Carrier VoIP

CS2000 Core Manager Configuration Management

NN10104-511

Document status: Standard
Document version: 08.04
Document date: 20 October 2006

Contents

CS 2000 Core Manager Configuration Management

Configuration management strategy

The Carrier Voice over IP network configuration management strategy is to provide solutions on a pre-configured basis. All components within these pre-defined configurations and components not included can be ordered separately.

Customer documentation provides information on installation, configuration, and upgrades for base functionality and software applications that run on the CS 2000 Core Manager.

Tools and utilities

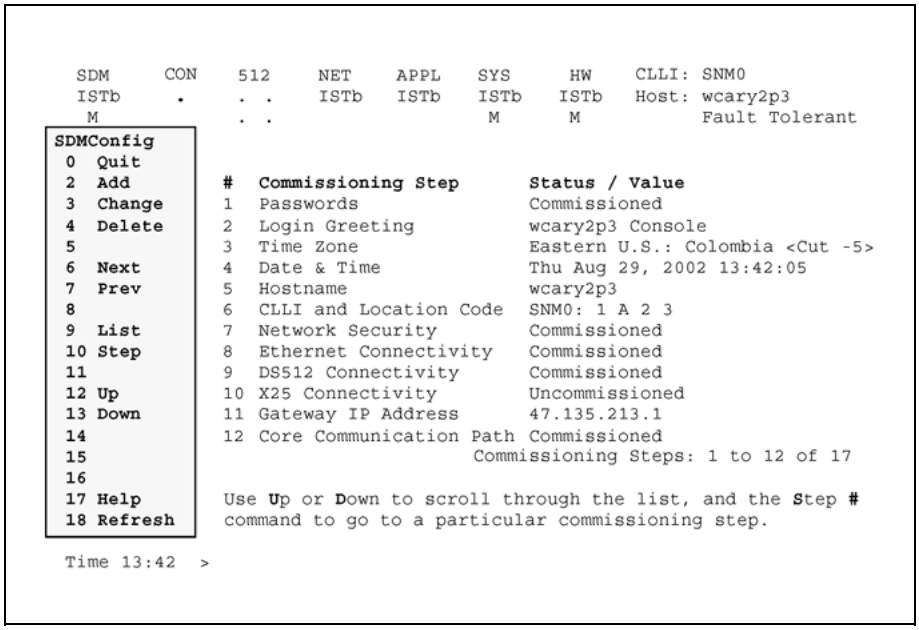
Preside Management for Succession Solutions (Preside MSS) includes the CS 2000 Core Manager and Multi-Service Data Manager (MDM) that together share all network fault, configuration, accounting, performance, and security (FCAPS) tasks. The CS 2000 Core Manager is responsible for FCAPS tasks related to Communication Server 2000, SPM, IW-SPM, and the media gateway suite (MG).

The SDMConfig level provides commands for commissioning the CS 2000 Core Manager. The SWIM level of the CS 2000 Core Manager interface contains commands for listing available filesets and executing software configuration programs.

Commissioning tool

The commissioning tool at the SDMConfig level is used to commission or recommission the components of the CS 2000 Core Manager. To use the tool, you must log on to the CS 2000 Core Manager as a root user, and enter the **SDMCONFIG** command. The system displays the SDMConfig level and the commissioning status of the components of the CS 2000 Core Manager. The following figure shows an SDMConfig level display.

SDMConfig level display



Note: This figure shows an *example* of a screen display at the SDMConfig level. The numbers assigned to the components in the list of commissioning steps can vary by release.

The following table lists command options for the commissioning steps.

Command options for the commissioning steps

If you want to	Enter
Scroll backward through the list of commissioning steps	**u** (up)
Scroll forward through the list of commissioning steps	**d** (down)
Select a component to commission	**step <n>** where **<n>** is the number of the commissioning step assigned to the component that you want to commission ***Note:*** The numbers assigned to components in the list of commissioning steps can vary by release.

After you select a component to commission, the system displays the SDMConfig screen for that component. Use the command options in the following table to commission the component.

Note: The commands in the table are for general reference. When commissioning a component or components of the CS 2000 Core Manager, use the specific procedures listed in the table "Commissioning procedures" (page 7).

Command options for commissioning a component

If you want to	Enter
Change a value for a component	**`c`** (change)
Accept the default value for a component	Press the Enter key
Confirm a change	**`y`** (yes)
Reject or abort a change	**`n`** (no), *or* **`abort`** ***Note:*** The **`abort`** command can be used at any time during the procedure.
Edit a change	**`e`** (edit)
Continue with (select) the next commissioning step	**`n`** (next)
Return (go back) to the previous screen	**`p`** (previous)
Display the list of available commissioning steps	**`l`** (list), or **`9`** *or* **`q`** (quit), or **`0`**
Quit the commissioning program	**`quit all`**

Configuration management procedures

For configuration management procedures, refer to the modules for specific CS 2000 Core Manager components.

Commissioning procedures

The following table lists the names and locations of the procedures that use the commissioning tool.

Commissioning procedures

Component	Procedure	Document
Date & Time	"Changing the system date or time"	Security and Administration

Component	Procedure	Document
DCE	• "Adding a NULL or an NTP time provider on a DCE server" • "Configuring a CS 2000 Core Manager in a DCE cell" • "Removing a CS 2000 Core Manager from a DCE cell"	Configuration Management
Edge Nodes	• "Commissioning or decommissioning edge node monitoring" • "Adding or removing edge nodes, or configuring edge node monitoring parameters"	Configuration Management
Network Time Protocol	"Commissioning or decommissioning Network Time Protocol"	Configuration Management
Passthru Users	"Adding or removing Passthru users"	Security and Administration
Password	"Changing a user password"	Security and Administration
Time Zone	"Changing the system time zone and daylight savings time parameters	Security and Administration
Add/remove maint users	"Adding or removing Maint users"	Security and Administration
X25 Connectivity	"Commissioning or recommissioning X.25 connectivity" "Decommissioning X.25 ports [on UMFIO or SYNC module]"	Upgrades Configuration Management

Installing and configuring the log delivery application

The following procedure outlines the steps that must be performed to install and configure the log delivery application on the CS 2000 Core Manager.

For full operation, the log delivery application requires installation of the following application filesets:

- Log delivery service
- Log delivery service client
- Generic data delivery
- Passport Log Streamer (only required for offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data)

  Note: The Passport Log Streamer application fileset requires the pserver application to be installed on the Preside MDM server. Ensure the pserver application is installed and configured on the Preside MDM server prior to upgrading the CS 2000 Core Manager. Refer to the Preside MDM information for instructions on how to install and configure the pserver application.

Prerequisites

ATTENTION

Do not install this application if you are using the Customer Network Manager (CNM) or duplicate logs appear at the CNM. The CNM handles all log streaming directly from each PM.

Prior to performing this procedure, ensure that there are no disk faults on the CS 2000 Core Manager.

Ensure that the Multiservice Data Manager (MDM) has all required cartridges installed.

Ensure that the cartridge version installed on the MDM and the MDM software version are compatible. See the compatibility list at http://www130.nortelneworks.com/cgi-bin/eserv/cs/main.jsp.

In order to ensure that the Passport Log Streamer is able to communicate with the configured MDMs and to collect logs, any restrictions for the configured MDM ports should be removed from all of the firewalls that exist between the MDM and the core manager.

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

Procedure

Installing and configuring the log delivery application

Step	Action

At the core manager

1 Use the following table to determine your first step.

If you are installing and configuring the Log delivery application for	Do
a PT-AAL1 or UA-AAL1 office	step 2
any other office	step 4

2 Obtain the IP address for each of the two nodes that constitute the Preside MDM.

3 Obtain the port number for the pserver application on each of the Preside MDM nodes.

Note: The port numbers are those the Passport Log Streamer application on the CS 2000 Core Manager will connect to.

4 Begin to install the Log Delivery application: log into the core manager using the maint user ID and password.

5 Switch user to root using the root ID and password.

6 Use the following table to determine your next step.

If the filesets are	Do
on CD or DVD	insert the disk and continue with step 7
in a directory	retrieve the filesets from the directory, and continue with step 8

7 Access the Apply level of the SDMCS 2000 Core Manager maintenance interface and display the list of filesets contained in the source location (tape or directory):

```
sdmmtc apply <x>
```

where

<x> is either the number that corresponds to the tape drive (0 if tape is in slot 2, or 1 if tape is in slot 13), or the path of the source directory

8 Select the filesets required for the Log delivery application:

```
select <fileset_number>
```

where

fileset_number is the number next to each of the following filesets:

- Log Delivery Service
- Log Delivery Service Client
- Generic Data Delivery
- Passport Log Streamer (only required for offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data)

9 Install the filesets:

```
apply
```

10 Confirm the apply command:

```
y
```

Note: The Generic Data Delivery application is automatically brought into service.

If you	Do
installed the Passport Log Streamer fileset	step 11
did not install the Passport Log Streamer fileset	step 12

11 Configure the Passport Log Streamer application as follows:

Note: If you previously had the log delivery service application fileset installed and configured, the values will default to those already defined. You can accept the default value by pressing the Enter key.

a. Access the Config level and display the list of applications:

```
config
```

b. Start the configuration process:

config <x>

where

<x> is the number next to the Passport Log Streamer application

c. When prompted, enter the IP address for the first Preside MDM node, then the second.

Examples

```
Enter the IP address for the first
MDM[000.000.000.000]:47.135.209.70
Enter the IP address for the
second MDM[000.000.000.000]:47.135.209.124
```

d. When prompted, enter the port number configured for the pserver application on the first Preside MDM node, then the second.

Examples

```
Enter the port number for the first
MDM[3197]:
Enter the port number for the second
MDM[3197]:
```

Note: If MDM filters were previously defined, they will be displayed.

e. When prompted, indicate whether you want to receive MDM filters.

Example response

```
No previous Preside MDM filters defined.
Do you want to specify Preside MDM filters?  [y/n]
```

If	Do
y (yes)	substep f
n (no)	substep g

f. When prompted, enter the host name of the first Preside MDM node, then the second.

Example response

```
Enter MDM hostname 1:  PGMDM00
Enter MDM hostname 2:  PGMDM01
```

g. When prompted, indicate whether you want to receive Passport 15000 filters.

Example response

```
No previous Passport 15000 filters defined.  Do you
want to specify Passport 15000 filters [y/n]
```

Note: If Passport 15000 filters were previously defined, they will be displayed.

If	Do
y (yes)	substep h
n (no)	substep m

h. When prompted, type the number of Passport 15000 filters you want to specify.

Example response

```
How many Passport 15000 filters do you wish to
specify?  [4]:
```

Note: Specify one filter per Passport 15000 to receive logs from.

i. When prompted, enter the required set of Passport 15000 module names (a typical module name is often defined to be the network element's CLLI). Logs will then be received only from the modules that are specified.

j. When prompted, indicate whether you want to receive Passport 8600 filters.

Example response

```
No previous Passport 8600 filters defined.
Do you want to specify Passport 8600 filters?  [y/n]
```

Note: If Passport 8600 filters were previously defined, they will be displayed.

If	Do
y (yes)	substep k
n (no)	substep m

k. When prompted, type the number of filters you want to specify.

l. When prompted, enter the required set of Passport 8600 module names (a typical module name is often defined to be the network element's CLLI). Logs will then be received only from the modules that are specified.

m. When prompted, confirm the configuration data you entered:

y

Response

```
Saving new configuration data...
```

ATTENTION

If you installed and configured the Passport Log Streamer application fileset, ensure the Preside MDM is installed, configured, and in service before continuing with this procedure.

12 Begin to bring the Log delivery service application and the Passport Log Streamer application into service. Access the Application (Appl) level:

```
appl
```

a. Busy the application filesetfilesets:

```
bsy <fileset_number>
```

where

fileset_number is the number next to the following application filesetfilesets:

- Log delivery service
- Passport Log Streamer (if installed)

b. Return the application filesetfilesets to service:

```
rts <fileset_number>
```

where

fileset_number is the number next to the application filesetfilesets you busied in the previous step

Once the application fileset is returned to service, the system retrieves any current log records. To view or store log records, see the procedure "Displaying or storing log records using log receiver" in the Fault Management document.

