumes on the DMS/CM. The records are stored on the CM backup volume. If the stream is set to `on`, the alarm is major; if the stream is set to `both`, the alarm is minor.

```
                          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.
```

The CS 2000 Core Manager generates the SDMB820 log report when this alarm is raised.

Impact

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

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's collector through the previously-established network that DIRP uses.

Action

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

BAK70 alarm clearing flowchart

```
                    ╭─────────────╮
                    │    Start    │
                    ╰──────┬──────╯
                           │
                           ▼
                    ┌─────────────┐
                    │ Receive BAK70│
                    │ alarm        │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Access the   │
                    │ SDMBIL level │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Find out why │
                    │ system is in │
                    │ backup mode  │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Run a manual │
                    │ audit        │
                    └──────┬──────┘
                           │
                           ▼
                    ╭─────────────╮
                    │     End     │
                    ╰─────────────╯
```
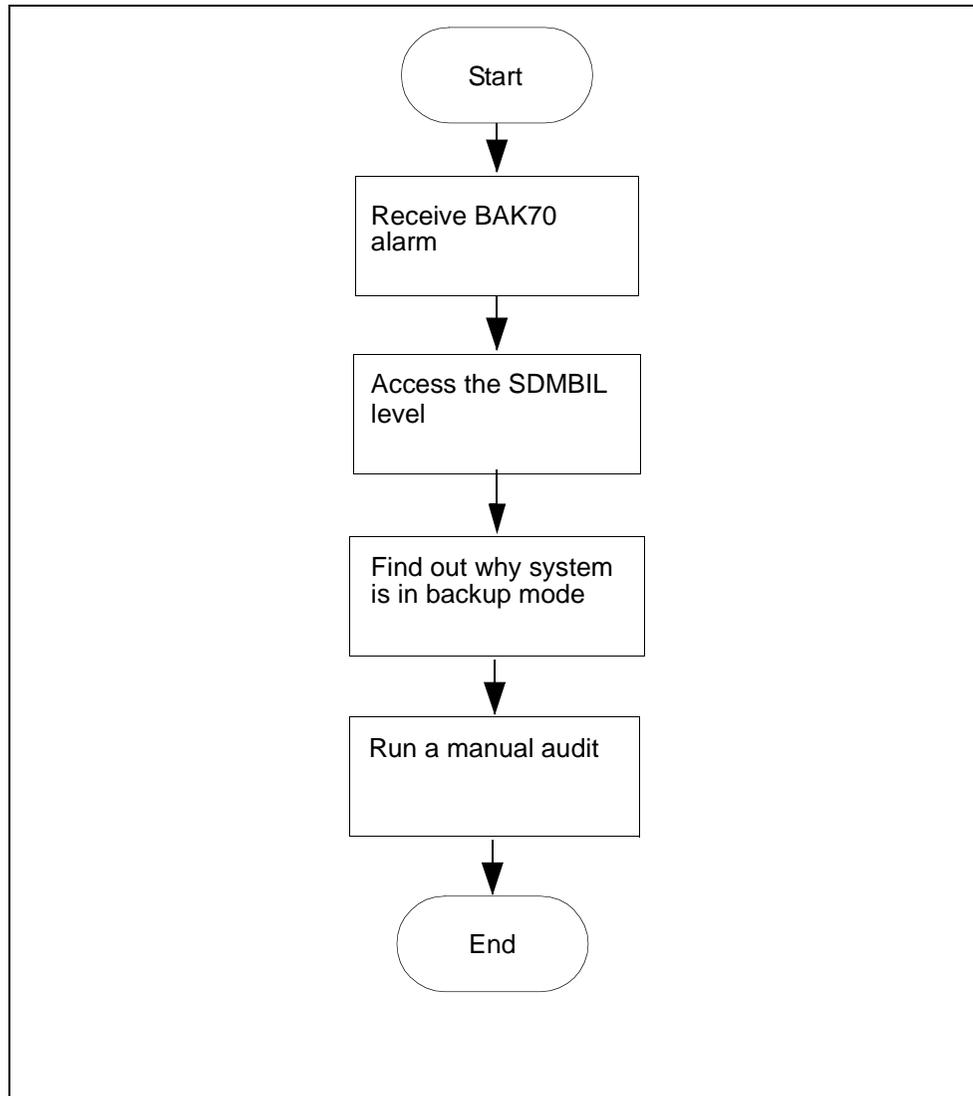
Clearing a BAK70 alarm

At the MAP

1   Post the billing stream by typing

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

and pressing the Enter key.

Where

<x> is the name of the billing stream.

2   Determine why the system is in backup mode and check the system node state.

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

If the SBA is	Do
SysB	refer to Clearing a DSKWR alarm, Clearing a NOCOM alarm, Clearing a major SBACP alarm, Clearing a minor SBACP alarm (depending on why you are receiving alarm)
ManB	determine if you still have sufficient space in the backup volume, continue with step 4
RBsy	refer to Clearing a major SBACP alarm

4   Display the names of the backup volumes by typing

> **conf view <x>**

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

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

> **diskut;lv s00d<xxxx>**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

> *Note:* This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D), or if the backup volumes are on IOP disks (their names start with F02L or F17L). If the volume information starts with D000 or D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

6   Display the size of the second volume and its number of free blocks by typing

        `> diskut;lv s01d<xxxx>`

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

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

If the volumes	Do
have enough disk space	you have completed this procedure
do not have enough disk space	refer to procedure "Configuring IOP disk drive backup volumes" in the Accounting section, if you are on XA-core. Otherwise, refer to procedures "Configuring SLM disk drive backup volumes" and "Configuring DDU disk drive backup volumes" in the Accounting section. You must use IOP volumes on XAC16 systems.

8   Use Audit to clear the alarm. If the alarm does not clear, contact your next level of support.

Clearing a BAK90 alarm

Indication

At the MTC level of the MAP display, BAK90 appears under the APPL header of the alarm banner and indicates an alarm for the backup system.

Note: The term "XAC16" is used in this document to mean an XA-Core system based on CSP16 or later. To determine if this applies to your system, run the IMAGENAME command on your CM. If the first line of the response begins with "XA", you are on a XA-Core system. If the line that begins "LAYER: TL" indicates 16 or higher, then "XAC16" notes apply to your system.

Meaning

The backup system is using more than 90 percent of the total space on backup volumes on the DMS/CM. If the stream is set to `on`, the alarm is critical; if the stream is set to `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.

The CS 2000 Core Manager generates the SDMB820 log report when this alarm is raised.

Impact

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

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's collector through the previously-established network that DIRP uses.

Action

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

BAK90 alarm clearing flowchart

```
                    ┌─────────────┐
                    │    Start    │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Receive BAK90│
                    │  alarm      │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Access the  │
                    │ SDMBIL level│
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │Find out why │
                    │system is in │
                    │backup mode  │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │Run a manual │
                    │audit        │
                    └──────┬──────┘
                           │
                           ▼
                    ┌─────────────┐
                    │     End     │
                    └─────────────┘
```
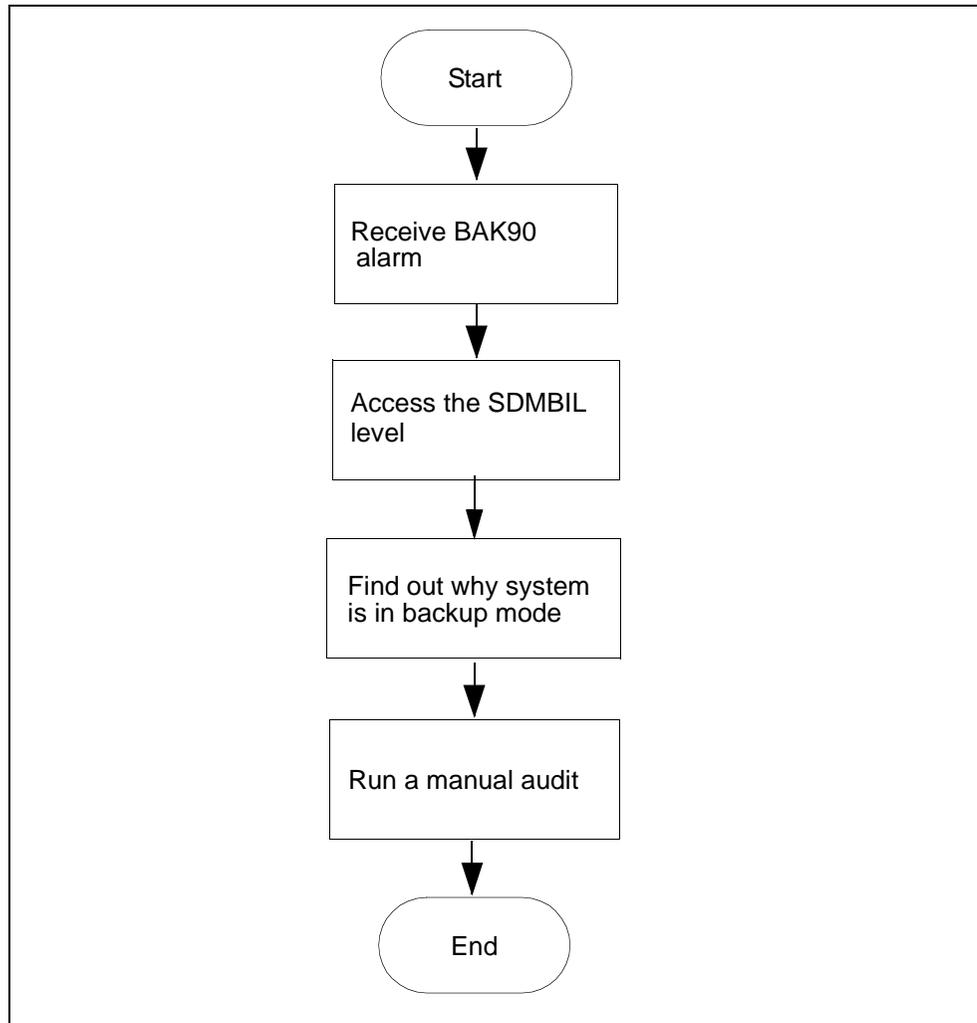
Clearing a BAK90 alarm

At the MAP

1   Post the billing stream by typing

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

and pressing the Enter key.

Where

<x> is the name of the billing stream.

2   Determine why the system is in backup mode and check the system node state.

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

If the SBA is	Do
SysB	refer to <u>Clearing a DSKWR alarm</u>, <u>Clearing a NOCOM alarm</u>, <u>Clearing a major SBACP alarm</u>, <u>Clearing a minor SBACP alarm</u> (depending on why you are receiving alarm)
ManB	determine if you still have sufficient space in the backup volume, continue with step <u>4</u>
RBsy	refer to <u>Clearing a major SBACP alarm</u>

4   Display the names of the backup volumes by typing

> **`> conf view <x>`**

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> ***Note:*** SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

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

> **`> diskut;lv s00d<xxxx>`**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

> ***Note:*** This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D), or if the backup volumes are on IOP disks (their names start with F02L or F17L). If the volume information starts with D000 or D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

6   Display the size of the second volume and its number of free blocks by typing

```
> diskut;lv s01d<xxxx>
```

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

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

If the volumes	Do
have enough disk space	you have completed this procedure
do not have enough disk space	refer to procedure "Configuring IOP disk drive backup volumes" in the Accounting section, if you are on XA-core. Otherwise, refer to procedures "Configuring SLM disk drive backup volumes" and "Configuring DDU disk drive backup volumes" in the Accounting section. You must use IOP volumes on XAC16 systems.

8   Use Audit to clear the alarm. If the alarm does not clear, contact your next level of support.

Clearing a BAKUP alarm

Indication

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

Note: The term "XAC16" is used in this document to mean an XA-Core system based on CSP16 or later. To determine if this applies to your system, run the IMAGENAME command on your CM. If the first line of the response begins with "XA", you are on a XA-Core system. If the line that begins "LAYER: TL" indicates 16 or higher, then "XAC16" notes apply to your system

Meaning

Records are stored on the DMS/CM backup volume for more than 10 minutes. If the stream is set to `on`, the alarm is major; if the stream is set to `both`, the alarm is minor.

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.

The CS 2000 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. If such a problem occurs, BAK`xx` alarms notify you (where `xx` is the percentage of disk storage used).

If the stream is set to `both`, data is still being routed to DIRP. Therefore, if the SBA storage reaches capacity and cannot accept more data, you can send the billing records to the operating company's collector through the previously-established network that DIRP uses.

It is possible for a backup volume to fill up and it can be swapped for a volume that has free space using the `conf set` command.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

Once the system goes into recovery mode, the volume that is swapped out can be swapped back into the system to complete the recovery.

Action

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

BAKUP alarm clearing flowchart

Clearing a BAKUP alarm

At the MAP

1   Post the billing stream by typing

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

and pressing the Enter key.

Where

<x> is the name of the billing stream.