Note: If the application fileset has been out of service for an extended period of time, the system retrieves any older log records that are available prior to any current log records.However, for Passport Log Streamer application, once it returns to service, the system retrieves only the current log records.

13 You have completed this procedure.

—End—

Configuring log delivery destinations

Purpose

Use this procedure to add an output log device. An output log device is a destination to which your system forwards user-defined streams of logs.

Application

You can add any of the following log devices using the Log Delivery Application Commissioning Tool (logroute):

- a TCP device (a host IP and port on the network)
- a TCP-IN device (a remote IP and a CS 2000 Core Manager port number)
- a file device (a file on the CS 2000 Core Manager)

You can configure up to 30 Log Delivery output devices. If you want to

- change any aspect of an existing device, including log routing entries, refer to the procedure "Modifying a log device using logroute" (page 23).
- delete an existing device, refer to the procedure "Deleting a device using logroute" (page 30).
- modify global parameters (parameters that apply to all devices), refer to the procedure "Configuring Log Delivery global parameters" (page 81).

All devices can be accessed either locally or from a remote location (console). To access the devices from a remote console, refer to the procedure "Accessing a TCP or TCP-IN log device from a remote location" in the Fault Management document.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

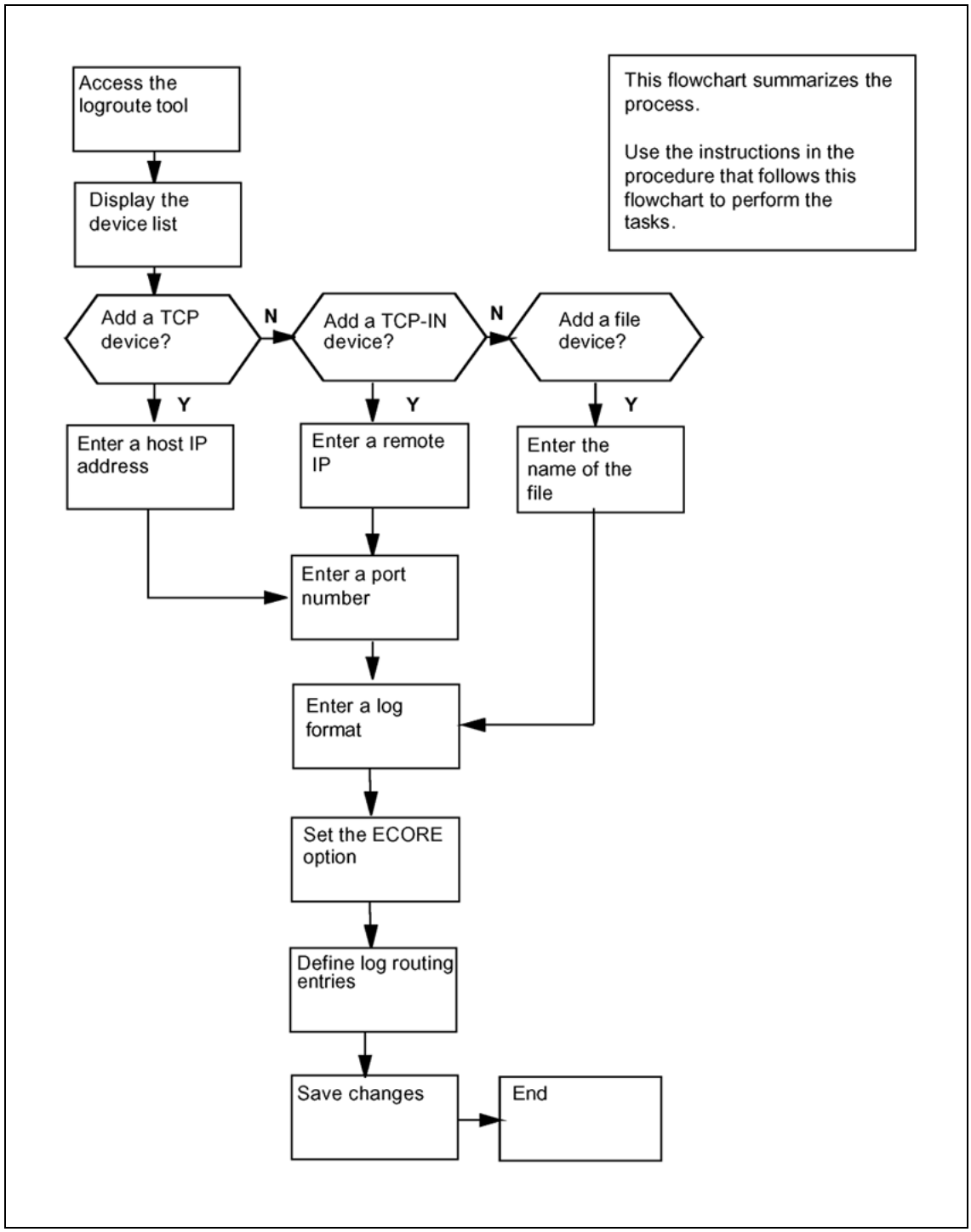
For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

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

Task flow diagram

The following task flow diagram provides a summary of the process. Use the instructions in the procedure that follows the flowchart to perform the task.

Task flow for Configuring log delivery destinations



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

Configuring log delivery destinations

Step	Action

At any workstation or console

1 Log into the CS 2000 Core Manager .

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu


            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



   Enter Option ==>
```

3 Display the device list:

```
1
```

The Device List Menu screen appears.

```
                    Device List Menu

            1 - View Device
            2 - Add Device
            3 - Delete Device
            4 - Modify Device
            5 - Help
            6 - Return to Main Menu



   Enter Option ==>
```

4 Begin to add a new log device:

2

The Add Device screen appears.

```
                      Add Device

            1 - Add TCP Device
            2 - Add TCPIN Device
            3 - Add File Device
            4 - Help
            5 - Return to Device List



   Enter Option ==>
```

5 If you want to view the devices currently configured, enter 1 and press the Enter key. Follow the on-screen instructions to display the details for the selected device.

If you want to add a	Do
TCP device	step 6
TCP-IN device	step 9
file device	step 12

6 Start adding a TCP device:

1

Example response:

```
                        TCP Device
  Enter ABORT to return to Add Device Screen

          1 - HOST IP      :
          2 - PORT         :
          3 - FORMAT       : STD
          4 - ECORE        : ON
          5 - Log Routing  :




  Enter host IP address <###.###.###.###> ==>
```

7 Enter a host IP address.

8 When prompted, enter a port number from the range displayed.

Continue with step 14.

9 Start adding a TCP-IN device:

2

Example response:

```
                      TCP-IN Device
  Enter ABORT to return to Add Device Screen

          1 - REMOTE IP      : any
          2 - PORT           :
          3 - FORMAT         : STD
          4 - ECORE          : ON
          5 - Log Routing    :




  Enter remote IP address <###.###.###.###> or a for any ==>
```

10 Enter an authorized remote IP address. Enter **a** if you want to leave the default value of `any`.

11 When prompted, enter an CS 2000 Core Manager port number.

Continue with step 14.

12 Start adding a file device:

```
3
```

Example response

```
                          File
Enter ABORT to return to Previous Screen

         1 - FILENAME     :
         2 - FORMAT       : STD
         3 - ECORE        : ON
         4 - Log Routing  :




Enter file name  ==> /data/logs/
```

13 Enter the name of the file where the logs will be stored.

14 When prompted, enter the log format (STD, STD_OLD, SCC2, or SCC2_OLD).

Enter STD or SCC2 if you want the following information to be displayed in all log reports (otherwise, enter STD_OLD or SCC2_OLD):

- user-defined office ID, same for all logs and streams
- the name of the node (ECORE) from which the log is generated
- the sequence number in dual (global and device) format

The default format is STD.

15 When prompted, set the ECORE option to ON or OFF.

Enter ON, if you want the log-generating node name to be displayed in all reports (the format must be STD or SCC2). Otherwise, enter OFF.

You are now prompted to define a log routing entry for the device that you are adding. Use the following table to determine your next step.

If you want to	Do
suppress logs (cause them not to be routed to this device)	enter **d**, and press the Enter key
un-suppress logs (cause them to be routed to this device)	enter **a**, and press the Enter key

The rules you enter here only accommodate the set of logs defined in the procedure "Specifying the logs delivered from the CM to the core manager" (page 74). Logs suppressed at the CM cannot be unsuppressed for a specific device.

Example response:

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

16 Enter a log type, or a combination of log type and log number (separated by a space). The new entry is added to the log routing list on the screen.

An example of a log type is "PM". This entry will suppress or un-suppress all PM logs.

An example of a combined log type and log number is PM 181. This entry will suppress or un-suppress the PM181 logs but leave the routing of other PM logs unchanged.

You can also enter **all**, which will suppress or un-suppress all logs routed to this device.

Example response:

```
Wish to enter more Logrouting Details?  (Y/N)[N]:
```

If you	Do
want to add more routing entries The maximum number of log routing entries is 1024. If you have 1024 entries, and you want to add another one, you must replace one of the existing entries with the new entry.	enter **y**, and return to step 15
do not want to add more routing entries	enter **n**, and go to step 17

17 You are prompted to save the device details. Save the new device:

y

The new device will be added to the system.

Example response:

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

Press the Enter key to return to the Add Device screen.

If you enter **n**, the system returns to the Device List Menu screen. No new device is added to the system.

If you	Do
want to add more devices	go to step 5
do not want to add more devices	go to step 18

18 Return to the Device List Menu screen:

```
5
```

19 Return to the Logroute Main Menu screen:

```
6
```

20 Quit the logroute tool:

```
6
```

21 You have completed this procedure.

—End—

Modifying a log device using logroute

Purpose

Use this procedure to change any parameter of an existing log device, including the routing entries that suppress or un-suppress logs delivered to that device.

The routing rules you enter for each device only accommodate the set of logs defined in the procedure "Specifying the logs delivered from the CM to the core manager" (page 74). Logs that are being suppressed at the CM cannot be un-suppressed for a specific device.

If you want to modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

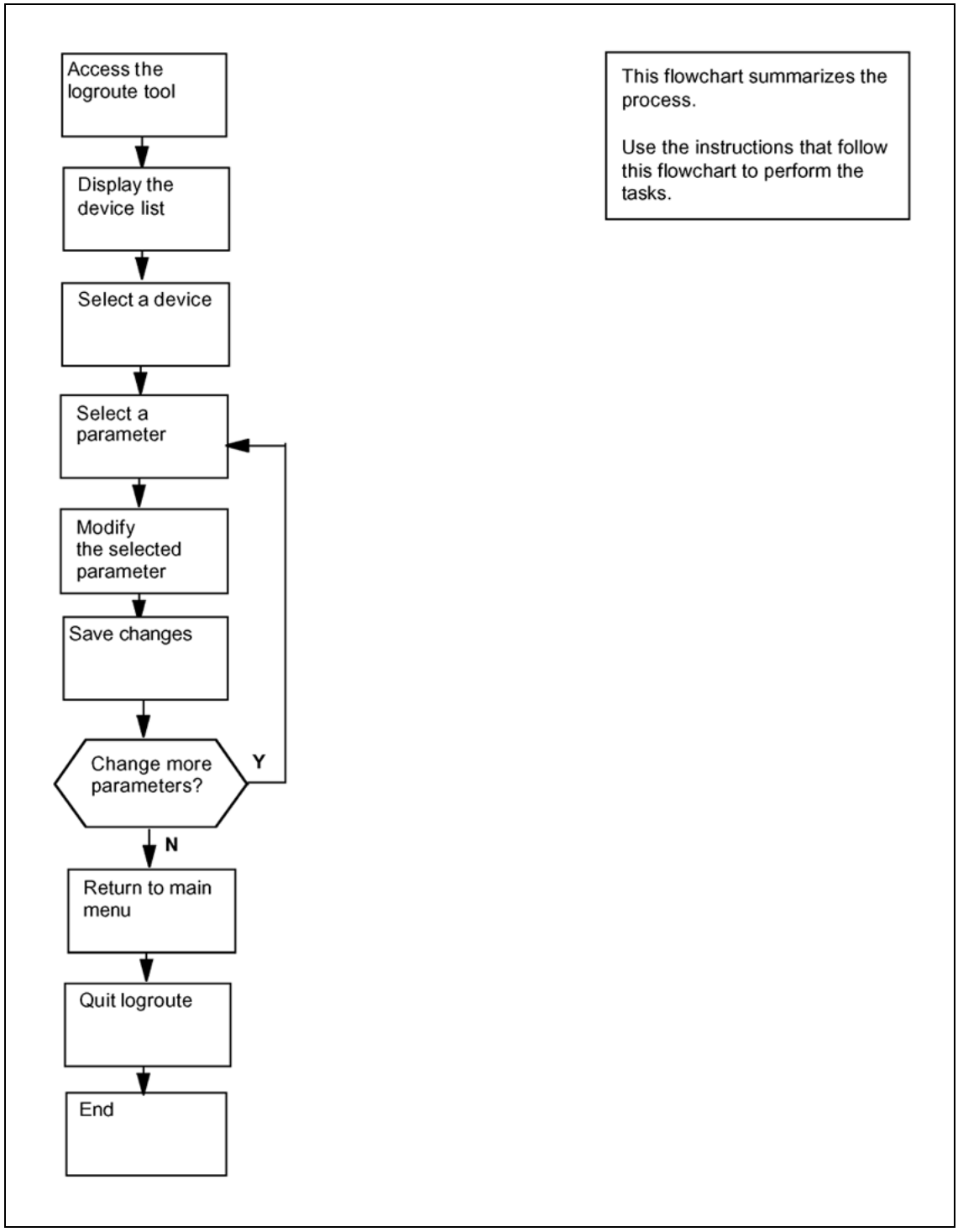
For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

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

Task flow diagram

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

Task flow for Modifying a log device using logroute



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

Procedure

Modifying a log device using logroute

Step	Action

At the VT100 console

1 Log into the core manager.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu

            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



    Enter Option ==>
```

3 Display the device list:

```
1
```

The Device List Menu screen appears.

```
                    Device List Menu

            1 - View Device
            2 - Add Device
            3 - Delete Device
            4 - Modify Device
            5 - Help
            6 - Return to Main Menu



    Enter Option ==>
```

4 Access the Modify Device Menu screen:

4

The system displays all currently configured devices.

Example response:

```
                Modify Device Menu

Enter ABORT to return to Device List Menu...
        Devices:                                    Type
        1 - /data/logs/niru1                        File
        2 - HOST: any            PORT: 8551         TCPIN
        3 - HOST: 47.135.213.86  PORT: 1027         TCP
        4 - HOST: any            PORT: 8556         TCPIN









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

5 Enter the number for the device that you want to modify.

The screen for the selected device is displayed.

Example of a TCPIN device screen (second device in the preceding example):

```
                TCP-IN Device

Enter ABORT to return to Modify Device Menu

        1 -  REMOTE IP              : any
        2 -  PORT                   : 8551
        3 -  FORMAT                 : STD
        4 -  ECORE                  : ON
        5 -  Log Routing            :
             ADDREP ALL
             ADDREP TRK 101
             ADDREP TRK 100
             ADDREP TRK 102



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

6 Enter the number for the parameter that you want to modify.

If the parameter that you selected is	Do
REMOTE IP, HOST IP, PORT, or FILENAME	step 7
FORMAT	step 8
ECORE	step 9
Log Routing	step 10

7 At the prompt, enter a new value for the selected parameter. Continue with step 16.

8 At the prompt, enter the new log format (from the range displayed).

Enter STD or SCC2 if you want the following information to be displayed in all log reports:

- user-defined office ID, same for all logs and streams
- the name of the node (ECORE) from which the log is generated
- the sequence number in dual (global and device) format

Continue with step 16.

9 At the prompt, change the setting for the ECORE option (ON or OFF).

If you enter ON, the name of the node from which the log is generated is displayed in all log reports (for STD and SCC2 formats only).

Continue with step 16.

10 The system displays all existing logrouting entries for the selected device, and prompts you to add or delete an entry. Complete the following steps to add or delete a routing entry.

If you want to	Do
add an entry	enter **a**, and continue with step 11
delete an entry	enter **d**, and continue with step 14

11 At the prompt, enter one of the following values:

- **a**

  if you want to un-suppress logs (cause them to be routed to the device)

- **d**

  if you want to suppress logs (cause them not to be routed to the device)

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 (separated by a space). The new entry is added to the log routing list on the screen. For example, an entry of:

- PM will suppress or un-suppress all PM logs. An entry of
- PM 100 will suppress or un-suppress the PM100 logs, but leave the routing of other PM logs unchanged.

Example response:

```
Wish to enter more Logrouting Details (Y/N) [N]:
```

13 If you want to suppress or un-suppress more logs, enter y, and go back to step 11. Otherwise, enter n, and continue with step 16.

14 Enter the number of the entry that you want to delete from the log routing list. The entry you specified is removed from the display.

Example response:

```
Wish to delete more Logrouting Details (Y/N) [N]:
```

15 If you want to delete more entries, enter **y**, and repeat step 14.

If you do not want to delete any more entries, enter n, and continue with step 16.

16 When prompted, save your changes:

y

Example response:

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

17 Confirm the save command:

y

Example response:

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

Press the Enter key to confirm the change.

If you do not want to save your change, enter n and press the Enter key.

If you	Do
want to make more changes for the selected device	step 6
do not want to make more changes for the selected device	step 18

18 Type **abort** and press the Enter key. The system returns to the Modify Device Menu screen.

19 If you want to modify another device, go back to step 5. Otherwise, continue with step 20.

20 Exit the Modify Device Menu screen:

```
abort
```

21 Return to the Logroute Main Menu screen:

```
6
```

22 Quit the logroute tool:

```
6
```

23 You have completed this procedure.

—End—

Deleting a device using logroute

Purpose

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 core manager)
- a file device (a file on the core manager)

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

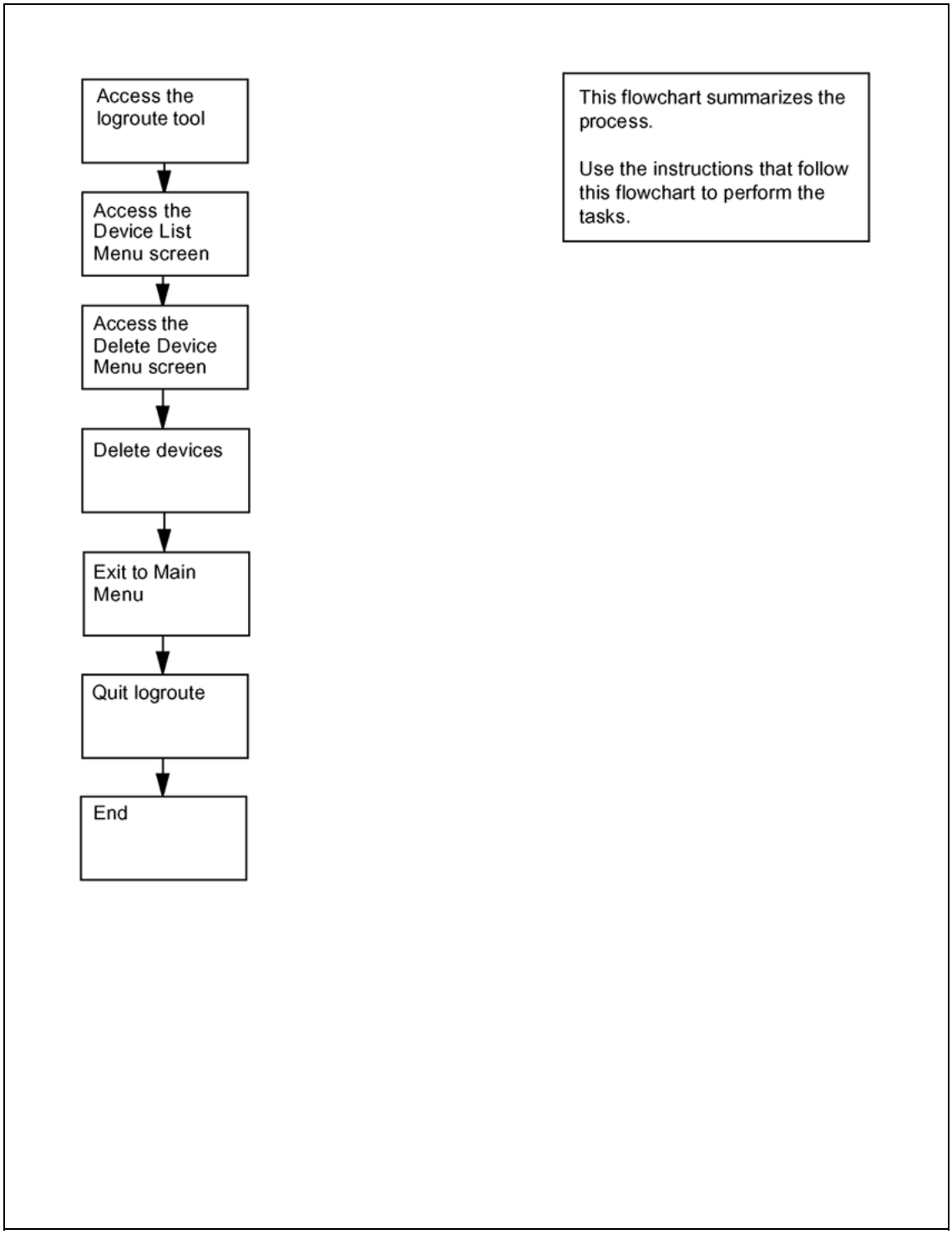
For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

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

Task flow diagram

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

Task flow for Deleting a device using logroute



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

Procedure

Deleting a device using logroute

Step	Action

At the VT100 console

1 Log into the core manager.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

3 Display the device list:

```
1
```

The Device List Menu screen appears.

```
                    Device List Menu

            1 - View Device
            2 - Add Device
            3 - Delete Device
            4 - Modify Device
            5 - Help
            6 - Return to Main Menu



    Enter Option ==>
```

If you want to view the devices currently configured, enter 1. Follow the on-screen instructions to display the details for the selected device.

4 Access the Delete Device Menu screen:

```
3
```

The system displays the list of configured devices and prompts you to enter the number of the device that you want to delete.

Example response:

```
                    Delete Device Menu
Enter ABORT to return to Device List Menu
          Devices:                                    Type:
          1 - HOST: any              PORT: 8551       TCPIN
          2 - HOST: 10.102.4.4       PORT: 14450      TCP
          3 - /data/logs/faults                       FILE




 Enter device number to delete ==>
```

5 Enter the number of the device you want to delete.

Response

```
Device will be deleted permanently.  Continue...
(Y/N)[N]:
```

6 Confirm that you want to delete the selected device:

y

Example response:

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

If you do not want to delete the selected device, enter **n**, press the Enter key, and select a new device to delete.

7 Press the Enter key to confirm that you want to continue.

The device is removed from the list and you are prompted to enter the next device to be deleted.