2   Determine why the system is in backup mode and check the system node state.

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

If the SBA is	Do
SysB	refer to <u>Clearing a DSKWR alarm</u>, <u>Clearing a NOCOM alarm</u>, <u>Clearing a major SBACP alarm</u>, <u>Clearing a minor SBACP alarm</u> (depending on why you are receiving alarm)
ManB	determine if you still have sufficient space in the backup volume, continue with step <u>4</u>
RBsy	refer to <u>Clearing a major SBACP alarm</u>

4   Display the names of the backup volumes by typing

> **conf view <x>**

and pressing the Enter key.

Where

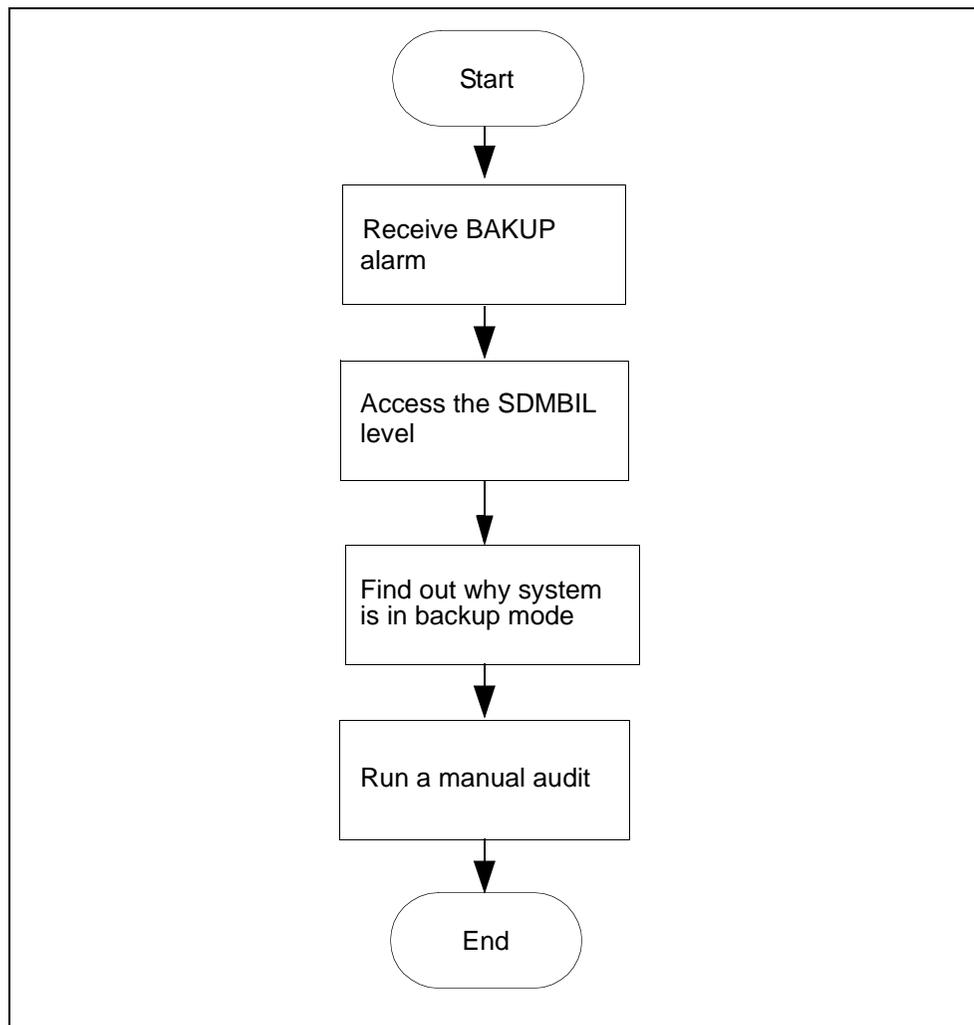<x> is the name of the billing stream.

> ***Note:*** SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

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

> `> diskut;lv s00d<xxxx>`

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

> *Note:* This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D), or if the backup volumes are on IOP disks (their names start with F02L or F17L). If the volume information starts with D000 or D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

6   Display the size of the second volume and its number of free blocks by typing

> `> diskut;lv s01d<xxxx>`

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the first volume.

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

If the volumes	Do
have enough disk space	you have completed this procedure
do not have enough disk space	refer to procedure "Configuring IOP disk drive backup volumes" in the Accounting section, if you are on XA-core. Otherwise, refer to procedures "Configuring SLM disk drive backup volumes" and "Configuring DDU disk drive backup volumes" in the Accounting section. You must use IOP volumes on XAC16 systems.

8   Use Audit to clear the alarm. If the alarm does not clear, contact your next level of support.

Clearing 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 CS 2000 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 ID's 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.

You can determine the value of the active template ID on the DMS/CM by using the following command:

```
> CTMPLT "template all"
```

You can set the CurrentTmpltID mib parameter to match the value of the active template ID on the CM by typing:

```
mib cdr set CurrentTmpltID <x>
```

Where

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

> *Note 1:* If you change the CurrentTmpltID MIB parameter after you have turned on the stream, you must BSY and then `rts` the SBA application to activate the change.

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

Clearing a DSKWR alarm

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 CS 2000 Core Manager disk because the disk is unavailable or the disk is full.

The CS 2000 Core Manager generates the SDMB355 log report when this alarm is raised.

Impact

The DMS/CM cannot send the billing records to the CS 2000 Core Manager. As a result, the DMS/CM send the billing records to backup storage. However, this backup storage is limited. As the backup storage becomes filled, alarms notify you as to how much of its capacity is used.

Action

Use the following procedure to clear DSKWR alarm.

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

Clearing a DSKWR alarm

At the MAP interface on the CM

1 Access the SDMBIL level by typing

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

and pressing the Enter key.

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

> **`dispal`**

and pressing the Enter key.

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

If the NOBAK or NOSTOR alarm	Do
appears in the alarm banner	performing the procedure "Configuring SLM disk backup volumes", and (if necessary) "Configuring DDU disk backup volumes", in the Accounting section
does not appear in the alarm banner	step 4

4   Log in to the CS 2000 Core Manager as the root user.

5   Access the maintenance level by typing

```
# sdmmtc
```

and pressing the Enter key.

6   Access the hardware level by typing

```
> hw
```

and pressing the Enter key.

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

If DSK1 or DSK2 is	Do
InSv (represented by a dot [.])	the disk hardware is in service (InSv) and you are still receiving an alarm, skip 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 by typing

`> rts <domain> <device>`

and pressing the Enter key.

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   Refer to the following table to determine your next step.

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 by typing

`> storage`

and pressing the Enter key.

Response:

Line x displays the following information

- 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 in line *x* 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 it to tape. However, prior to sending the billing files, first determine if you have received an FTPW critical alarm.

11 Quit the SDMMTC interface by typing

> **`> quit all`**

and pressing the Enter key.

12 Access the BILLMTC interface by typing

> **`> billmtc`**

and pressing the Enter key.

13 Access the FILESYS level by typing

> **`> filesys`**

and pressing the Enter key.

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

`> sendfile <x>`

and pressing the Enter key.

Where:

<x> is the name of the stream.

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

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

If the SENDFILE command	Do
is not successful	refer to procedures <u>Verifying the file transfer protocol</u> and <u>Verifying the FTP Schedule</u> in the Fault Management section, then return to this procedure and repeat step <u>14</u>
is successful	step <u>16</u>
is not successful after you reference the procedures	contact your next level of support

16 Quit the BILLMTC interface by typing

> **`> quit all`**

and pressing the Enter key.

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

> `> cd/sba/<x>/orphan`

and pressing the Enter key.

Where:

<x> is the name of the billing stream.

If	Do
your billing files are full because they have accumulated in orphan files and you are unclear 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 incurring a problem	step 18

18   Verify the write permission and ownership for the directories in /sba/<x>, where <x> is the billing stream.

19   Refer the following table to determine your next step.

If the	Do
permissions {rwx r-x r-x} and file ownership {maint} are correct	contact your next level of support
permissions for a directory are not rwx r-x r-x	step 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 by typing

> `> chmod 755 <directory>`

and pressing the Enter key.

Where:

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

21 Change the ownership of a directory by typing

> `> chown maint <directory>`

and pressing the Enter key.

Where:

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

22 You have completed this procedure.

Clearing an EXT FSP major alarm

Application

Use this procedure to clear an EXT FSP major MAP alarm that has been triggered by the CS 2000 Core Manager.

Note: The EXT FSP alarm is used to report fault conditions on frame supervisory panels (FSPs) and modular supervisory panels (MSPs) in various types 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 manual 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, it may be that the alarm card or the fuse is 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 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 following figure). This LED is normally on (green), but if it is off, there is no input power to the CS 2000 Core Manager.

- The CS 2000 Core Manager has reached its maximum allowable operating temperature threshold. 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 following figure). 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.

- The CS 2000 Core Manager power supply has failed. 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 following figure). This LED is normally on (green), but if it is off, there is no output power from the CS 2000 Core Manager power supply.

LEDs on the MSP at the top of the CS 2000 Core Manager cabinet
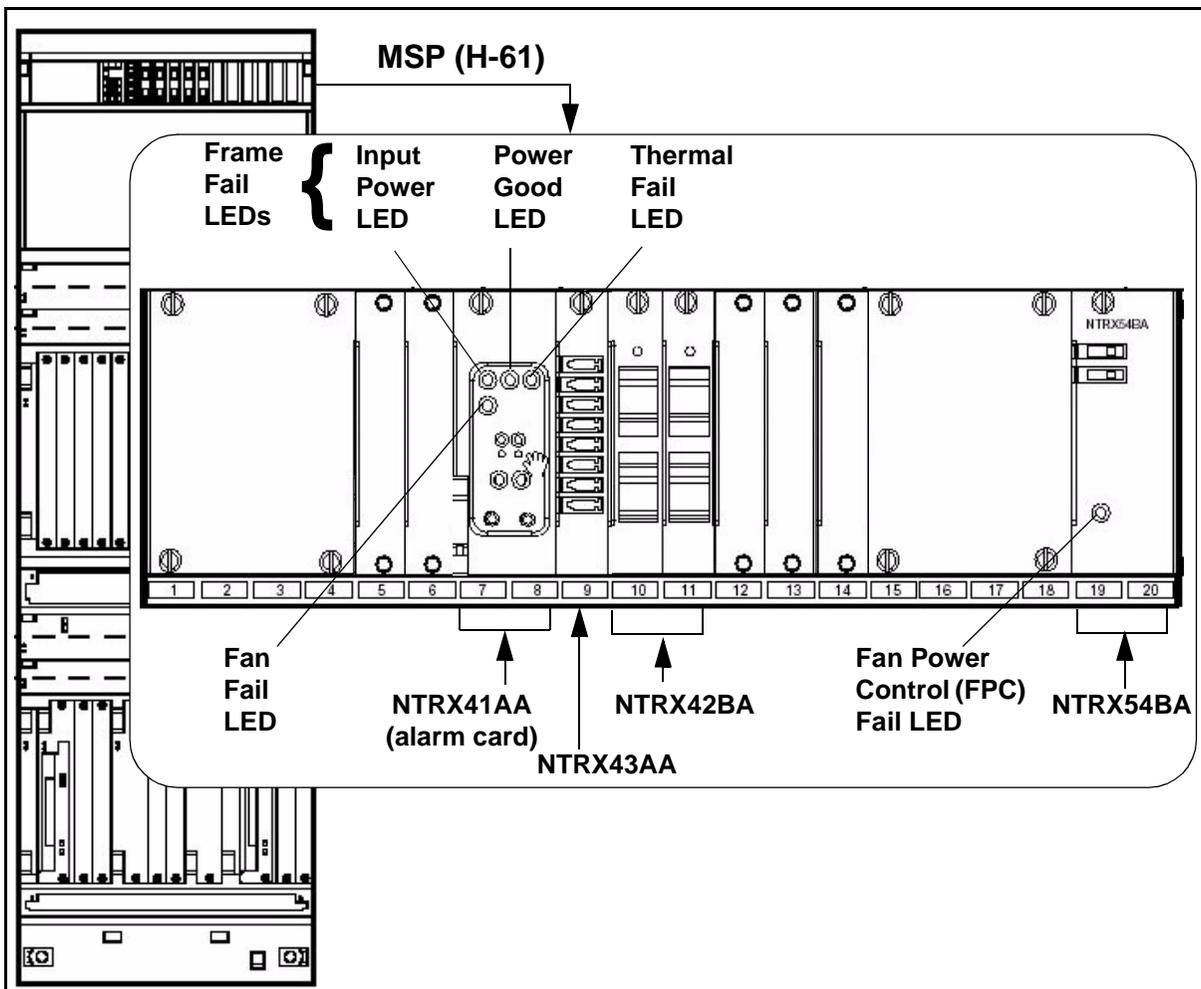
Impact

The CS 2000 Core Manager is out of service and no applications can run.