8 Use the following table to determine your next step.

If you	Do
want to delete another device	step 5
do not want to delete another device	step 9

9 Return to the Device List Menu screen:

abort

10 Return to the Logroute Main Menu screen:

6

11 Quit the logroute tool:

6

12 You have completed this procedure.

—End—

Configuring log delivery for MDM/PPEM security and audit logs (MDM 601 and PPEM 601)

Purpose

Use this procedure to set up a log device that contains only the security and audit logs that are sent to the core manager's syslog system.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

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

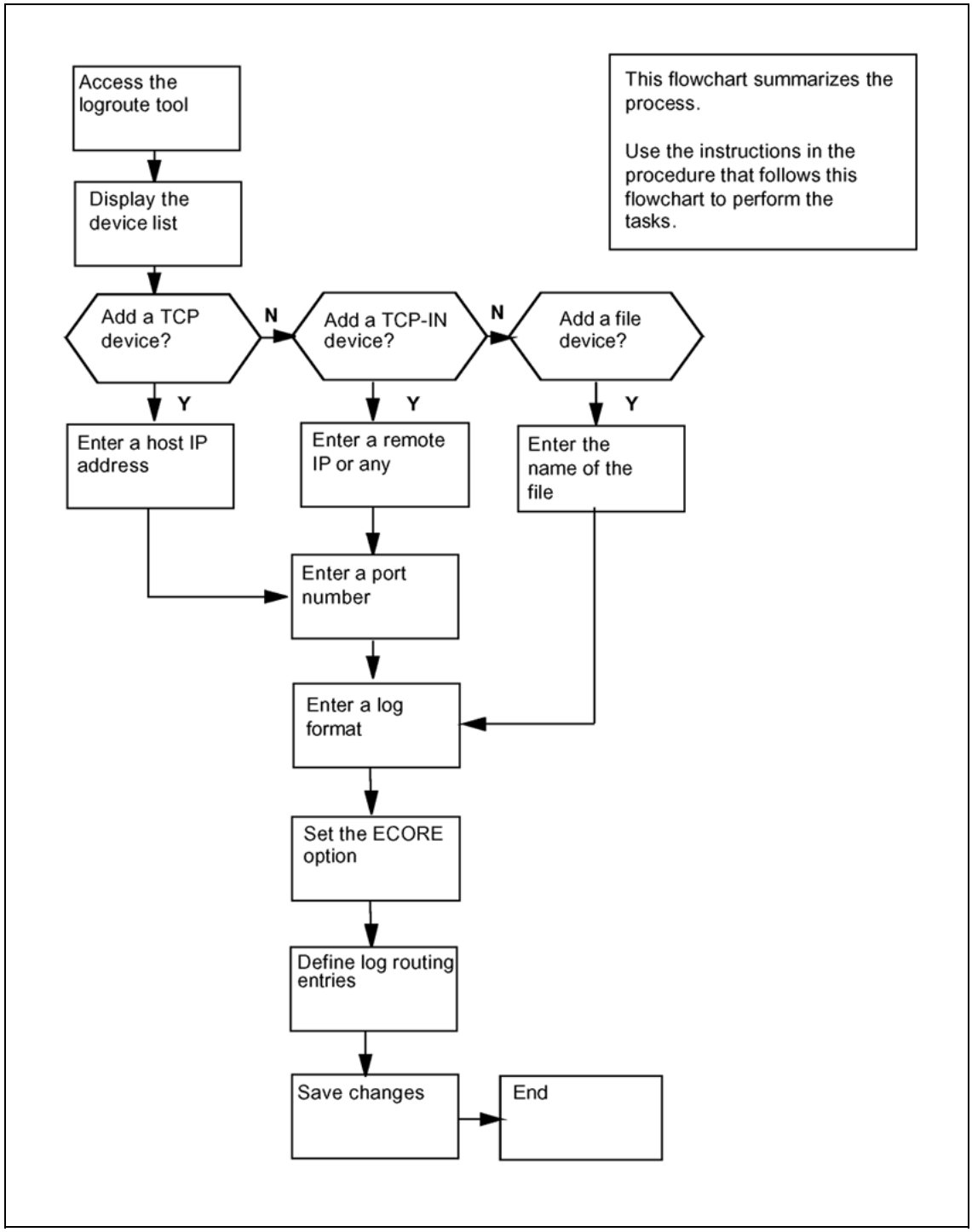
System requirements

The Nortel Multiservice Switch Log Streamer application should be configured on the core manager to retrieve logs from the MDM. To configure the Nortel Multiservice Switch Log Streamer application on the CS 2000 Core Manager, use the procedure Installing and configuring the log delivery application in NN10104-511, *CS 2000 Core Manager Configuration Management*.

Task flow diagram

The following task flow diagram provides a summary of the process. Use the instructions in the procedure that follows the flowchart to perform the task.

Task flow for Configuring log delivery destinations



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

Configuring log delivery for MDM/PPEM security and audit logs (MDM 601 and PPEM 601)

Step	Action

At any workstation or console

1 Log into the core manager.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu

            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



   Enter Option ==>
```

3 Enter "1" to display the device list.

The Device List Menu screen appears.

```
                    Device List Menu

            1 - View Device
            2 - Add Device
            3 - Delete Device
            4 - Modify Device
            5 - Help
            6 - Return to Main Menu



    Enter Option ==>
```

4 Enter "2" to add a new log device.

The Add Device screen appears.

```
                    Add Device

          1 - Add TCP Device
          2 - Add TCPIN Device
          3 - Add File Device
          4 - Help
          5 - Return to Device List




  Enter Option ==>
```

5 Use the following table to determine your next step.

If you want to add a	Do
TCP device	step 6
TCP-IN device	step 18
file device	step 30

6 Enter "1" to add a TCP device.

Example response:

```
                    TCP Device
 Enter ABORT to return to Add Device Screen
          1 - HOST IP     :
          2 - PORT        :
          3 - FORMAT      : STD
          4 - ECORE       : ON
          5 - Log Routing :




 Enter host IP address <###.###.###.###> ==>
```

7 Enter a host IP address.

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : 10.10.10.10
         2 - PORT         :
         3 - FORMAT       : STD
         4 - ECORE        : ON
         5 - Log Routing  :



Enter port number (range - 1024 to 32767) ==>
```

8 Enter a port number from the range displayed.

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : 10.10.10.10
         2 - PORT         : 1111
         3 - FORMAT       : STD
         4 - ECORE        :
         5 - Log Routing  :



Enter format type (STD or SCC2 or STD_OLD or SCC2_OLD)
```

9 Enter the log format (STD, STD_OLD, SCC2, or SCC2_OLD).

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : 10.10.10.10
         2 - PORT         : 1111
         3 - FORMAT       : SCC2
         4 - ECORE        :
         5 - Log Routing  :




Enter Ecore option (ON or OFF) ==>
```

10 Set the ECORE option to ON or OFF.

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : 10.10.10.10
         2 - PORT         : 1111
         3 - FORMAT       : SCC2
         4 - ECORE        : ON
         5 - Log Routing  :




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

11 Enter "a" to add report.

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : 10.10.10.10
         2 - PORT         : 1111
         3 - FORMAT       : SCC2
         4 - ECORE        : ON
         5 - Log Routing :




Enter log identifier (log_type or log_type log_number)
```

12 Enter log identifier as "MDM 601"

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : 10.10.10.10
         2 - PORT         : 1111
         3 - FORMAT       : SCC2
         4 - ECORE        : ON
         5 - Log Routing :
             ADDREP MDM 601




Wish to enter more Logrouting Details? (Y/N)[N] ==>
```

13 Enter "Y" to add more logrouting details.

Example response:

```
                    TCP Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : 10.10.10.10
        2 - PORT         : 1111
        3 - FORMAT       : SCC2
        4 - ECORE        : ON
        5 - Log Routing :
            ADDREP MDM 601



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

14 Enter "a" to add report.

Example response:

```
                    TCP Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : 10.10.10.10
        2 - PORT         : 1111
        3 - FORMAT       : SCC2
        4 - ECORE        : ON
        5 - Log Routing :
            ADDREP MDM 601



Enter log identifier (log_type or log_type log_number)
```

15 Enter log identifier as "PPEM 601"

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

          1 - HOST IP      : 10.10.10.10
          2 - PORT         : 1111
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing :
              ADDREP MDM 601
              ADDREP PPEM 601



Wish to enter more Logrouting Details? (Y/N)[N] ==>
```

16 Enter "N" to indicate you don't want to add more logrouting details.

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

          1 - HOST IP      : 10.10.10.10
          2 - PORT         : 1111
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing :
              ADDREP MDM 601
              ADDREP PPEM 601



Save device Details? (Y/N)[N] ==>
```

17 Enter "Y" to save device details.

The message, "Save data completed -- press return to continue" displays.

Press the Enter key to return to the Add Device screen.

If you enter n, the system returns to the Device List Menu screen. No new device is added to the system.

If you	Do
want to add more devices	go to step 5
do not want to add more devices	go to step 41

18 Enter "2" to add a TCP_IN device.

Example response:

```
                        TCP-IN Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      :
         2 - PORT         :
         3 - FORMAT       : STD
         4 - ECORE        : ON
         5 - Log Routing  :




Enter remote IP address <###.###.###.###> or a for any
```

19 Enter a remote IP address or "a" for any IP address.

Example response:

```
                        TCP-IN Device
Enter ABORT to return to Add Device Screen

         1 - HOST IP      : any
         2 - PORT         :
         3 - FORMAT       : STD
         4 - ECORE        : ON
         5 - Log Routing  :




Enter port number (range - 8550 to 8579) ==>
```

20 Enter a port number from the range displayed.

Example response:

```
                    TCP-IN Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : any
        2 - PORT         : 8558
        3 - FORMAT       : STD
        4 - ECORE        :
        5 - Log Routing  :




Enter format type (STD or SCC2 or STD_OLD or SCC2_OLD)
```

21 Enter the log format (STD, STD_OLD, SCC2, or SCC2_OLD).

Example response:

```
                    TCP-IN Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : any
        2 - PORT         : 8558
        3 - FORMAT       : SCC2
        4 - ECORE        :
        5 - Log Routing  :




Enter Ecore option (ON or OFF) ==>
```

22 Set the ECORE option to ON or OFF.

Example response:

```
                        TCP-IN Device
Enter ABORT to return to Add Device Screen

          1 - HOST IP      : any
          2 - PORT         : 8558
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing  :




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

23 Enter "a" to add report.

Example response:

```
                        TCP-IN Device
Enter ABORT to return to Add Device Screen

          1 - HOST IP      : any
          2 - PORT         : 8558
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing  :




Enter log identifier (log_type or log_type log_number)
```

24 Enter log identifier as "MDM 601".

Example response:

```
                    TCP-IN Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : any
        2 - PORT         : 8558
        3 - FORMAT       : SCC2
        4 - ECORE        : ON
        5 - Log Routing :
            ADDREP MDM 601



Wish to enter more Logrouting Details? (Y/N)[N] ==>
```

25 Enter "Y" to add more logrouting details.

Example response:

```
                    TCP-IN Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : any
        2 - PORT         : 8558
        3 - FORMAT       : SCC2
        4 - ECORE        : ON
        5 - Log Routing :
            ADDREP MDM 601



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

26 Enter "a" to add report.

Example response:

```
                    TCP-IN Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : any
        2 - PORT         : 8558
        3 - FORMAT       : SCC2
        4 - ECORE        : ON
        5 - Log Routing :
            ADDREP MDM 601



Enter log identifier (log_type or log_type log_number)
```

27 Enter log identifier as "PPEM 601".

Example response:

```
                    TCP-IN Device
Enter ABORT to return to Add Device Screen

        1 - HOST IP      : any
        2 - PORT         : 8558
        3 - FORMAT       : SCC2
        4 - ECORE        : ON
        5 - Log Routing :
            ADDREP MDM 601
            ADDREP PPEM 601



Wish to enter more Logrouting Details? (Y/N)[N] ==>
```

28 Enter "N" to indicate you don't want to add more logrouting details.

Example response:

```
                        TCP-IN Device
Enter ABORT to return to Add Device Screen

          1 - HOST IP      : any
          2 - PORT         : 8558
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing  :
              ADDREP MDM 601
              ADDREP PPEM 601