Action

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

Summary of clearing an Ext FSP major alarm

Check the input and output power LEDs on the MSP of the CS 2000 Core Manager cabinet

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

Check MSP breakers

Breakers tripped? — **Y** → Restore power → **1**

N

Power available? — **N** → Restore power → **1**

Y

Check SDM550 logs

Ambient heat source? — **N** → Check fan trays, and log reports → Fan failure? — **N** → Contact next level of support → **2**

Y

Remove heat source

Y (Fan failure) → Replace fan module(s)

Check alarms → **2**

Allow the system to cool down

3 → Cycle power to the system

Monitor boot process ← **1**

3

End ← **2**

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   Use the following table to determine your next step.

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, then two logs were generated. The first log was generated when the CS 2000 Core Manager reached its thermal warning threshold (60x C or 140x F). The second log was generated to indicate that shutdown will occur in 1 min. because its shutdown thermal threshold has been reached (80x C or 176x F)

At the C28B cabinet containing the CS 2000 Core Manager

12   At the C28B cabinet, determine if an ambient heat source has caused the thermal shutdown.

   Note: An ambient heat source may consist of an excessively high air temperature in the vicinity of the CS 2000 Core

Manager, excessive heat from an adjacent frame, or a combination of these factors.

If	Do
an ambiant heat source is present	step 20
the temperature 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 the fan blades in each fan are rotating, and then 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 to ensure it has returned 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's progress as follows:

- The critical alarm LED shows red

- The Component Out-of-Service LED flashes

- The component Out-of-Service LED turns solid

- The LEDs on the various service modules show green as they go into service

- The critical alarm LED and the Component Out-of-Service LED turn off: the System in Service LED and the CPU1 service module LED flash

- The 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.

398

Clearing a FREE SPACE alarm

Indication

> **ATTENTION**
> Do not attempt to clear a free space alarm when the volume group is performing re-integration.

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 on the condition that 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 (default threshold value: 400MB).

Impact

The free space for a volume group is lower than the default threshold, which can cause difficulties during upgrade.

Action

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

FREE SPACE alarm clearing flowchart

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

Receive a FREE SPACE alarm

Access storage level

Volume group mirrored? — **Y** → Force to clear? — **Y** → Confirm change? — **Y** → End of procedure

N ↓
Wait for re-integration to complete

N ↓
Upgrade the corresponding input/output module

N ↓ 1

Alarm cleared after re-integration? — **Y** → End of procedure

N ↓ 1

1 (Force to clear)

Clearing a FREE SPACE alarm

At the maintenance interface

1   Access the storage level by typing

> `> sdmmtc storage`

and pressing the Enter key.

If the state is	Do
not mirrored	step 2
mirrored	step 3

2   Wait until the re-integration is complete, then refer to the following table to determine your next step.

Is the alarm	Do
not cleared after re-integration	step 3
cleared after re-integration	step 7

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

Is the alarm cleared	Do
normally	step 4
by force to clear	step 5

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

If the alarm is for	Do
rootvg	procedure *"Upgrading the rootvg MFIO to MFIO or to UMFIO"* in the Upgrades section to add more space to rootvg
datavg	procedure *"Upgrading a datavg MFIO to MFIO or to UMFIO"* in the Upgrades section to add more space to datavg

5   Force to clear the alarm by typing

> **`> change <volume_group_name> <new_threshold>`**

and pressing the Enter key.

where:
volume_group_name = 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

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 CS 2000 Core Manager generates the SDMB375 log report when this alarm is raised.

Impact

The CS 2000 Core Manager cannot FTP files to the downstream destination. It is possible that the CS 2000 Core Manager has reached storage capacity, depending on the amount of storage and the volume of records. As the CS 2000 Core Manager storage becomes full, alarms notify you of how much of its capacity is used. When this storage is full, the DMS/CM sends subsequent records to backup storage.

Action

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

FTP alarm clearing flowchart

```
                    ┌─────────────┐
                    │    Start    │
                    └─────────────┘
                           │
                           ▼
                    ┌─────────────┐
                    │ Receive the │
                    │  FTP alarm  │
                    └─────────────┘
                           │
                           ▼
                    ┌─────────────┐
                    │  Verify FTP │
                    │             │
                    └─────────────┘
                           │
                           ▼
                                    N    ┌─────────────┐      ┌─────────┐
                   ╱            ╲───────▶ │ Contact your│ ───▶ │   End   │
                  ╱ Alarm cleared?╲       │ next level of│      └─────────┘
                   ╲            ╱         │   support   │
                           │             └─────────────┘
                           │ Y
                           ▼
                    ┌─────────────┐
                    │     End     │
                    └─────────────┘
```

Clearing an FTP alarm

At the MAP

1   Examine the SDMB logs for details about the FTP problem, by typing

> **logutil;open sdmb**

and pressing the Enter key.

> *Note:* This command displays the most recent logs.

2   Verify that the FTP is working by performing Verifying the file transfer protocol in the Fault Management section.

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

4   You have completed the procedure.

Clearing an FTPW alarm

Indication

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

Meaning

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

Note: The FTPW alarm may be present on the CM for a non-existent schedule. For example, if an operator shut down the server, which made the ftp service on the server unavailable to the CS 2000 Core Manager, and did not delete the associated schedule tuple on the CS 2000 Core Manager first, the FTPW alarm is generated.
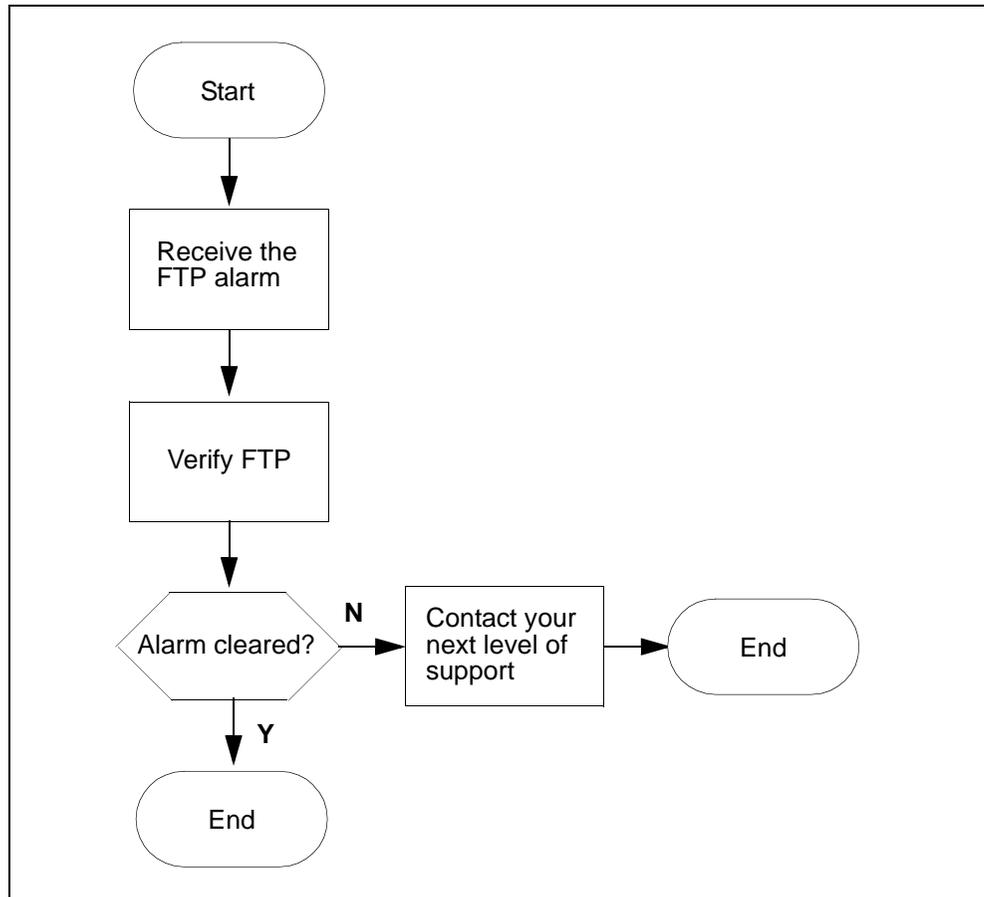
Impact

The CS 2000 Core Manager cannot send files to the downstream destinations. The CS 2000 Core Manager has possibly reached storage capacity, depending on the amount of storage and the volume of records. When this storage is full, the DMS switch/CM sends subsequent records to backup storage. When backup storage reaches capacity, billing records are lost.

Action

Clearing an FTPW alarm

At the CS 2000 Core Manager

1   Complete procedure <u>Verifying the file transfer protocol</u> in the Fault Management section.

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

Note: If you determine that the alarm was raised for a non-existent schedule, add a schedule tuple with the same stream name and destination as the one for which the alarm was raised using procedure "Configuring the outbound file transfer schedule" in the Accounting section, then return to this procedure. Once the alarm is cleared, you can delete the tuple you added.

3   You have completed the procedure.

406

Recovering from a half shelf down power failure

Application

Use this procedure to bring the X.25 link back into service following routine maintenance or a power failure.

Note that this procedure is only valid for a system configured with a single X.25 card.

If a problem occurs that requires the help of the local maintenance personnel gather all important logs, reports, and system information for analysis. The related logs, maintenance notes, and system information help make sure 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 NN10194-113, *Lawful Intercept Product and Technology Fundamentals, Intl).*

408

Clearing an inbound file transfer alarm

Indication

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

Meaning

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

Detailed information about the alarm condition is documented in a log report that is generated when the alarm is raised (SDMB375 or SDMB380). After this alarm is cleared, log report SDMB675 or SDMB680 are generated.

Impact

Inbound file transfer attempts for the billing stream are not successful.

Action

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

*   the ftpdir directory has no write access

*   the storage for the billing stream has no space available

*   the <rcLogicalVolumeDirectory>/ftpdir directory does not exist

Determine which alarm is present by observing the log text and mapping it to the associated alarm.

Clearing an IFT alarm

At the MAP

1   Log in to the CS 2000 Core Manager as maint user.

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

If	Do
the /home/maint/ftpdir directory has write permissions	no action is required.
the /home/maint/ftpdir directory does not have write permissions	perform step 3 only.
the <rcLogicalVolumeDirectory>/ ftpdir directory has write permissions	no action is required.
the <rcLogicalVolumeDirectory>/ ftpdir directory does not have write permissions	perform step 4 only.
the storage disk has sufficient space	no action is required.
the storage disk does not have sufficient space	perform step 5 only.
the <rcLogicalVolumeDirectory> path is correct	no action is required.
the <rcLogicalVolumeDirectory> path is incorrect	correct the <rcLogicalVolumeDirectory> path into the CONFSTRM.
the <rcLogicalVolumeDirectory>/ ftpdir is a directory	no action is required.
the <rcLogicalVolumeDirectory>/ ftpdir is not a directory	perform step 6 only.
the IFT alarm persists once you have performed the appropriate steps in Procedure	contact your next level of support.

3   Change the permissions of the /home/maint/ftpdir directory by typing

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

and pressing the Enter key.

4   Remove the <rcLogicalVolumeDirectory>/ftpdir directory by typing

> `> rm /<rcLogicalVolumeDirectory>/ftpdir`

and pressing the Enter key,

where

<rcLogicalVolumeDirectory> is the logical volume assigned to the billing stream in the `confstrm` for the billing files to be stored.

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

5   Retrieve some closed not sent files and rename them to closed sent.

> *Note 1:* Closed not sent files for DNS and DIRP have the suffixes of .pri and .unp respectively. When you rename them, change the suffixes 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, you can consider increasing the size of the logical volume.

6   Remove the <rcLogicalVolumeDirectory>/ftpdir directory by typing

> `> rm /<rcLogicalVolumeDirectory>/ftpdir`

and pressing the Enter key.

<rcLogicalVolumeDirectory> is the logical volume assigned to the billing stream in the `confstrm` for the billing files to be stored.

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

7   You have completed the procedure.

Clearing an LODSK alarm

> **CAUTION**
> **Possible Loss of Service**
> If you receive a LODSK alarm, FTP the billing files in the closedNotSent directory or write to tape immediately. Refer to <u>Verifying the file transfer protocol</u> for more information.

Indication

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 CS 2000 Core Manager generates the SDMB355 log report when this alarm is raised.

Impact

The CS 2000 Core Manager storage capacity is becoming full. As the storage becomes full, alarms notify you of how much capacity is used. In addition, there is a possibility that the DMS/CM does not go into backup mode if the disks reach 100 percent capacity.