Save device Details? (Y/N)[N] ==>
```

29 Enter "Y" to save device details.

The message, "Save data completed -- press return to continue" displays.

Press the Enter key to return to the Add Device screen.

If you enter **n**, the system returns to the Device List Menu screen. No new device is added to the system.

If you	Do
want to add more devices	go to step 5
do not want to add more devices	go to step 41

30 Enter "3" to add file device.

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

          1 - FILENAME     :
          2 - FORMAT       : STD
          3 - ECORE        : ON
          4 - Log Routing  :




Enter file name ==>
```

31 Enter the file name with the full path, where logs will be stored.

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

          1 - FILENAME     : /cbmdata/00/data/logs/fl1
          2 - FORMAT       : STD
          3 - ECORE        : ON
          4 - Log Routing  :




Enter format type (STD or SCC2 or STD_OLD or SCC2_OLD)
```

32 Enter the log format (STD, STD_OLD, SCC2, or SCC2_OLD).

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

          1 - FILENAME     : /cbmdata/00/data/logs/fl1
          2 - FORMAT       : SCC2
          3 - ECORE        : ON
          4 - Log Routing  :




Enter Ecore option (ON or OFF) ==>
```

33 Set the ECORE option to ON or OFF.

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

         1 - FILENAME     : /cbmdata/00/data/logs/fl1
         2 - FORMAT        : SCC2
         3 - ECORE         : ON
         4 - Log Routing   :




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

34 Enter "a" to add report.

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

         1 - FILENAME     : /cbmdata/00/data/logs/fl1
         2 - FORMAT        : SCC2
         3 - ECORE         : ON
         4 - Log Routing   :




Enter log identifier (log_type or log_type log_number)
```

35 Enter log identifier as "MDM 601".

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

         1 - FILENAME     : /cbmdata/00/data/logs/fl1
         2 - FORMAT        : SCC2
         3 - ECORE         : ON
         4 - Log Routing   :
             ADDREP MDM 601




Wish to enter more Logrouting details? (Y/N)[N] ==>
```

36 Enter "Y" to add more logrouting details.

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

         1 - FILENAME     : /cbmdata/00/data/logs/fl1
         2 - FORMAT        : SCC2
         3 - ECORE         : ON
         4 - Log Routing   :
             ADDREP MDM 601




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

37 Enter "a" to add report.

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

          1 - FILENAME     : /cbmdata/00/data/logs/fl1
          2 - FORMAT        : SCC2
          3 - ECORE         : ON
          4 - Log Routing   :
              ADDREP MDM 601




Enter log identifier (log_type or log_type log_number)
```

38 Enter log identifier as "PPEM 601".

Example response:

```
                        File
Enter ABORT to return to Add Device Screen

          1 - FILENAME     : /cbmdata/00/data/logs/fl1
          2 - FORMAT        : SCC2
          3 - ECORE         : ON
          4 - Log Routing   :
              ADDREP MDM 601
              ADDREP PPEM 601




Wish to enter more Logrouting Details? (Y/N)[N] ==>
```

39 Enter "N" to indicate you don't want to add more logrouting details.

Example response:

```
                        TCP Device
Enter ABORT to return to Add Device Screen

          1 - FILENAME     : /cbmdata/00/data/logs/fl1
          2 - FORMAT       : SCC2
          3 - ECORE        : ON
          4 - Log Routing  :
              ADDREP MDM 601
              ADDREP PPEM 601



Save device Details? (Y/N)[N] ==>
```

40 Enter "Y" to save device details.

The message, "Save data completed -- press return to continue" displays.

Press the Enter key to return to the Add Device screen.

If you enter **n**, the system returns to the Device List Menu screen. No new device is added to the system.

If you	Do
want to add more devices	go to step 5
do not want to add more devices	go to step 41

41 Return to the Device List Menu screen:

enter 5

42 Return to the Logroute Main Menu screen:

enter 6

43 Quit the logroute tool:

enter 6

44 You have completed this procedure.

—End—

Excluding MDM/PPEM audit and security logs from other log devices

Purpose

Use this procedure to exclude MDM/PPEM audit and security logs from other log devices.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

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

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

System requirements

The Nortel Multiservice Switch Log Streamer application should be configured on the core manager to retrieve logs from the MDM. To configure the Nortel Multiservice Switch Log Streamer application on the CS 2000 Core Manager, use the procedure Installing and configuring the log delivery application in NN10104-511, *CS 2000 Core Manager Configuration Management*.

Procedure

The following procedures show how to exclude the MDM/PPEM audit and security logs from all log device types.

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

Excluding the MDM/PPEM audit and security logs from other log devices.

Step	Action

At the VT100 console

1 Log into the core manager.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu


            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



   Enter Option ==>
```

3 Enter "1" to display the device list.

The Device List Menu screen appears.

```
                    Device List Menu

            1 - View Device
            2 - Add Device
            3 - Delete Device
            4 - Modify Device
            5 - Help
            6 - Return to Main Menu



    Enter Option ==>
```

4 Enter "1" to view the configured devices.

The Device List screen appears.

This example screen, and other example screens shown in this procedure, shows log removal only for a TCP device. These examples are provided to show the type of screen that will display in response to the steps performed in this procedure. Thus, the content of the screens that actually displays when you are preforming this procedure will vary according to device type and your system's configuration.

```
                    Device List Screen

           Devices:
           1 - HOST: 10.10.10.10.    PORT: 1111   Type: TCP









    Enter Device number for more details or
    Press Enter to return to Device List Menu:
```

5 Enter the number for the device you want to review. For example, in the example screen shown in step 4, you would enter "1" to display the details for the device shown.

Example response

```
                    TCP Device

          1 - HOST IP      : 10.10.10.10
          2 - PORT         : 1111
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing :
              ADDREP MDM 601
              ADDREP PPEM 601


  Press Enter to return to Device List Screen:
```

6 In the device detail screen that displays, verify that logs "MDM 601" and "PPEM 601" are shown configured for the device. Also verify whether the device is configured for ALL logs.

If the device	
is configured for ALL logs	step 23
is configured for "MDM 601" and "PEM 601" logs	step 7

7 Press Enter to return to the Device List Screen and when the Device List Screen displays, press Enter again to return to the Device List Menu.

The Device List Menu screen appears.

```
                  Device List Menu

          1 - View Device
          2 - Add Device
          3 - Delete Device
          4 - Modify Device
          5 - Help
          6 - Return to Main Menu


  Enter Option ==>
```

8 Enter "4" to modify a device.

The Device List screen appears.

```
                    Device List Screen

            Devices:
            1 - HOST: 10.10.10.10.    PORT: 1111   Type: TCP




    Enter device number to delete ==>
```

9 Enter the number for the device you want to modify. For example, in the example screen shown in step 8, you would enter "1" to display the device shown.

Example response

```
                        TCP Device

            1 - HOST IP      : 10.10.10.10
            2 - PORT         : 1111
            3 - FORMAT       : SCC2
            4 - ECORE        : ON
            5 - Log Routing  :
                ADDREP MDM 601
                ADDREP PPEM 601



    Enter number of device parameter to change:
```

10 Enter "5" to change the Log Routing device parameter.

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP MDM 601
          2 - ADDREP PPEM 601




 Enter "a" to add report or "d" to delete report ==>
```

11 Enter "d" to delete a report.

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP MDM 601
          2 - ADDREP PPEM 601




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

12 Enter the log routing number for MDM 601. For example, in the Logrouting of TCP Device screen shown in step 11, you would enter "1".

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen

          1 - ADDREP PPEM 601




 Wish to delete more Logrouting Details? (Y/N)[N]:
```

13 Enter "Y" to indicate that you want to delete another Logrouting detail.

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP PPEM 601




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

14 Enter the log routing number for PPEM 601. For example, in the Logrouting of TCP Device screen shown in step 13, you would enter "1".

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen




 Wish to delete more Logrouting Details? (Y/N)[N]:
```

15 Enter "N" to indicate that you don't want to delete more Logrouting details.

16 Enter "Y" to save the Logrouting details changes you have made.

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen




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

17 Enter "Y" to confirm that you wish to proceed with saving the Logrouting details changes.

Example response:

```
                    Logrouting of TCP Device
Enter ABORT to return to previous screen




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

18 Press Enter to continue.

Example response

```
                        TCP Device
Enter ABORT to return to Previous Screen
          1 - HOST IP      : 10.10.10.10
          2 - PORT         : 1111
          3 - FORMAT       : SCC2
          4 - ECORE        : ON
          5 - Log Routing  :




Enter number of device parameter to change:
```

19 Enter "abort" to return to the Modify Device Menu.

Example response:

```
                    Modify Device Menu
Enter ABORT to return to Device List Menu
          Devices:                                        Type:
          1 - HOST: 10.10.10.10     PORT: 1111            TCP




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

20 Enter "abort" to return to the Device List Menu.

The Device List Menu screen appears.

```
                    Device List Menu

          1 - View Device
          2 - Add Device
          3 - Delete Device
          4 - Modify Device
          5 - Help
          6 - Return to Main Menu



 Enter Option ==>
```

21 Enter "6" to return to the Logroute main menu screen.

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu

            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



    Enter Option ==>
```

22 Use the following table to determine your next step.

If you	Do
want to exclude MDM/PPEM audit and security logs from another device	step 3
do not want to exclude MDM/PPEM audit and security logs from another device	step 40

23 Press Enter to return to the Device List Screen and when the Device List Screen displays, press Enter again to return to the Device List Menu.

The Device List Menu screen appears.

```
                    Device List Menu

            1 - View Device
            2 - Add Device
            3 - Delete Device
            4 - Modify Device
            5 - Help
            6 - Return to Main Menu



    Enter Option ==>
```

24 Enter "4" to modify a device.

The Device List screen appears.

```
                    Device List Screen

            Devices:
            1 - HOST: any    PORT: 8558   Type: TCP-IN









    Enter device number to delete ==>
```

25 Enter the number for the device you want to modify. For example, in the example screen shown in step 24, you would enter "1" to display the device shown.

Example response

```
                        TCP-IN Device

            1 - HOST IP      : any
            2 - PORT         : 8558
            3 - FORMAT       : SCC2
            4 - ECORE        : ON
            5 - Log Routing  :
                ADDREP ALL




    Enter number of device parameter to change:
```

26 Enter "5" to change the Log Routing device parameter.

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL




 Enter "a" to add report or "d" to delete report ==>
```

27 Enter "a" to add report.

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL




 Enter "a" to add report or "d" to delete report ==>
```

28 Enter "d" to delete report.

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL




 Enter log identifier (log_type or log_type log_number)
```

29 Enter the log identifier, "MDM 601".

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL
          2 - DELREP MDM 601




 Wish to enter more Logrouting Details? (Y/N)[N]:
```

30 Enter "Y".

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL
          2 - DELREP MDM 601




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

31 Enter "d" to delete report.

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL
          2 - DELREP MDM 601




 Enter log identifier (log_type or log_type log_number)
```

32 Enter the log identifier, "PPEM 601".

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL
          2 - DELREP MDM 601
          3 - DELREP PPEM 601




 Wish to enter more Logrouting Details? (Y/N)[N]:
```

33 Enter "N" to indicate that you don't want to enter more Logrouting details.

34 Enter "Y" to save the Logrouting details changes you have made.

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen









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

35 Enter "Y" to confirm that you wish to proceed with saving the Logrouting details changes.

Example response:

```
                    Logrouting of TCP-IN Device
Enter ABORT to return to previous screen




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

36 Press Enter to continue.

Example response

```
                        TCP-IN Device
Enter ABORT to return to Previous Screen

         1 - HOST IP      : any
         2 - PORT         : 8558
         3 - FORMAT       : SCC2
         4 - ECORE        : ON
         5 - Log Routing  :




Enter number of device parameter to change:
```

37 Enter "abort" to return to the Modify Device Menu.

Example response:

```
                    Modify Device Menu
Enter ABORT to return to Device List Menu
          Devices:                                    Type:
          1 - HOST: any     PORT: 8558                TCP-IN




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

38 Enter "abort" to return to the Device List Menu.

The Device List Menu screen appears.

```
                    Device List Menu

          1 - View Device
          2 - Add Device
          3 - Delete Device
          4 - Modify Device
          5 - Help
          6 - Return to Main Menu



 Enter Option ==>
```