Action

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

LODSK alarm clearing flowchart

```
                    ┌─────────┐
                    │  Start  │
                    └────┬────┘
                         │
              ┌──────────▼──────────┐        ┌──────────────────────┐
              │ Receive LODSK       │        │ Verify that the FTP  │
              │ alarm               │        │ schedule is          │
              │                     │        │ working              │
              └──────────┬──────────┘        └──────────┬───────────┘
                         │                              │
              ┌──────────▼──────────┐        ┌──────────▼───────────┐
              │ Verify that FTP     │        │ Send the primary     │
              │ is working          │        │ billing files to the │
              │                     │        │ destination and      │
              └─────────────────────┘        │ contact your next    │
                                             │ level of support     │
                                             └──────────┬───────────┘
                                                        │
                                                   ┌────▼────┐
                                                   │   End   │
                                                   └─────────┘
```
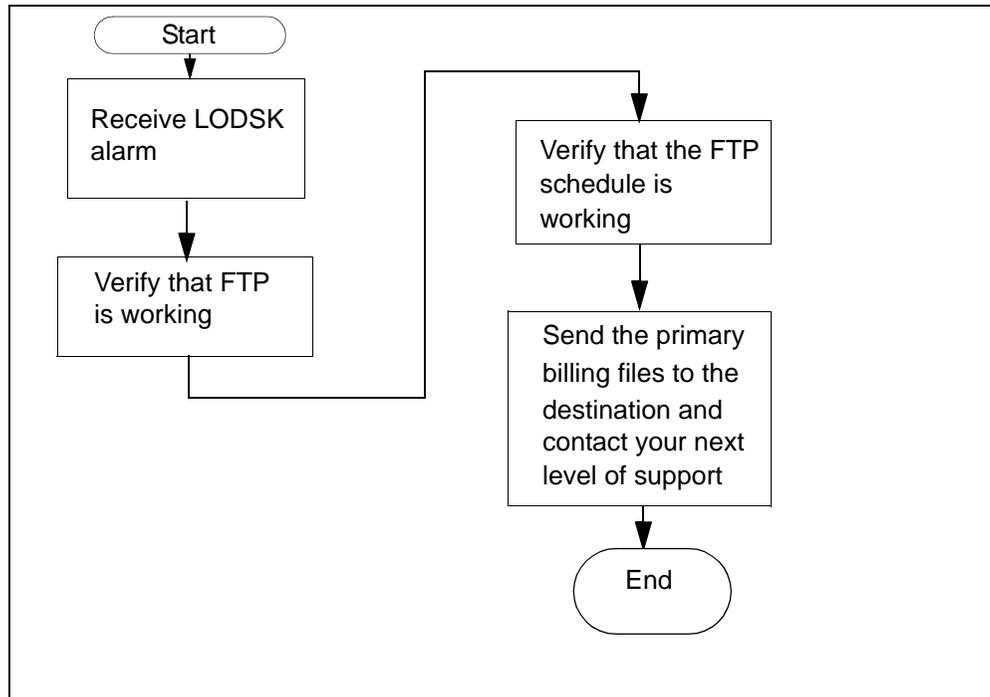
Clearing a LODSK alarm

At the MAP

1   Use the procedure <u>Verifying the file transfer protocol</u> to determine if the FTP is working properly.

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

If the alarm	Do
clears	you have completed this procedure
does not clear	refer to procedure <u>Verifying the FTP Schedule</u> in the Fault Management section
does not clear after you have performed the procedure	contact your next level of support

Clearing a NOBAK alarm

Indication

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

Meaning

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

Impact

If the stream is set to `on`, billing records are lost.

If the stream is set to `both`, data continues to route to DIRP. Therefore, you can send the billing records to the operating company's collector through the previously-established network that DIRP uses.

Action

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

NOBAK alarm clearing flowchart
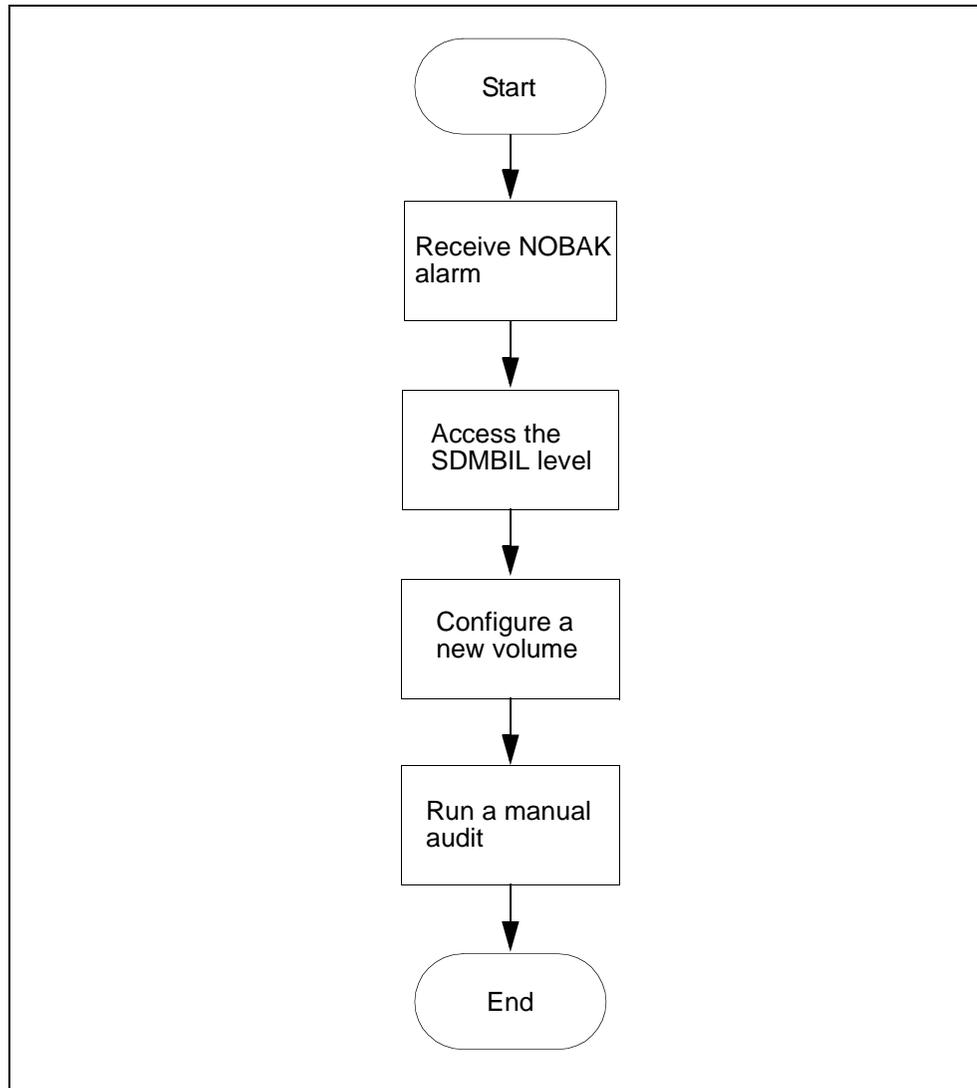
Clearing a NOBAK alarm

At the MAP

1   Post the billing stream by typing

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

and pressing the Enter key.

Where

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

2   Display the names of the billing stream by typing

`> conf view <x>`

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

3   Display the storage usage by typing

`> mtc;sys;storage`

and pressing the Enter key.

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

Send the primary file (closedNotSent directory) by typing

`> sendfile <x>`

and pressing the Enter key.

Where

<x> is the name of the stream.

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

5   Use Audit to clear the alarm.

6   Refer to the following table for your next step.

If the alarm	Do
clears	you have completed this procedure
does not clear	contact your next level of support

Clearing a NOCLNT alarm

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

Indication

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

Meaning

The stream was activated by the SDMBCTRL command before initialization was complete. If the stream is set to `on`, the alarm is critical; if the stream is set to `both`, the alarm is major.

Impact

No data is buffered by the SBA system. Therefore, no data is backed up or made available for delivery to the CS 2000 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's collector through the previously-established network that DIRP uses.

Action

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

Clearing a NOCOM alarm

Indication

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

Meaning

Communications between the Communication Server 2000 core and the CS 2000 Core Manager is disrupted.

The most likely causes of this alarm are that the DS-512 links are not in-service making the CS 2000 Core Manager SysB, the CS 2000 Core Manager power is off, or the CS 2000 Core Manager is rebooting.

Impact

No data is transferred to the CS 2000 Core Manager. Data is sent to the configured backup disk on the Communication Server 2000 core.

If the stream is set to `both`, data is still being routed to device independent recording package (DIRP). Therefore, you can send the billing records to the operating company's collector through the previously established network that DIRP uses.

ATTENTION

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

Action

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

At the MAP

1 Access the APPL SDM Menu level by typing

> `mapci;mtc;appl;sdm`

and pressing the Enter key.

2 Use the following table to determine your next step.

If the CS 2000 Core Manager is	Do
Offl or SysB	step 3
ManB	step 4
InSv or ISTb	step 5

3 Busy the CS 2000 Core Manager by typing

> **bsy**

and pressing the Enter key.

4 Return the CS 2000 Core Manager to service by typing

> **rts**

and pressing the Enter key.

Note 1: Returning the CS 2000 Core Manager to service establishes communication between the Communication Server 2000 core and the CS 2000 Core Manager. If the first attempt fails to return the CS 2000 Core Manager to service, the system re-attempts to establish communication until it is successful.

Note 2: The SDM Billing Application (SBA) and any streams configured for real-time billing (RTB) are also returned to service when the CS 2000 Core Manager is returned to service. Log report SDMB375 is generated when a stream configured for RTB fails to return to service.

If the CS 2000 Core Manager	Do
returns to service successfully	step 5
does not return to service successfully	contact your next level of support

5 Use the following table to determine your next step.

If the alarm	Do
cleared	step 6
did not clear	contact your next level of support

At the CS 2000 Core Manager

6   Use the following table to determine your next step.

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

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

a   Access the billing maintenance level by typing

 # billmtc

and pressing the Enter key.

b   Access the schedule level by typing

> schedule

and pressing the Enter key.

c   Access the real-time billing level by typing

> rtb

and pressing the Enter key.

d   Busy the stream by typing

> bsy <stream name>

and pressing the Enter key.

Where:

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

e Return the stream to service by typing

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

and pressing the Enter key.

Where:

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

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

Clearing an NOFL alarm

Indication

At the MTC level of the MAP display, NOFL appears under the APPL header of the alarm banner and indicates an 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 `on`, the alarm is critical; if the stream is set to `on`, 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

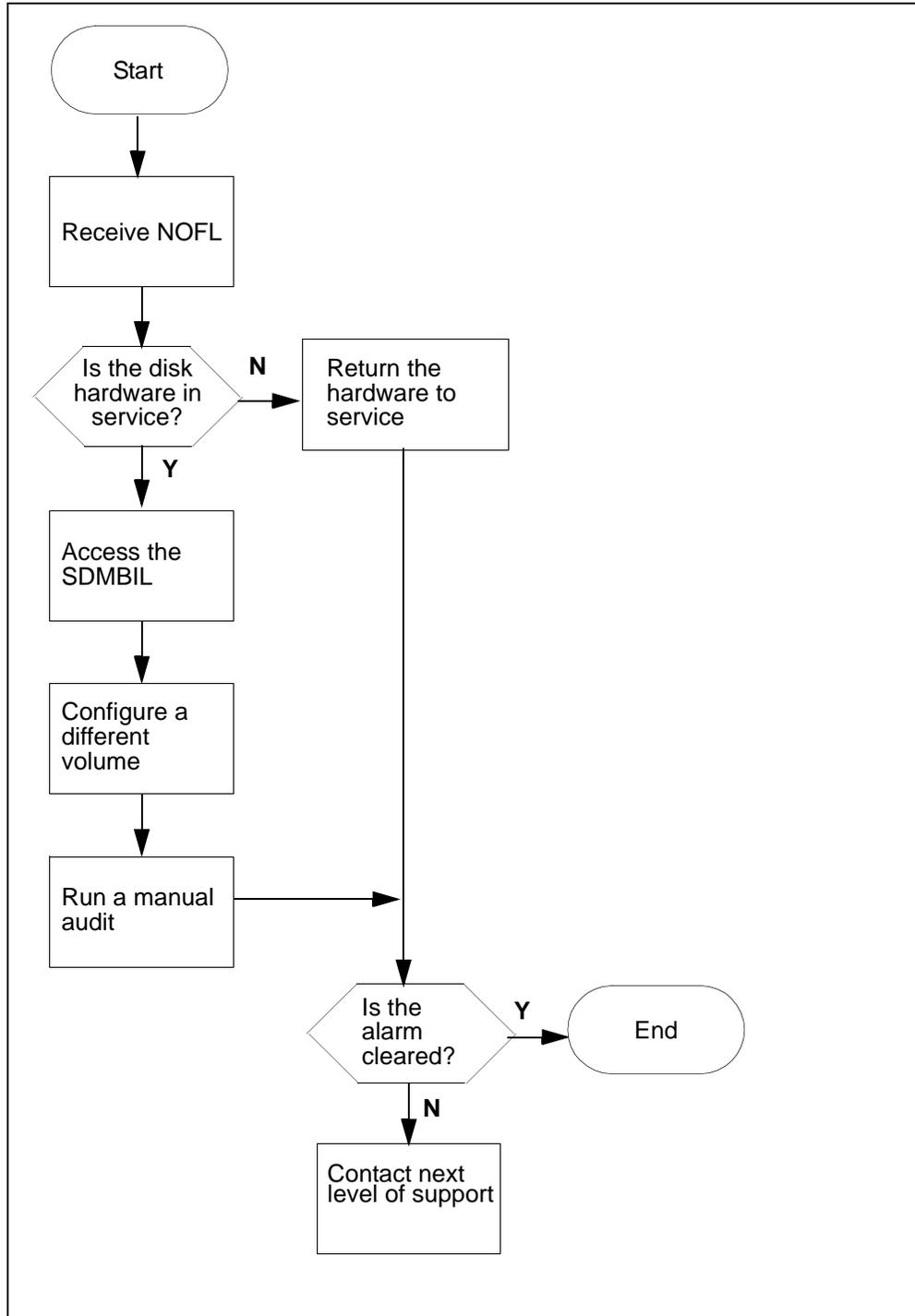Because no file is available for SBA data storage, data intended for storage is lost.

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's collector through the previously-established network that DIRP uses.

Action

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

NOFL alarm clearing flowchart

```
                    ┌──────────────┐
                   (    Start      )
                    └──────┬───────┘
                           │
                           ▼
                    ┌──────────────┐
                    │ Receive NOFL │
                    └──────┬───────┘
                           │
                           ▼
                     ╱──────────╲         N    ┌──────────────┐
                    ╱  Is the    ╲──────────────▶│ Return the   │
                    ╲  disk       ╱              │ hardware to  │
                     ╲ hardware  ╱               │ service      │
                      ╲in        ╱               └──────┬───────┘
                       ╲service? ╱                      │
                        ╲──┬──╱                         │
                           │ Y                          │
                           ▼                            │
                    ┌──────────────┐                    │
                    │ Access the   │                    │
                    │ SDMBIL       │                    │
                    └──────┬───────┘                    │
                           │                            │
                           ▼                            │
                    ┌──────────────┐                    │
                    │ Configure a  │                    │
                    │ different    │                    │
                    │ volume       │                    │
                    └──────┬───────┘                    │
                           │                            │
                           ▼                            │
                    ┌──────────────┐                    │
                    │ Run a manual │────────────┐       │
                    │ audit        │            │       │
                    └──────────────┘            ▼       ▼
                                            ╱──────────╲       Y    ┌──────────┐
                                           ╱  Is the    ╲───────────▶(   End    )
                                           ╲  alarm      ╱           └──────────┘
                                            ╲ cleared?  ╱
                                             ╲────┬───╱
                                                  │ N
                                                  ▼
                                           ┌──────────────┐
                                           │ Contact next │
                                           │ level of     │
                                           │ support      │
                                           └──────────────┘
```

Clearing a NOFL alarm

<table>
<tr>
<td>

CAUTION

Because the SLM is accessed by anyone who has access to the DMS/CM, coordinate with operating company personnel in charge of switch maintenance prior to any changes to the SLM.

</td>
</tr>
</table>

At the MAP

1 Access the I/O device and SLM Menu level to determine if the disk hardware is in service by typing

> **mapci;mtc;iod;slm**

and pressing the Enter key.

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

If the disk hardware is	Do
not InSv	step 3
InSv	step 4

3 Return the disk hardware (SLM or DDU in some cases) to service by typing

> **rts <n>**

and pressing the Enter key.

Where

<x> is either DSK0 or DSK1.

4 Post the billing stream by typing

> **appl;sdmbil;post <x>**

and pressing the Enter key.

Where

<x> is DSK0 or DSK1.

5 Determine the available disk space of the billing stream's existing backup volumes by typing

> **`> conf view <x>`**

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> *Note:* SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

6 Display the size of the first volume (DSK0) and its number of free blocks by typing

> **`> diskut;lv <s00dxxxx>`**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the volume.

> *Note:* This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D). If the volume information starts with D000 or D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

7 Display the size of the second volume (DSK1) and its number of free blocks by typing

> **`> diskut;lv <s01dxxxx>`**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the volume.

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

If the available disk space is	Do
insufficient	perform procedure "Configuring SLM disk drive backup volumes" or "Configuring DDU disk drive backup volumes" in the Accounting section
sufficient	step 9

9 Use Audit to clear the alarm.

10 Refer to the following table for your next step.

If the alarm	Do
clears	you have completed this procedure
does not clear	contact your next level of support

Clearing a NOREC alarm

Indication

At the MTC level of the MAP display, NOREC appears under the APPL header of the alarm banner and 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 CS 2000 Core Manager is full (also causes DSKWR and LODSK alarms where if the stream is set to `on`, the alarm is major and if the stream is set to `both`, the alarm is minor.

Impact

No backup files are recovered by the SBA system.

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

Action

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

432

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 CS 2000 Core Manager alarm.

Meaning

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

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

The CS 2000 Core Manager generates the SDMB370 log report when this alarm is raised.

Impact

The CDR2BAF conversion process does not create BAF records.

Action

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

Clearing a NOSTOR alarm

Indication

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

Meaning

The SBA buffer pool cannot allocate buffers. This means that all buffers are in use; it does not necessarily mean that the disk is full. If, however you also have alarms that indicate the disk is full, you need to configure a new volume. The NOSTOR alarm is usually seen when the system is in backup mode and the traffic is too high for the SLM to keep up with.

If the stream is set to `on`, the alarm is critical; if the stream is set to `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.
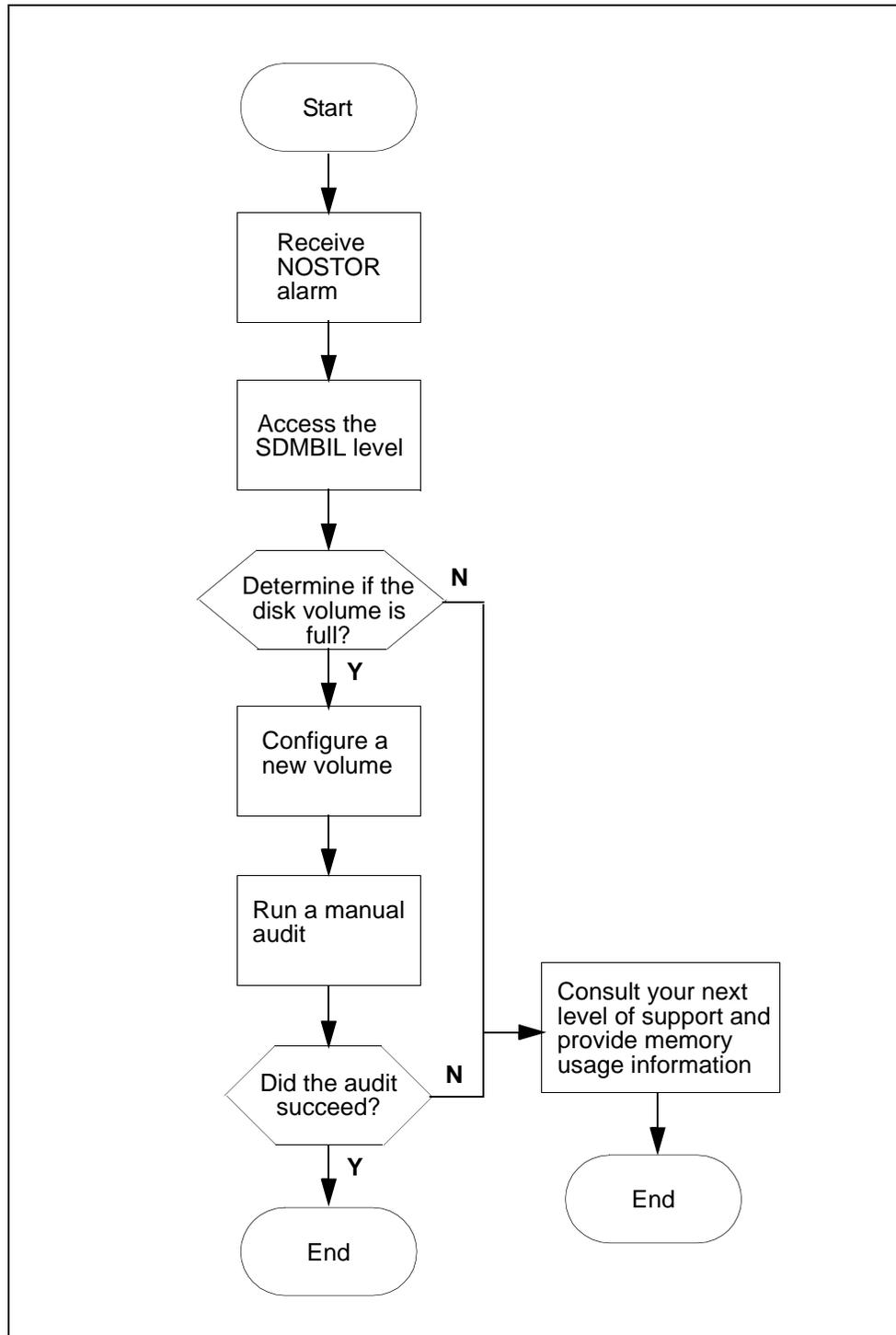

Impact

If the stream is set to `on`, there is a loss of billing records.

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's collector through the previously-established network that DIRP uses.

Action

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

NOSTOR alarm clearing flowchart

```
                          ┌──────────┐
                         (   Start    )
                          └─────┬────┘
                                │
                                ▼
                         ┌──────────────┐
                         │  Receive     │
                         │  NOSTOR      │
                         │  alarm       │
                         └──────┬───────┘
                                │
                                ▼
                         ┌──────────────┐
                         │  Access the  │
                         │  SDMBIL level│
                         └──────┬───────┘
                                │
                                ▼
                         ╱───────────────╲        N
                        ╱  Determine if the ╲──────────┐
                        ╲  disk volume is   ╱          │
                         ╲     full?      ╱            │
                          ╲──────┬──────╱              │
                                 │ Y                   │
                                 ▼                     │
                         ┌──────────────┐              │
                         │  Configure a │              │
                         │  new volume  │              │
                         └──────┬───────┘              │
                                │                      │
                                ▼                      │
                         ┌──────────────┐    ┌──────────────────────┐
                         │  Run a manual│    │ Consult your next    │
                         │  audit       │    │ level of support and │
                         └──────┬───────┘    │ provide memory       │
                                │            │ usage information    │
                                ▼            └──────────┬───────────┘
                         ╱───────────────╲   N          │
                        ╱   Did the audit  ╲────────────┘
                        ╲     succeed?     ╱             │
                         ╲──────┬─────────╱             ▼
                                │ Y                ┌──────────┐
                                ▼                 (    End     )
                          ┌──────────┐             └──────────┘
                         (    End     )
                          └──────────┘
```

Clearing a NOSTOR alarm

At the MAP

1   Post the billing stream by typing

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

and pressing the Enter key.

Where

<x> is the name of the billing stream.

2   Determine why the system is in backup mode by checking the node state.

3   Refer to the following table for your next step.

If the CS 2000 Core Manager is	Do
SysB	perform the procedure Clearing a NOCOM alarm
ManB	determine if you still have sufficient space in the backup volume, continue with step 4

4   Determine the available disk space of the billing stream's existing backup volumes by typing

> `> conf view <x>`

and pressing the Enter key.

Where

<x> is the name of the billing stream.

   Note: SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

5   Display the size of the first volume (DSK0) and its number of free blocks by typing

> `> diskut;lv <s00dxxxx>`

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the volume.

   Note: This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D). If the volume information starts with D000 or

D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

If you need to create disk volumes for XA-Core, refer to the *XA-Core Maintenance Manual*, 297-8991-510.

6 Display the size of the second volume (DSK1) and its number of free blocks by typing

```
> diskut;lv <s01dxxxx>
```

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the volume.

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

If available disk space is	Do
insufficient	refer to procedures "Configuring SLM disk drive backup volumes" or "Configuring DDU disk drive backup volumes" in the Accounting section
sufficient	step 8

8 Use Audit to clear the alarm.

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

If the alarm	Do
clears	you have completed this procedure
does not clear	contact your next level of support

Clearing a NOVOL alarm

Indication

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

Meaning

On startup, the SBA backup file system is unable to find a volume in which to create a file. If the stream is set to `on`, the alarm is critical; if the stream is set to `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

Because there is no volume available for SBA storage, data intended for backup storage can be lost. If the stream is set to `on`, billing records intended to be written to the backup volumes can be lost.

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's collector through the previously-established network that DIRP uses.