39 Enter "6" to return to the Logroute main menu screen.

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu

            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



   Enter Option ==>
```

40 Enter "6" to exit from the Logroute tool.

41 You have completed this procedure.

—End—

Specifying the logs delivered from the CM to the core manager

Purpose

Use this procedure to specify the logs to be delivered from the computing module (CM) to the core manager. When the Log Delivery service is first installed, it receives all logs in the CM log stream by default. If you wish to modify the incoming CM log stream, use the CM Configuration File menu in the logroute tool to add or delete individual logs or log types.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

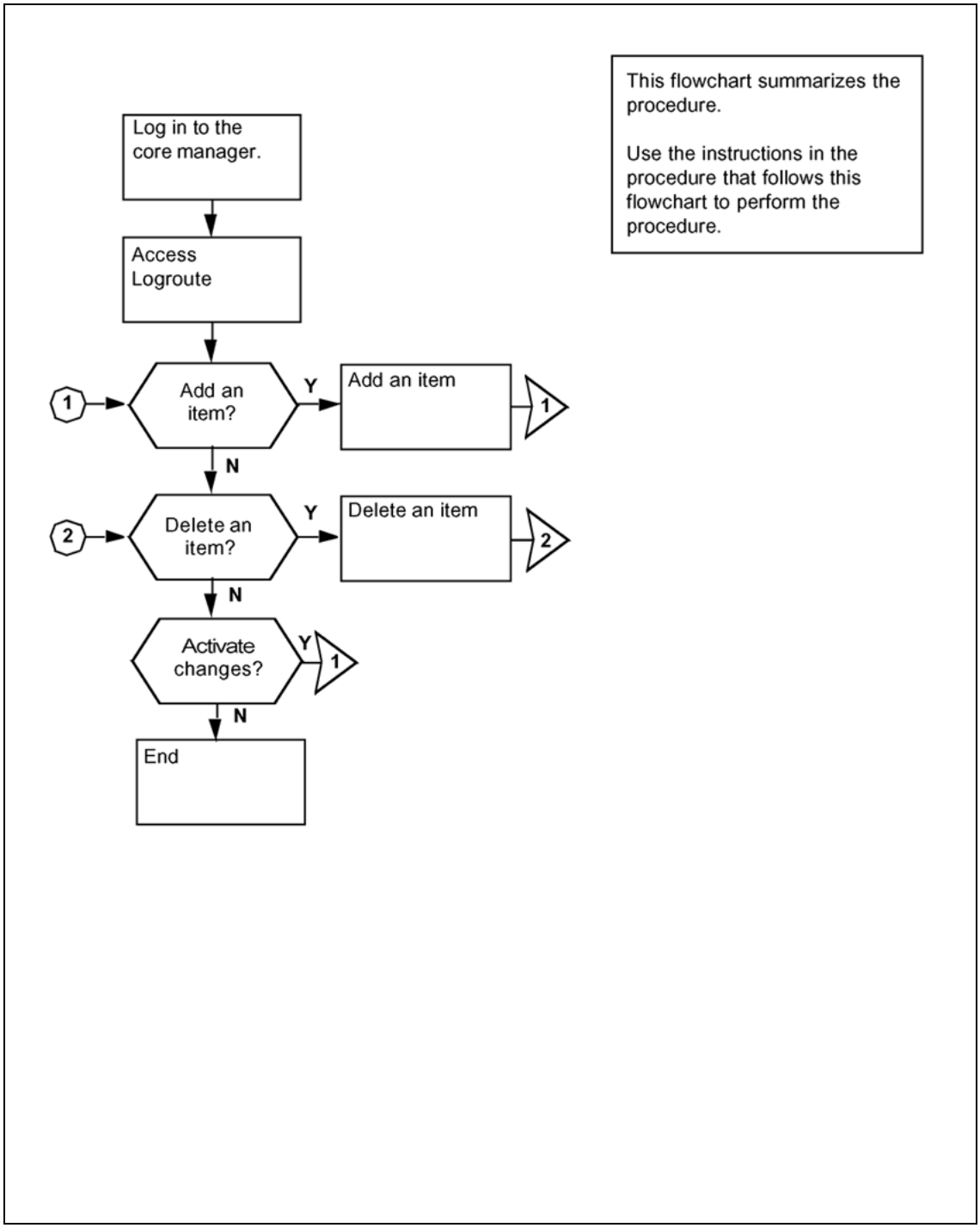
Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Task flow diagram

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

Task flow for Specifying the logs delivered from the CM the core manager



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

Procedure

Specifying the logs delivered from the CM to the core manager

Step	Action
	At the VT100 console
1	Log into the core manager.
2	Access the logroute tool: **`logroute`** The Logroute Main Menu screen is displayed.

```
                    Logroute Main Menu

            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - GDD Configuration
            5 - Help
            6 - Quit Logroute



    Enter Option ==>
```

3	Access the CM Configuration File menu: `3` The CM Config File Menu screen is displayed.

```
                    CM Config File Menu

            1 - View Config List
            2 - Add Report
            3 - Delete Report
            4 - Help
            5 - Return to Main Menu



    Select Option ==>
```

If you want to	Do
add routing report to the list	step 4
delete routing report from the list	step 7

4 Access the CM - Add Report screen:

2

The system displays the list of the current routing entries for the incoming CM log stream.

Example response: response

```
                    CM - Add Report
Enter ABORT to return to CM Config File Menu

          1 - DEL IOAUD 107




Warning: You must BSY and RTS the Log Delivery application
for the CM configuration to take effect.
```

If you want to	Do
suppress logs (cause them to be removed from the incoming CM log stream)	enter **d**, and press the Enter key
un-suppress logs (cause them to be included in the incoming CM log stream)	enter **a**, and press the Enter key

An entry of n (NOCMLOGS) will suppress all CM logs -- no CM logs will be delivered to your system.

Response

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

5 Enter a log type or a combination of log type and log number (separated by a space).

An example of a log type is "PM". This entry will suppress or un-suppress all PM logs.

An example of a combined log type and log number is PM 181. This entry will suppress or un-suppress the PM181 logs but leave the routing of other PM logs unchanged.

Example response:

```
Save Report details?  (Y/N)[N]:
```

6 Save your changes:

y

The new item is added to the list.

If you	Do
want to add more entries to the list	step 4
do not want to add more entries to the list	step 10

7 Access the CM - Delete Report screen:

```
3
```

The system displays the list of the current routing entries for the incoming CM log stream.

Example response:

```
                    CM - Delete Report
Enter ABORT to return to CM Config File Menu

           1 - DEL IOAUD 107
           2 - ADD PM 181









      Select report to delete ==>
```

8 Enter the number of the item you want to delete from the list.

Example response:

```
Report will be deleted permanently.  Continue?
(Y/N)[N]:
```

9 Confirm the delete command:

```
Y
```

Example response:

The system displays the CM Delete Report screen with the following warning

```
Warning:  You must BSY and RTS the Log Delivery
application for the CM configuration to take effect.
```

If you	Do
want to delete more entries from the list	step 8
do not want to delete more entries from the list	step 10

10 Return to the CM Config File Menu screen:

```
abort
```

If you	Do
want to make more changes to the CM log stream list	step 4
do not want to make more changes to the CM log stream list	step 11

11 Return to the Logroute Main Menu screen:

```
5
```

12 Quit the logroute tool:

```
6
```

13 You have completed this procedure.

—End—

Configuring Log Delivery global parameters

Purpose

Use this procedure to configure the Log Delivery global parameters. The global parameters are set to default values at initial installation and should not require modification.

The online Log Delivery commissioning tool called logroute controls Log Delivery global parameters. The Log Delivery global parameters apply to all Log Delivery output devices and are separate from device-specific parameters.

For information on configuring or modifying device-specific parameters, refer to one of the following procedures:

- "Configuring log delivery destinations" (page 15)
- "Modifying a log device using logroute" (page 23)

The logroute tool allows you to customize the following global parameters:

- log_office_id (office name)

  This parameter is valid only for devices that have log format set to STD or SCC2.
- buffer size (number of logs)
- reconnect time-out value (seconds)
- lost logs threshold (number of lost logs before the system generates a design log)

  This parameter is for Nortel personnel only.
- incoming end of line character (ASCII code)
- outgoing end of line characters (ASCII code)
- start of log characters (ASCII code)
- end of logs characters (ASCII code)
- the number of days to keep log files
- maximum size of a log file (Mbyte)
- maximum size action

ATTENTION

Any settings changed by the Log Delivery application and the logroute tool will not affect Generic Data Delivery settings or the logs in the /gdd volume.

If the global parameters do require modification, the ranges and default for each parameter are as follows:

- log_office_id: values are NULL, CLLI, CORE-COMPAT, or up to 12-characters office name, default is CLLI

  The log_office_id parameter refers to the office name, which will be attached to all logs delivered to all devices that have log format set to STD or SCC2. If you enter

  — NULL, the office name will not be attached to the logs.

  — CLLI, the CLLI name of your system will be attached to all logs.

  — CORE-COMPAT, the core's LOG_OFFICE_ID defined in table OFCVAR will be used for all logs. Until the first log arrives from the core, the system CLLI is used.

- buffer size (number of logs): range is 50 to 300, default is 150
- reconnect time-out value (secs): range is 1 to 3600, default is 15
- lost logs threshold: range is 1 to 300, default is 100 (-1 turns this option off)
- number of days to keep log files: range is 1 to 45, default is 5
- maximum size of a log file (Mbytes): range is 5 to 300, default is 40
- maximum size action: values are STOPDEV, CIRCULATE, and ROTATE

  The maximum size action parameter allows you to configure the action the system performs when the file reaches its maximum size. The STOPDEV value tells the file device to save the data in separate files every 12 hours. When the file created at each 12-hour rotation is full, the system stops writing log data to the file. The system loses any log data generated from the time the system stops writing to the file to the start of a new file at the next rotation.

  The ROTATE value tells the file device to save the data in separate files every 12 hours. When the file created at each 12-hour rotation is full, the system creates another file to continue saving any log data. The system does not wait until the next 12-hour rotation to create a new file.

  The CIRCULATE value tells the file device to save the data in separate files every 12 hours. When the file reaches its maximum size, the system saves the new log data by overwriting the earliest data in the file.

The remaining global parameters are represented by ASCII character codes. For more information on these parameters including their ranges, see the logroute help menu. The values for the global parameters represented by ASCII character codes are as follows:

- incoming end of line character: default is 10 which corresponds to a line feed character (go to the next line)
- outgoing end of line characters: default is 10 13 which represents a line feed (go to the next line) followed by a carriage return
- start of log characters: default is 10 13 which represents a line feed (go to the next line) followed by a carriage return
- end of logs characters: default is 10 13 which represents a line feed (go to the next line) followed by a carriage return

  Any configuration changes take effect immediately. You do not have to busy and return the Log Delivery application to service for the changes to take effect.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

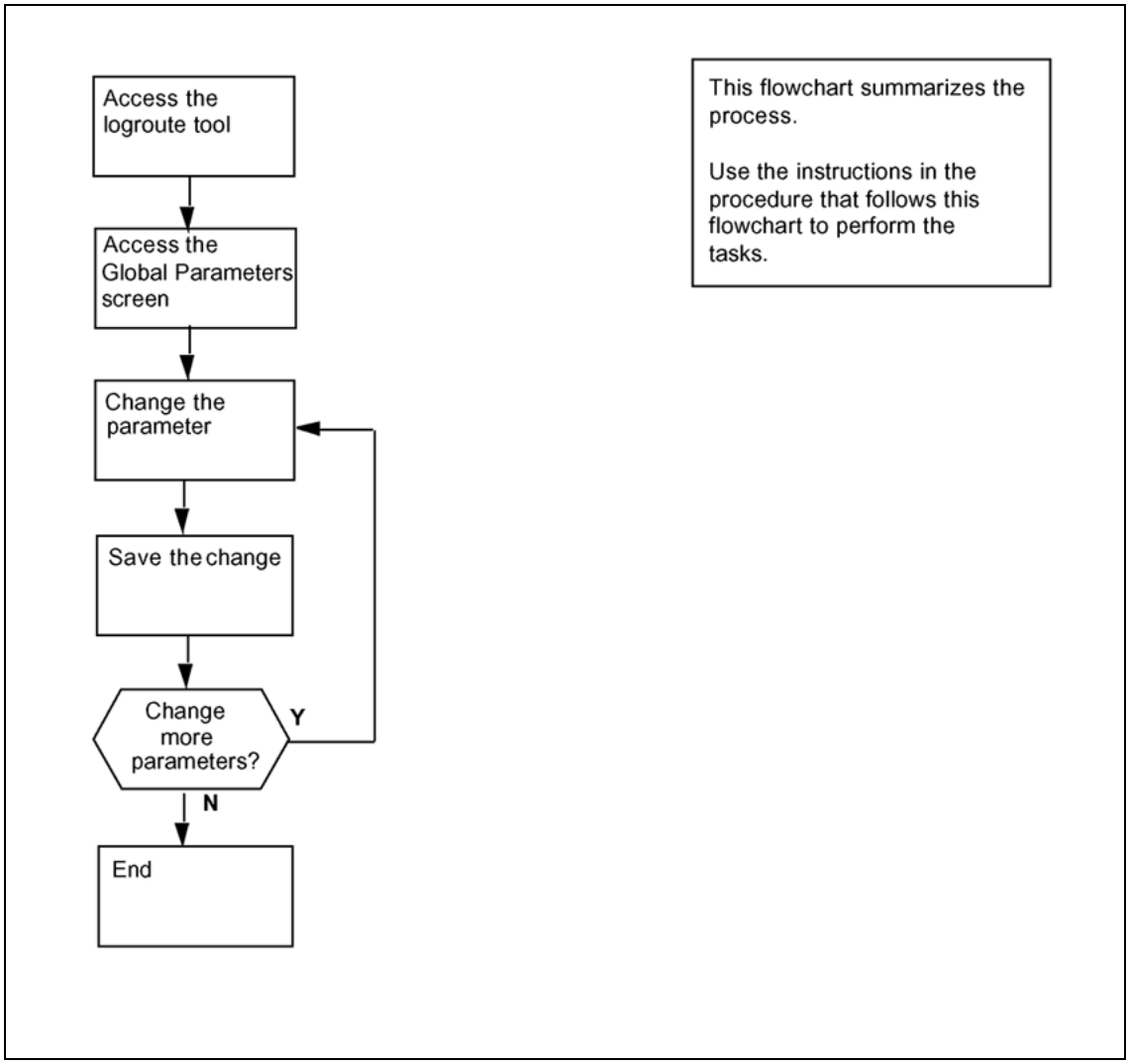
Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Task flow diagram

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

Task flow for Configuring Log Delivery global parameters



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

Procedure

Configuring Log Delivery global parameters

Step	Action
	At the VT100 console
1	Log into the core manager.
2	Access the logroute tool:

logroute

The Logroute Main Menu screen appears.

3 Access the Global Parameters screen:

2

Example response:

```
          Global Parameters
1  - LOG_OFFICE_ID : CLLI
2  - Buffer size (number of logs)     : 150
3  - Reconnect timeout value (secs)   : 15
4  - Lost logs threshold (NT only)    : 100
5  - Incoming end of line character   : 10
6  - Outgoing end of line characters  : 10 13
7  - Start of log characters          : 10 13
8  - End of logs characters           : 10 13
9  - Number of days to keep log files : 5
10 - Maximum size of a log file (Meg) : 40
11 - Maximum size action  : STOPDEV
12 - Help
13 - Return to Main Menu
Enter Option ==>
```

This display shows the default values for the Global Parameters menu.

4 Select the parameter that you want to change:

<n>

where

<n> is the menu number next to the global parameter you want to change

Example response for changing the buffer size:

```
          Global Parameters
1  - LOG_OFFICE_ID : CLLI
2  - Buffer size (number of logs)     : 150
3  - Reconnect timeout value (secs)   : 15
4  - Lost logs threshold (NT only)    : 100
5  - Incoming end of line character   : 10
6  - Outgoing end of line characters  : 10 13
7  - Start of log characters          : 10 13
8  - End of logs characters           : 10 13
9  - Number of days to keep log files : 5
10 - Maximum size of a log file (Meg) : 40
11 - Maximum size action  : STOPDEV
12 - Help
13 - Return to Main Menu
Enter buffer size (range - 50 to 300) ==>
```

The log and line delimiters (incoming and outgoing end of line characters, and start and end of log characters) must be entered as decimal or hexadecimal ASCII code.

For a detailed description of each parameter, see the Help menu (option 12).

5 Enter a new value for the selected parameter.

6 The system prompts you to save the change. The following message is displayed:

```
Save Global Parameter details  [Y/N][N]:
```

If you	Do
want to save your change	enter **y**, press the Enter key, and continue with step 7
do not want to save your change	enter **n**, press the Enter key, and go to step 11

7 The system displays the following warning:

```
WARNING: All log devices will be restarted.  Do you
wish to proceed.
```

If you want to	Do
complete the saving process	step 9
stop the saving process	step 8

8 Enter **n**.

The unchanged value appears on the Global Parameter screen.

Continue with step 11.

9 Enter **y**.

The system displays the following message:

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

10 Press the Enter key again to confirm the change. The new value appears on the Global Parameter screen.

If you	Do
want to change another global parameter	step 4
do not want to change another global parameter	step 11

11 Return to the Logroute Main Menu:

```
13
```

12 Quit the logroute tool:

```
6
```

13 You have completed this procedure.

—End—

Configuring the GDD parameter using logroute

Purpose

Use this procedure to configure the Generic Data Delivery (GDD) parameter. This parameter defines how many days the log files will be stored in the /gdd directory on the datavg volume.

When the configured number of days is reached (maximum 30 days), the logs are rotated, and the oldest log file is replaced by the newest.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

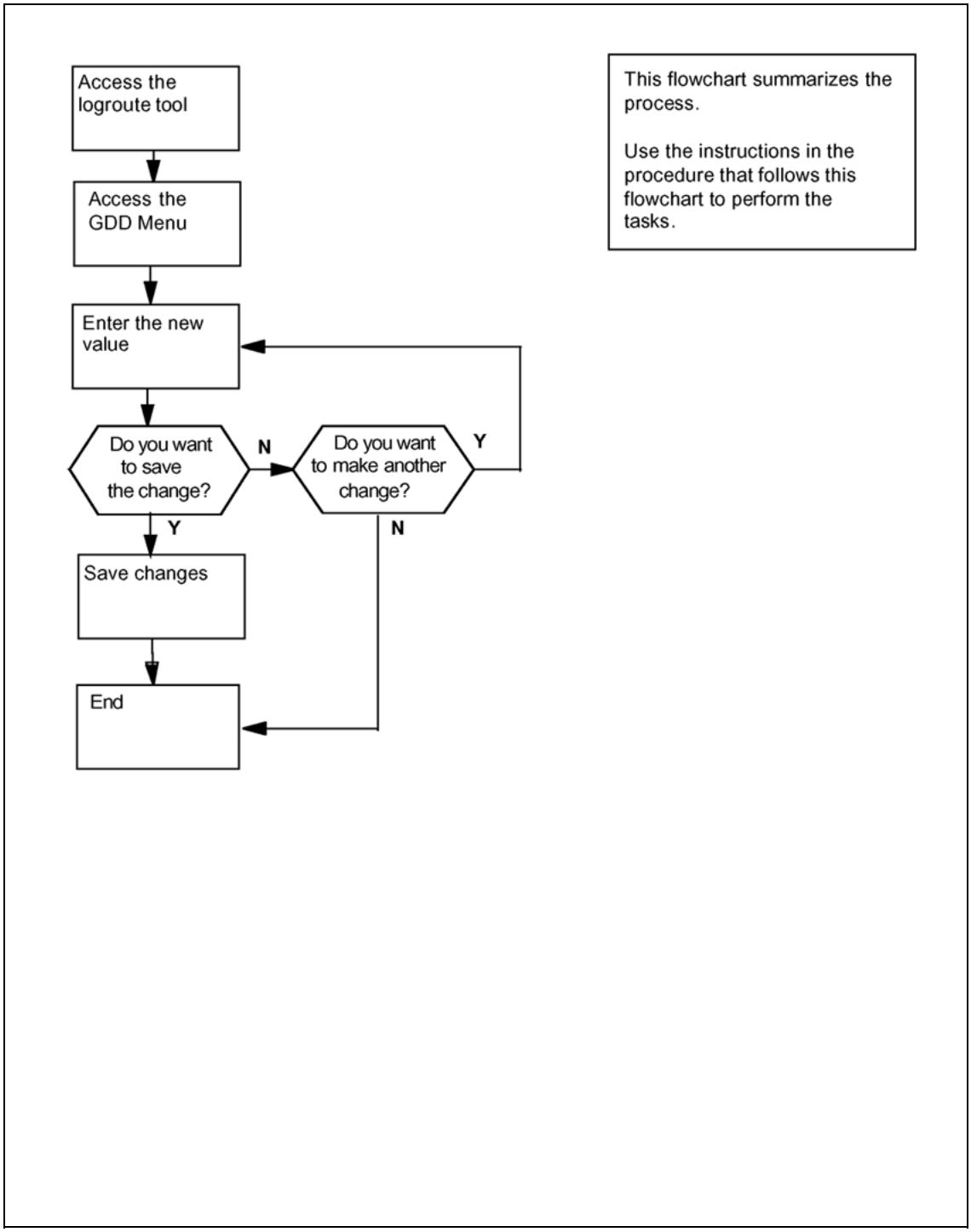
Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Task flow diagram

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

Task flow for Configuring GDD parameter using logroute



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

Configuring GDD parameter using logroute

Step	Action

At the VT100 console

1 Log into the core manager.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu

            1 - Device List
            2 - Global Parameters
            3 - CM Configuration File
            4 - Gdd Configuration
            5 - Help
            6 - Quit Logroute



    Enter Option ==>
```

3 Access the GDD Menu:

```
4
```

Example response:

```
                        GDD Menu

      1 - Number of days to keep log files in /gdd:  30
      2 - Help
      3 - Return to Main Menu




    Enter Option ==>
```

4 Select the GDD parameter:

```
1
```

Example response:

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

5 Specify how many days you want the log files to be stored in the /gdd directory. Enter the number (within the range) and press the Enter key.

Example response:

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

If you	Do
want to save your change	step 7
do not want to save your change	step 6

6 Cancel your change:

```
n
```

If you	Do
want to make another change	step 4
do not want to make another change	step 10

7 Save the GDD value:

```
y
```

Example response:

```
Warning:  This would change the number of days to store
logs in /gdd.  Log files older than the day specified
would be deleted.
```

8 Press the Enter key to confirm the change.

Example response:

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

9 Press the Enter key to continue. The new value is displayed.

10 Return to the Logroute Main Menu screen:

```
3
```

11 Quit the logroute tool:

```
6
```

12 You have completed this procedure.

—End—

Commissioning or decommissioning Network Time Protocol (NTP)

Purpose

Use this procedure to add or remove a Network Time Protocol (NTP) server or peer on the CS 2000 Core Manager.