Action

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

NOVOL alarm clearing flowchart

```
                    ┌──────────────┐
                    │    Start     │
                    └──────┬───────┘
                           │
                           ▼
                    ┌──────────────┐
                    │ Receive NOVOL│
                    │ alarm        │
                    └──────┬───────┘
                           │
                           ▼
                  ╱─────────────╲      N    ┌──────────────┐
                 ╱  Is the disk   ╲─────────▶│ Return the   │
                 ╲  hardware      ╱          │ hardware to  │
                  ╲ in service?  ╱           │ service      │
                   ╲────┬───────╱            └──────┬───────┘
                        │ Y                         │
                        ▼                           │
                 ┌──────────────┐                   │
                 │ Determine why│                   │
                 │ the system is│                   │
                 │ in backup    │                   │
                 │ mode         │                   │
                 └──────┬───────┘                   │
                        │                           ▼
                        ▼              N   ╱─────────────╲   Y    ┌──────────┐
                 ┌──────────────┐◀─────────╲ Is the alarm ╱───────▶│   End    │
                 │ Access the   │          ╲  cleared?   ╱        └──────────┘
                 │ SDMBIL level │           ╲───────────╱
                 └──────┬───────┘
                        │
                        ▼
                 ┌──────────────┐
                 │ Configure a  │
                 │ different    │
                 │ volume       │
                 └──────┬───────┘
                        │
                        ▼
                 ┌──────────────┐          ┌──────────┐
                 │ Run a manual │─────────▶│   End    │
                 │ audit        │          └──────────┘
                 └──────────────┘
```
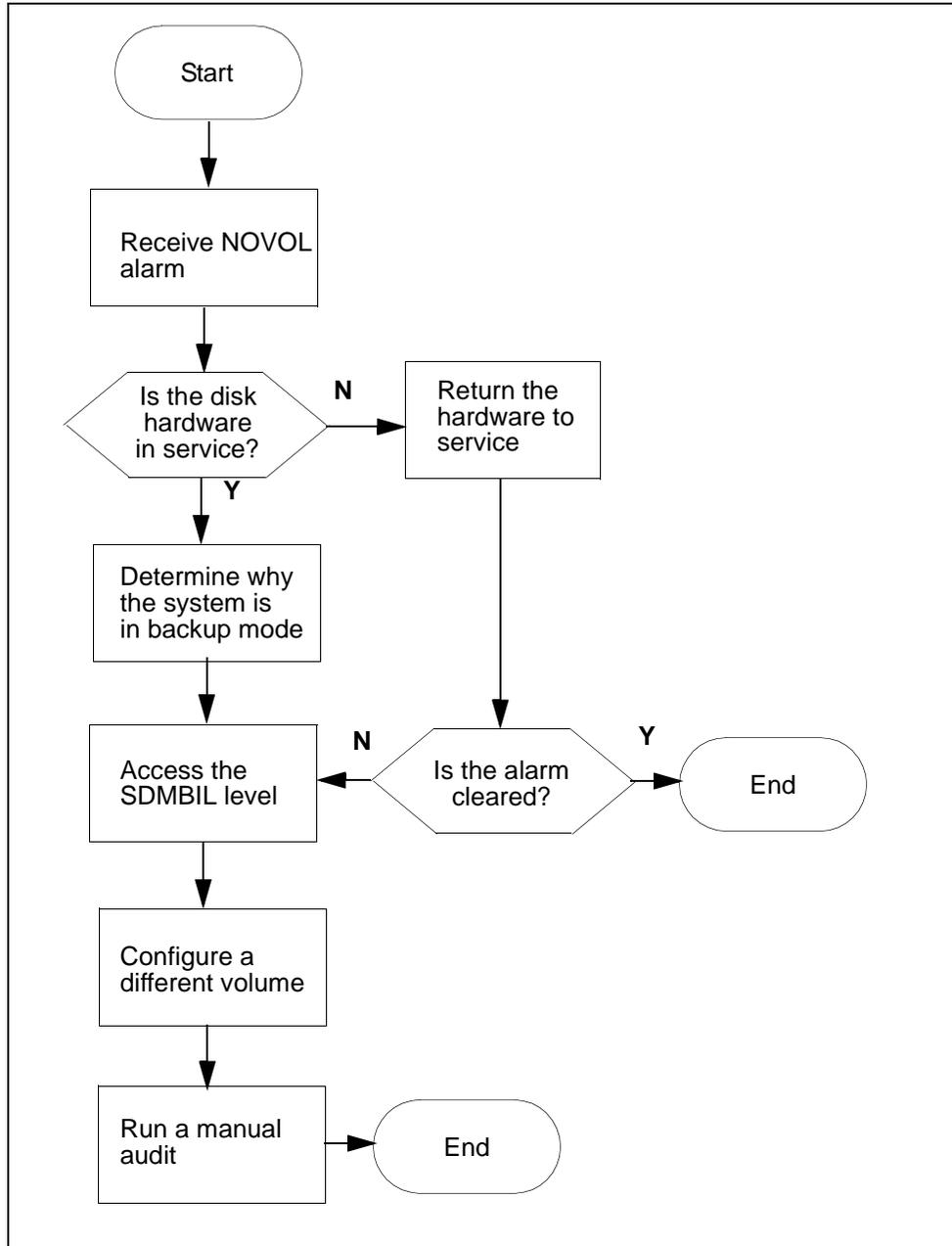
Clearing a NOVOL alarm

	CAUTION
⚠️	Because the SLM is accessed by anyone who has access to the DMS/CM, coordinate with operating company personnel in charge of switch maintenance prior to any changes to the SLM.

At the MAP

1   Access the I/O device and SLM Menu level to determine if the disk hardware is in service by typing

> **> mapci;mtc;iod;slm**

and pressing the Enter key.

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

If the disk hardware is	Do
InSv	step 4
not InSv	step 3

3   Return the disk hardware (SLM or DDU in some cases) to service by typing

> **> rts <x>**

and pressing the Enter key.

Where

<x> is either DSK0 or DSK1.

4   Post the billing stream by typing

> **> appl;sdmbil;post <X>**

and pressing the Enter key.

Where

<x> is DSK0 or DSK1.

5 Determine the available disk space of the billing stream's existing backup volumes by typing

> **`> conf view <x>`**

and pressing the Enter key.

Where

<x> is the name of the billing stream.

> ***Note:*** SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

6 Display the size of the first volume (DSK0) and its number of free blocks by typing

> **`> diskut;lv <s00dxxxx>`**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the volume.

> ***Note:*** This version of the disk utility command only works if the backup volumes are on SLM disks (their names start with S00D or S01D). If the volume information starts with D000 or D010, the backup volumes are on DDU disks (IOC) and you must use the DSKUT;SV command to retrieve the equivalent information.

> If you need to create disk volumes for XA-Core, refer to the *XA-Core Maintenance Manual*, 297-8991-510.

7 Display the size of the second volume (DSK1) and its number of free blocks by typing

> **`> diskut;lv <s01dxxxx>`**

and pressing the Enter key.

Where

<xxxx> is the unique identifier you choose to name the volume.

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

If the available disk space is	Do
insufficient	perform procedure "Configuring SLM disk drive backup volumes" or "Configuring DDU disk drive backup volumes" in the Accounting section
sufficient	step 9

9   Use Audit to clear the alarm.

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

If the alarm	Do
clears	you have completed this procedure
does not clear	contact your next level of support

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 indicates an alarm for the paging space configuration on the condition that the percentage full (*% full*) is within the threshold.

> *Note:* When the percentage full exceeds the threshold, refer to the procedure *"Changing logical volume thresholds"* in the Security section.

Meaning

A critical alarm indicates that the size of paging space configured on the SDM is less than 250MB. A major alarm indicates that the size of paging space configured on the CS 2000 Core Manager is between 250MB 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 impact depends on the current size of paging space and the loads of the system.

Action

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

PAGING SPACE alarm clearing flowchart

This flowchart summarizes the procedure.

Use the instructions in the procedure that follows this flowchart to perform the procedure.

Receive a PAGING SPACE alarm

↓

Access storage level in the maintenance interface

↓

1 → Enough free space? —**Y**→ Enter the command to clear the alarm

↓ **N**

Upgrade storage system to add more disk space to rootvg module

↓ **N**

1

Enter the command to clear the alarm
↓
Alarm cleared? —**Y**→ End of procedure

↓ **N**

Contact next level of support

Clearing a PAGING SPACE alarm

At the maintenance interface

1   Access the storage level by typing

> **> sdmmtc storage**

and pressing the Enter key.

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 by typing **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 Upgrades section) 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 by typing

> **> change lv paging normal**

and pressing the Enter key.

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 RTBCF alarm

Indication

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

Meaning

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

The CS 2000 Core Manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the CS 2000 Core Manager generates the SDMB675 log report. Refer to the log reports for more information about the condition causing the alarm.

Impact

RTB moves to the SysB state and stops transferring open files.

Action

You can refer to log report SDMB675 for more information about the RTBCF alarm. Also, you can contact your next level of support.

Clearing 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 the RTB program.

Meaning

The RTBER alarm indicates that the restart count has been exceeded.

The CS 2000 Core Manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the CS 2000 Core Manager generates the SDMB675 log report. Refer to the log reports for more information about the condition causing the alarm.

Impact

RTB moves to the SysB state.

Action

You can refer to log report SDMB675 for more information about the RTBER alarm. Also, you can contact your next level of support.

452

Clearing an RTBFM alarm

Indication

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

Meaning

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

The CS 2000 Core Manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the CS 2000 Core Manager generates the SDMB675 log report. Refer to the log reports for more information about the condition causing the alarm.

Impact

RTB moves to the SysB state.

Note: If the SDM is utilizing RTB streams, ensure that whenever you busy (BSY) and return the SBA application to service (RTS) you must also return any RTB streams to service separately. The RTB stream will not return itself to service when the SBA application is returned to service. Use the Query command to determine whether you have RTB streams running on your SDM.

Action

You can refer to log report SDMB675 for more information about the RTBFM alarm. Also, you can contact your next level of support.

Clearing an RTBPD alarm

Indication

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

Meaning

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

The CS 2000 Core Manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the CS 2000 Core Manager generates the SDMB675 log report. Refer to the log reports for more information about the condition causing the alarm.

Impact

RTB moves to the SysB state.

Action

You can refer to log report SDMB675 for more information about the RTBFM alarm. Also, you can contact your next level of support.

Clearing an RTBST alarm

Indication

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

Meaning

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

The CS 2000 Core Manager generates the SDMB375 log report when this alarm is raised. When this alarm is cleared, the CS 2000 Core Manager generates the SDMB675 log report. Refer to the log reports for more information about the condition causing the alarm.

Impact

RTB moves to the SysB state.

Action

You can refer to log report SDMB675 for more information about the RTBST alarm. You need to verify that the protocol is set to "RFTPW" and the file format type is set to "DIRP" in the schedule tuple associated with the alarm. Also, you can contact your next level of support.

Clearing a major SBACP alarm

Indication

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

Meaning

The SBA is shutting down because a user either busied the SBA or the CS 2000 Core Manager, or a process keeps dying and the SBA shut down.

Impact

The SBA is out of service.

Action

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

At the MAP

1   Access the APPL SDM Menu level by typing

> **> mapci;mtc;appl;sdm**

and pressing the Enter key.

2   Use the following table to determine your next step.

If the CS 2000 Core Manager is	Do
Offl or SysB	step 3
ManB	step 4
InSv or ISTb	step 6

3   Busy the CS 2000 Core Manager by typing

> **> bsy**

and pressing the Enter key.

4   Return the CS 2000 Core Manager to service by typing

> **> rts**

and pressing the Enter key.

> ***Note 1:*** Returning the CS 2000 Core Manager to service establishes communication between the Communication

Server 2000 core and the CS 2000 Core Manager. If the first attempt fails to return the CS 2000 Core Manager to service, the system re-attempts to establish communication until it is successful.

Note 2: The SDM Billing Application (SBA) and any streams configured for real-time billing (RTB) are also returned to service when the CS 2000 Core Manager is returned to service. Log report SDMB375 is generated when a stream configured for RTB fails to return to service.

If the CS 2000 Core Manager	Do
returned to service successfully	step 5
did not return to service successfully	contact your next level of support

At the CS 2000 Core Manager

5 Access the Appl level by typing

> **appl**

and pressing the Enter key.

6 Use the following table to determine your next step.

If the SBA application is	Do
ISTB, Offl, or SysB	step 7
ManB	step 8
InSv, and the alarm is no longer present	step 9
InSv, but the alarm is still present	contact your next level of support

7 Busy the SBA application by typing

> **bsy <x>**

and pressing the Enter key.

Where

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

8 Return the SBA application to service by typing

> **> rts \<x>**

Where

\<x> 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	step 9
did not return to service successfully	contact your next level of support

9 Use the following table to determine your next step.

If the system	Do
generates log SDMB375	step 10
does not generate log SDM375	you have completed this procedure

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

a Exit the maintenance interface by typing

> **> quit all**

and pressing the Enter key.

b Access the billing maintenance level by typing

> **# billmtc**

and pressing the Enter key.

c Access the schedule level by typing

> **> schedule**

and pressing the Enter key.

d Access the real-time billing level by typing

> `> rtb`

and pressing the Enter key.

e Busy the stream by typing

> `> bsy <stream name>`

and pressing the Enter key.

Where:

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

f Return the stream to service by typing

> `> rts <stream name>`

and pressing the Enter key.

Where:

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

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

Clearing a minor SBACP alarm

Indication

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

Meaning

The SBA program is shutting down because one of the processes is failed three times in 1 minute.

Impact

The SBA program ends but restarts within 2 minutes.

Action

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

SBACP (minor) alarm clearing flowchart
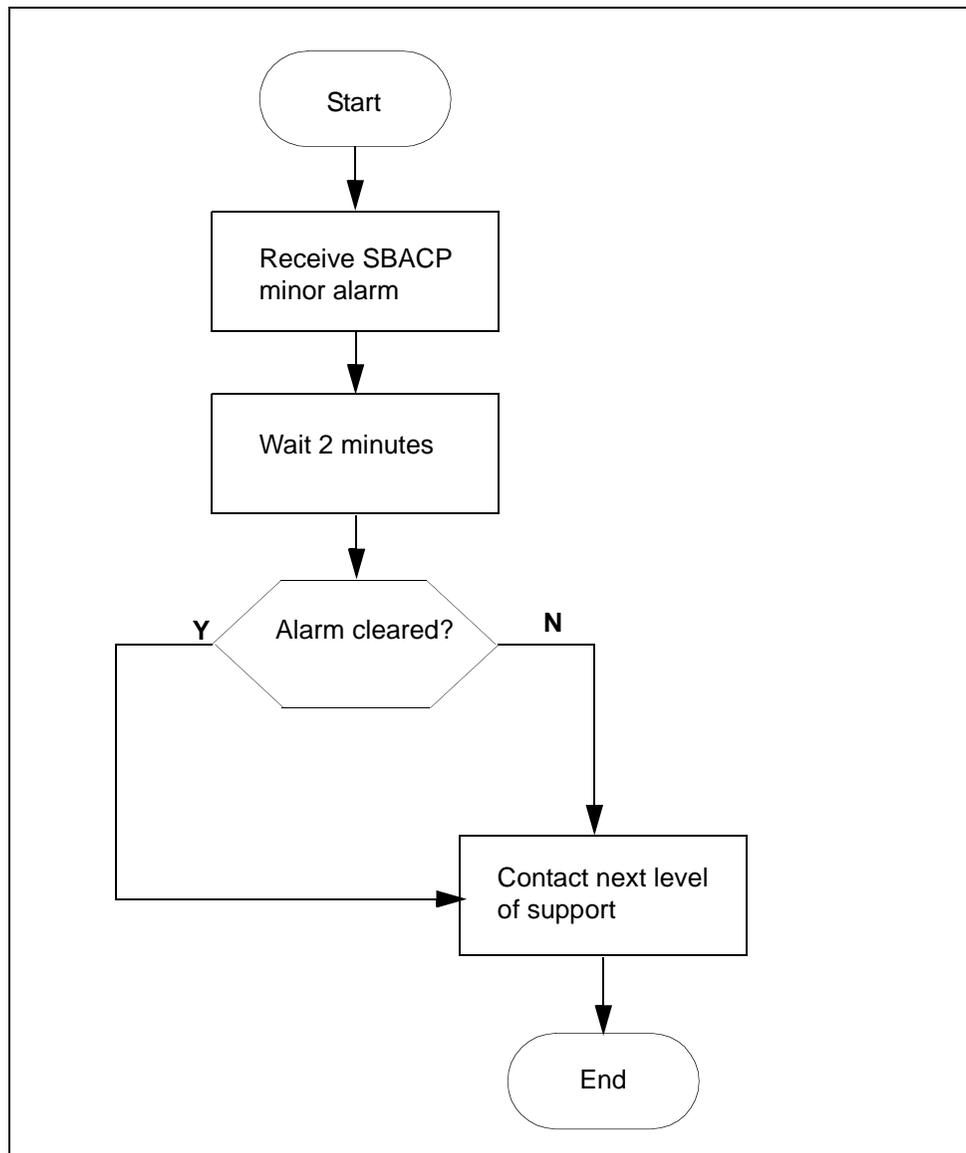
Clearing a minor SBACP alarm

At the MAP

1 Wait 2 minutes for the SBA to restart

2 If the alarm does not clear, or the SBA application fails three times within one minute, contact your next level of support.

3 You have completed the procedure.

Clearing an 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 for the file server.

Meaning

The connection to the file server is lost.

Impact

This problem can be temporary. If the alarm does not clear, the CS 2000 Core Manager is not able to FTP files to the downstream destination and must use CS 2000 Core Manager storage. As the storage becomes full, alarms notify you how of much of its capacity is used.

If CS 2000 Core Manager storage becomes full, the DMS/CM is unable to send billing records to the CS 2000 Core Manager, does send the billing records to backup storage. As the backup storage becomes full, alarms notify you of how much of its capacity is used.

Action

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

SBAIF alarm clearing flowchart
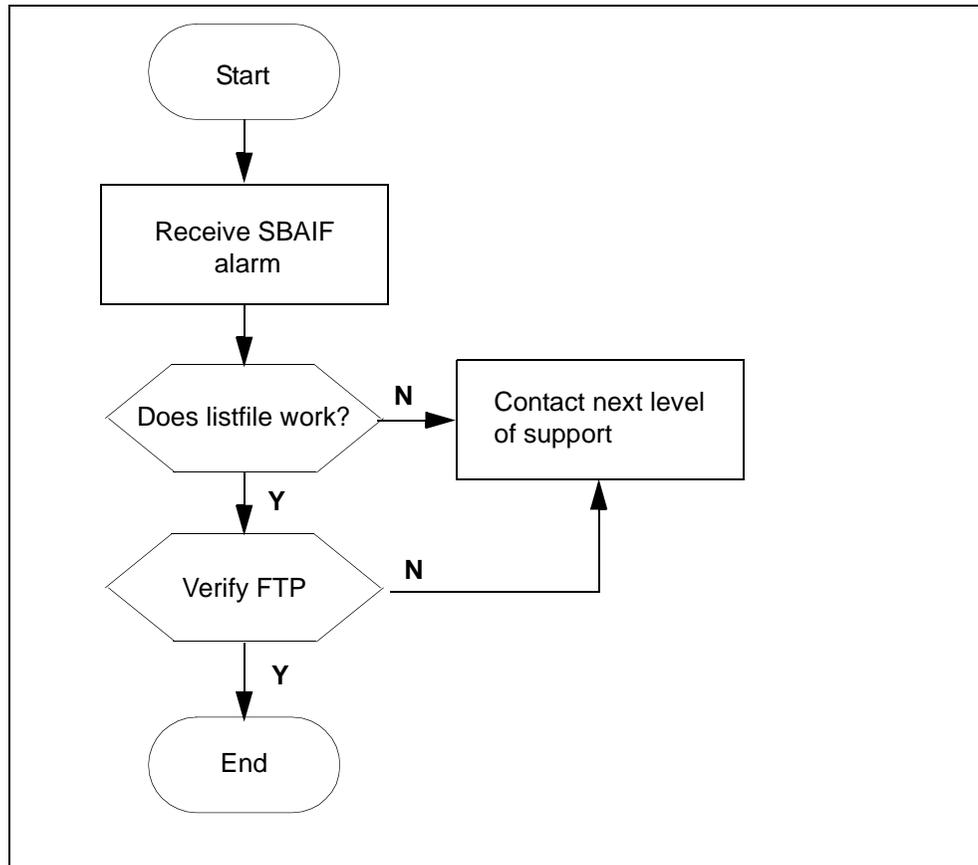
Clearing an SBAIF alarm

At the CS 2000 Core Manager

1 Access the bill maintenance level by typing

 # billmtc

and pressing the Enter key.

2 Access the file system by typing

> filesys

and pressing the Enter key.

3   List the primary file (closedNotSent directory) by typing

    > listfile <x>

and pressing the Enter key.

Where

<x> is the name of the stream.

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

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

If the "listfile" command	Do
returns a filename	refer to procedure Verifying the file transfer protocol in the Fault Management section
does not return a filename	contact your next level of support

5   You have completed this procedure.

Clearing an SDM CONFIG 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

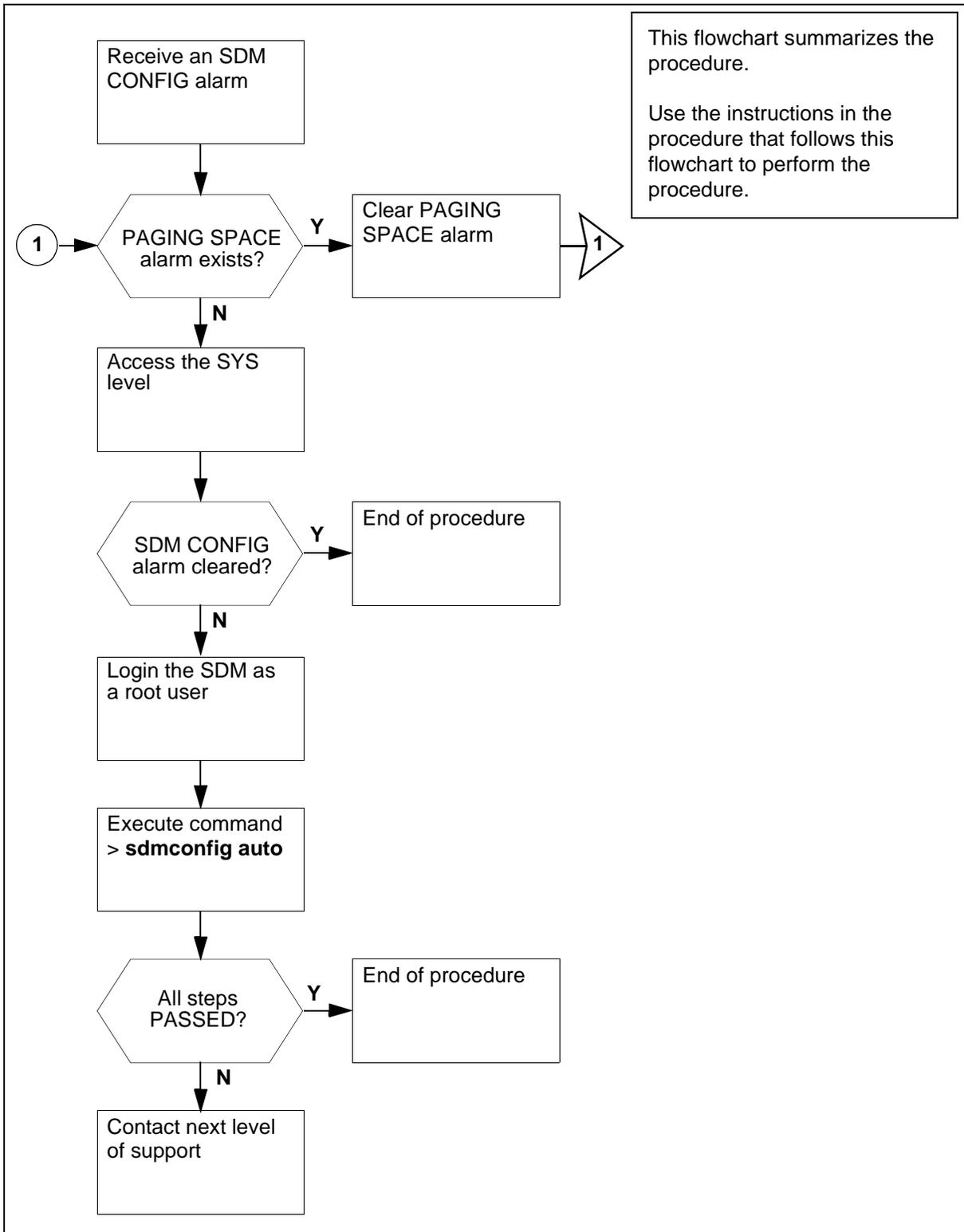A problem exists related to the SDM automatic commissioning.

Impact

The problem with the commissioning can prevent the completion of a fresh installation or upgrade.

Action

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

SDM CONFIG alarm clearing flowchart

```
        ┌─────────────────┐
        │ Receive an SDM  │                              ┌──────────────────────────┐
        │ CONFIG alarm    │                              │ This flowchart summarizes │
        │                 │                              │ the procedure.            │
        └────────┬────────┘                              │                          │
                 │                                       │ Use the instructions in  │
                 ▼                                       │ the procedure that        │
       ╱─────────────────╲    Y   ┌──────────────┐       │ follows this flowchart to │
  1 ──▶│ PAGING SPACE    │───────▶│ Clear PAGING │──▶ 1  │ perform the procedure.    │
       │ alarm exists?   │        │ SPACE alarm  │       └──────────────────────────┘
       ╲─────────────────╱        └──────────────┘
                 │ N
                 ▼
        ┌─────────────────┐
        │ Access the SYS  │
        │ level           │
        │                 │
        └────────┬────────┘
                 │
                 ▼
       ╱─────────────────╲    Y   ┌──────────────────┐
       │ SDM CONFIG      │───────▶│ End of procedure │
       │ alarm cleared?  │        │                  │
       ╲─────────────────╱        └──────────────────┘
                 │ N
                 ▼
        ┌─────────────────┐
        │ Login the SDM as│
        │ a root user     │
        │                 │
        └────────┬────────┘
                 │
                 ▼
        ┌─────────────────┐
        │ Execute command │
        │ > sdmconfig auto│
        │                 │
        └────────┬────────┘
                 │
                 ▼
       ╱─────────────────╲    Y   ┌──────────────────┐
       │ All steps       │───────▶│ End of procedure │
       │ PASSED?         │        │                  │
       ╲─────────────────╱        └──────────────────┘
                 │ N
                 ▼
        ┌─────────────────┐
        │ Contact next    │
        │ level of support│
        │                 │
        └─────────────────┘
```

Clearing an SDM CONFIG alarm

At the maintenance interface

1 Access the storage level by typing

> **sdmmtc storage**

and pressing the Enter key.

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 by typing

> **sys**

and pressing the Enter key.

If the SDM CONFIG alarm is	Do
not cleared	step 3
cleared	step 6

3 Log into the SDM as a root user by typing

> **telnet <host_name_of_the_SDM>**

and pressing the Enter key.

4 Execute the command by typing

 # sdmconfig auto

and pressing the Enter key.

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.

472

Clearing a backup Required alarm

Indication

At the SYS level of the maintenance interface on the CS 2000 Core Manager, the Backup Status indicates "Required". 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 (that is, changes at the Config level of the maintenance interface)
- a fresh install occurs
- platform configuration changes are made

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 ensures that you perform regular backups in the event that system recovery becomes necessary.

Action

Perform a system image backup (S-tape) using procedure *"Creating system image backup tapes (S-tapes)"* in the Security and Administration section, 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 by typing

> **> sys**

and pressing the Enter key.

Note: If you are at the AIX prompt (#), access the System level by typing

 # sdmmtc sys

and pressing the Enter key.

2 Clear the Backup Required alarm by typing

> **> backup clear**

and pressing the Enter key.

3 When prompted, confirm you want to clear the alarm by typing

> **> y**

and pressing the Enter key.

4 You have completed this procedure.

Verifying the FTP Schedule

You can use this procedure to verify that the schedule is set up correctly and can transfer files using FTP. The following flowchart summarizes the steps in the procedure.

Verifying the FTP schedule flowchart
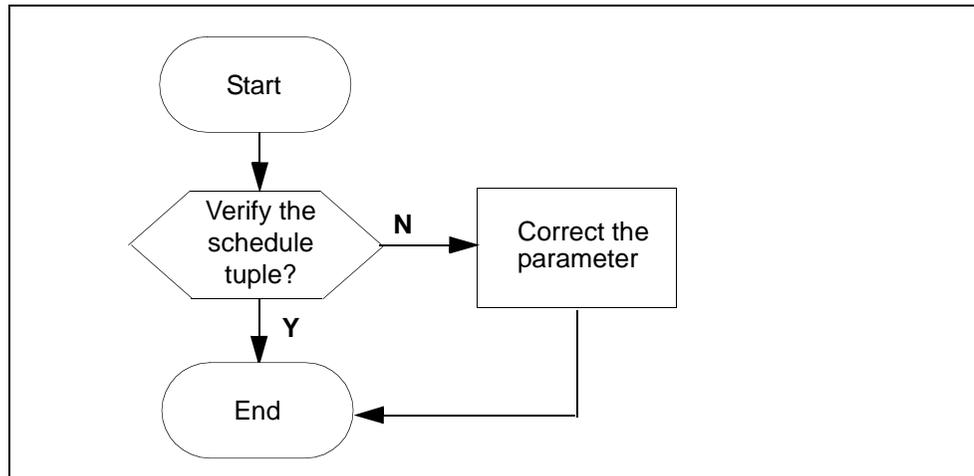
Verifying the FTP schedule

At any workstation or console

1   Log in to the CS 2000 Core Manager.

2   Access the bill maintenance level by typing

      # billmtc

      and pressing the Enter key.

3   Verify the schedule tuple by typing

      > schedule

      and pressing the Enter key.

4   List the parameters of the schedule tuple by typing

      > list

      and pressing the Enter key.

5 Use the following table to determine your next step.

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

6 Reset the schedule tuple parameters by typing

> **change**

and pressing the Enter key.

7 Enter the stream name (billing file name), and press the Enter key.

8 Enter the file format, and press the Enter key.

9 Enter the destination name, and press the Enter key.

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

10 Observe the schedule tuple displayed.

11 Enter the parameters that you need to correct, and press the Enter key.

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

12 Enter the new values of the parameters you have chosen to change, and press the Enter key after each parameter.

13 Save the changed parameters by typing

> **save**

and pressing the Enter key.

14 Use the following table to determine your next step.

If the parameters are	Do
correct, or if you have corrected the parameters, but are still receiving an alarm	contact your next level of support
correct and you are no longer receiving an alarm	step 15

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

16 You have completed the procedure.

Verifying the file transfer protocol

You can use this procedure on the CS 2000 Core Manager to verify that the file transfer protocol (FTP) is set up correctly to transfer files. The following flowchart summarizes the steps outlined in the procedure.

FTP verification flowchart
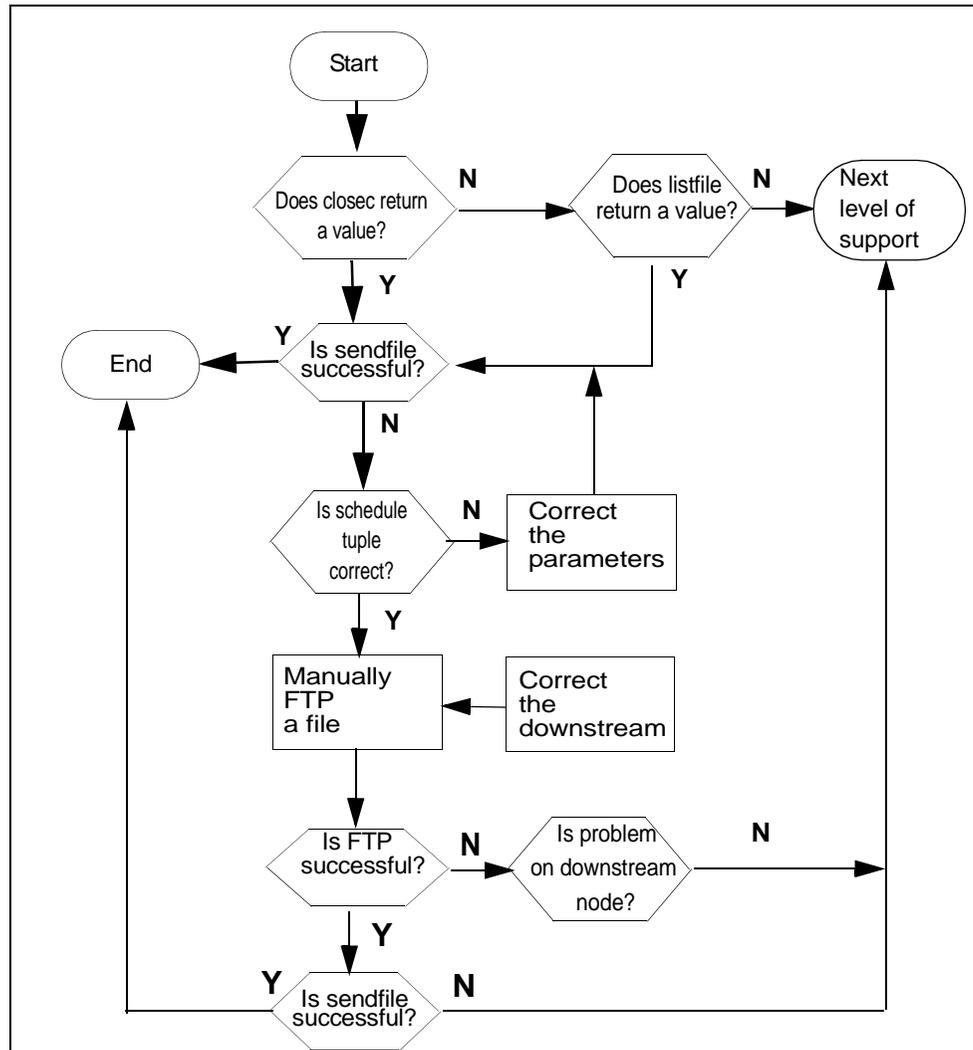
Verify the FTP

At the CS 2000 Core Manager

1 Access the bill maintenance level by typing

 # billmtc

and pressing the Enter key.

2   Access the file system by typing

> **filesys**

and pressing the Enter key.

3   Close active billing files by typing

> **closec <x>**

and pressing the Enter key.

Where

<x> is the name of the stream.

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

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

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

5   List the primary file (closedNotSent directory) by typing

> **listfile <x>**

and pressing the Enter key.

Where

<x> is the name of the stream.

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

6   Send the primary file (closedNotSent directory) by typing

> **sendfile <x>**

and pressing the Enter key.

Where

<x> is the name of the stream.

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

7   Go to the previous level of the CS 2000 Core Manager by typing

> **quit**

and pressing the Enter key.

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

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

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

9   Access the schedule level by typing

> **schedule**

and pressing the Enter key.

10   List the parameters of the schedule tuple by typing

> **list**

and pressing the Enter key.

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

If the parameters are	Do
correct, but you are receiving an alarm	step 22
incorrect	step 12

12   Reset the schedule tuple parameters by typing

> **change**

and pressing the Enter key.

13   Enter the stream name (name of billing file) and press the Enter key.

14   Enter the file format, and press the Enter key.

15   Enter the destination name, and press the Enter key.

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

16   Observe the schedule tuple displayed.

17   Enter the parameters you want to correct by typing

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

18 Enter the new values of the parameters you have chosen to change, and press the Enter key after each parameter.

19 Save the changed parameters by typing

> `save`

and pressing the Enter key.

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

If you have	Do
corrected the parameters in the schedule tuple	step 6
determined that the parameters are correct	step 21 (verifies that the login and write permissions are correct for the FTP process without testing an actual billing file)
determined that the parameters are correct	step 24 (verifies that the login and write permissions are correct for the FTP process while testing an actual billing file)

21 Exit the maintenance interface by typing

> `quit all`

and pressing the Enter key.

22 Login as root user.

23 Attempt to FTP any billing file to the destination used by the "sendfile" command to verify that FTP is properly functioning for that node and directory.

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

24 Exit back to the command prompt by typing

> `quit all`

and pressing the Enter key.

25 Login as root user.

26 Copy a billing file from the closedNotSent directory to a temporary directory by typing

`# cp /<x>/closedNotSent/<y> /tmp`

and pressing the Enter key.

Where

<x> is the logical volume for the stream that is in use and <y> 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. The format is **>/sba/<streamname>**.

27 Access the /tmp directory by typing

`# cd /tmp`

and pressing the Enter key.

28 FTP to the downstream node by typing

`> ftp <x> <y>`

and pressing the Enter key.

Where

<x> is the Primary_Destination IP address of the destination node and <y> is the Primary_Port of the destination node.

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

> *Note:* A successful login is confirmed by a "230 User <x> 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.

30 Change the directory to the one the schedule tuple is using by typing

`ftp> cd <x>`

and pressing the Enter key.

Where

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

> *Note:* A successful login is confirmed by a "250 CWD command successful" message returned by the FTP. If the "cd" command is unsuccessful, obtain a valid directory from the downstream node and update the schedule tuple with the valid values.

31 Set the file transfer mode to binary by typing

`ftp> binary`

and pressing the Enter key.

> *Note:* A successful command is confirmed by a "200 Type set to l" message returned by the FTP.

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

`ftp> put <y>`

and pressing the Enter key.

Where

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

33 Exit from the FTP session by typing

`ftp> quit`

and pressing the Enter key.

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

If the file transfer is	Do
successful	step 37
unsuccessful because of a permission error	step 35
unsuccessful for a reason other than permission error	step 38

35 Correct the directory permissions to allow write access.

36 Repeat steps 22 through 33.

37 Send the primary files in the closedNotSent directory by typing

`> sendfile <x> dest <y>`

and pressing the Enter key.

Where

<x> is the name of the billing stream and <y> 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.

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

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