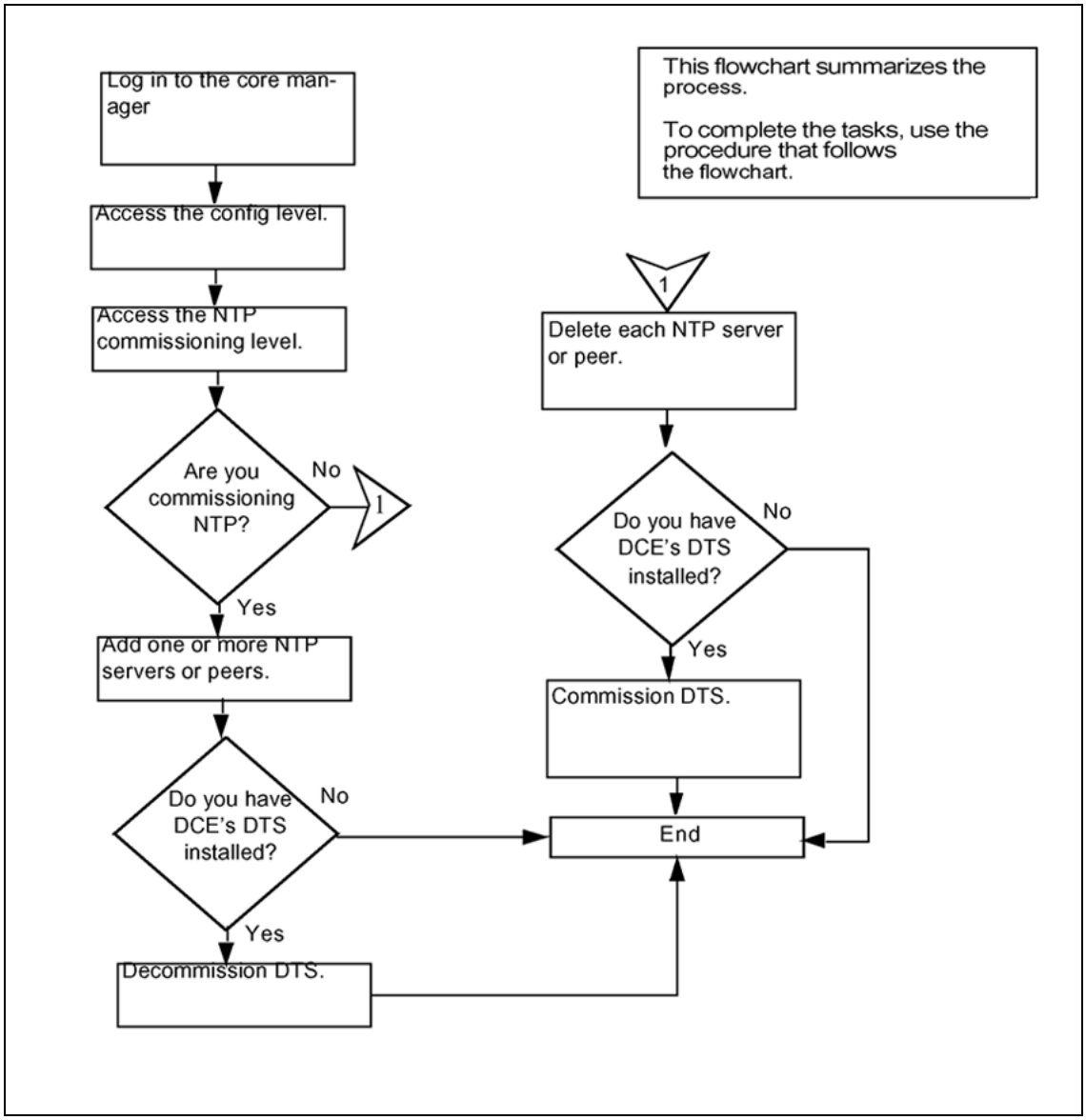
Prerequisites

If you have a distributed Computing Environment (DCE) Distributed Time Service (DTS) commissioned, you will be prompted to remove it once you have commissioned NTP. For this, you will need a DCE administrator password.

Task flow diagram

The following task flow diagram summarizes the commissioning or decommissioning Network Time Protocol (NTP) process. To complete the tasks, use the instructions in the procedure that follows the flowchart.

Task flow for Commissioning or decommissioning NTP



Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

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

Procedure

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

Commissioning or decommissioning NTP

Step Action

At the local VT100 console

1 Log into the core manager. Refer to "Prerequisites" (page 92) for details.

2 Access the sdm configuration level:

```
sdmconfig
```

3 Access the NTP commissioning step:

```
step <#>
```

where

`<#>` is the number next to the Network Time Protocol commissioning step

Note: Use Up (12) or Down (13) to scroll through the list until you see the Network Time Protocol commissioning step.

If you are	Do
commissioning NTP	step 4
decommissioning NTP	step 8

4 Add an NTP server or peer:

```
add
```

a. When prompted, select the type of host you want to add:

```
1 (to add a server) or 2 (to add a peer)
```

Note: A peer can act as a server.

b. When prompted, enter a description for that server or peer.

c. When prompted, enter the host name for that server or peer.

d. When prompted, enter the IP address for that server or peer.

Note: You can add a maximum of 20 server or peers.

5 When prompted, confirm the add command:

```
y
```

Response:

```
Synchronization in progress, may take up to 10 mins.
```

If you	Do
have DTS installed	step 6
do not have DTS installed	step 4

6 When prompted, enter your DCE administrator password and remove DTS.

7 Use the following table to determine your next step.

If you	Do
want to add more NTP servers or peers	step 4
do not want to add more NTP servers or peers	step 10

8 Remove each of the NTP servers or peers:

`delete <#>`

where

`<#>` is the number next to the NTP server or peer

Note: You can also delete an NTP server or peer using its hostname or IP address.

9 When prompted, confirm the delete command:

```
y
```

Note: If you are deleting the last NTP server or peer on the list and you have DCE installed on your system, you will be

prompted to setup DCE's DTS. For this, you will need a DCE administrator password.

If you	Do
want to delete another NTP server or peer	step 8
do not want to delete another NTP server or peer	step 10

10 You have completed this procedure.

—End—

Commissioning or decommissioning edge node monitoring

Use these procedures to commission or decommission edge node monitoring. When edge node monitoring is commissioned, the core manager can detect failures on active Ethernet interfaces and switch the Ethernet connection to the other domain.

Prerequisites

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

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

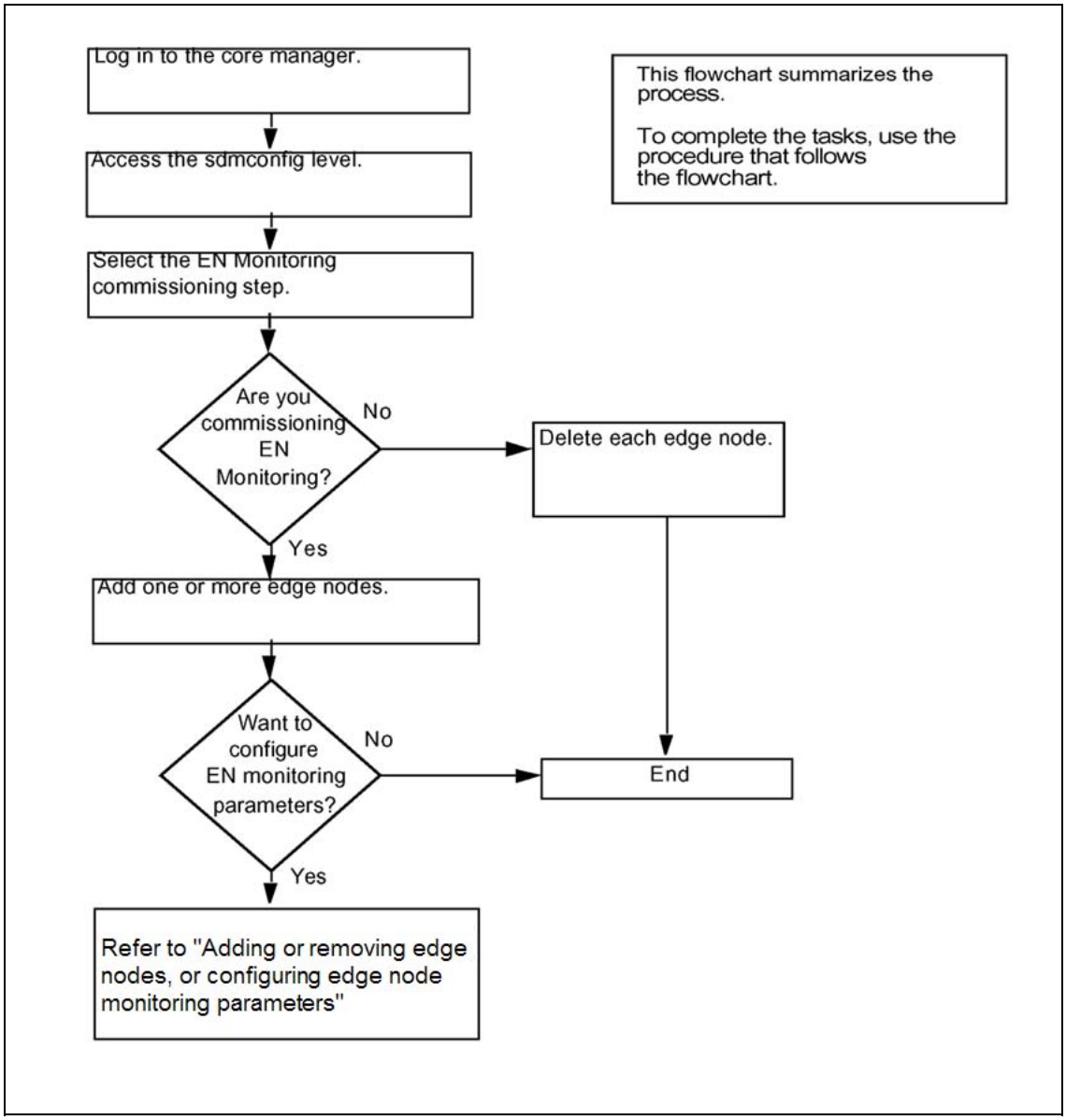
Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Task flow diagram

The following flowchart summarizes the process. To complete the tasks, use the instructions in the procedures that follow the flowchart.

Task flow for Commissioning or decommissioning edge node monitoring



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

Procedures

Commissioning edge node monitoring

Step	Action
	At the workstation or console

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

2 Access the configuration level:

```
sdmconfig
```

3 Access the Edge Node Monitoring commissioning step level:

```
step <#>
```

where

`<#>` is the number next to the Edge Node Monitoring commissioning step.

Note: Use Up (12) or Down (13) to scroll through the list until you see the Edge Node Monitoring commissioning step.

4 Add an edge node:

```
add
```

5 Enter the logical ethernet number for the edge node.

6 Enter a description for the edge node.

7 Enter the IP address for the edge node.

8 Confirm the add command:

```
y
```

Response

```
Add NODE - Command complete.
```

Note: You can change the values for an edge node at any time using the Change command.

If you want to	Do
add another edge node	go to step 4
configure the monitoring parameters for the edge nodes	refer to procedure Adding or removing edge nodes, or configuring edge node monitoring parameters
do neither of the above actions	you have completed this procedure

—End—

Decommissioning edge node monitoring

Step	Action

At the workstation or console

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

2 Access the configuration level:

```
sdmconfig
```

3 Remove each of the edge nodes:

```
delete node <#>
```

where

`<#>` is the number next to the edge node.

4 When prompted, confirm the delete command:

```
y
```

If	Do
you have another edge node to remove	step 3
all edge nodes are removed	you have completed this procedure

—End—

Adding or removing edge nodes, or configuring edge node monitoring parameters

Use these procedures to add or remove edge nodes, or to configure the monitoring parameters for the edge nodes.

This procedure should also be used to change existing edge node monitoring parameters in response to system problems. For example, the "Period" edge node monitoring parameter may need to be changed when frequent edge node alarms are raised due to network delays.

Note: Before changing existing edge node parameters, be aware of the following normal conditions under which the SDM will lose connection to the edge node, resulting in "connection is unstable" logs being raised:

- dbgent switching occurs once every 24 hours. During the dbgent switch, the SDM switches from one pent device to another if both pent devices are online. During this switch, the SDM loses pings from the edge node for approximately 2 or 3 seconds, resulting in "connection is unstable" logs being raised. Pings are then received normally, however, once the dbgent switch has completed.
- During a dbgent switch from one edge node to another when two or more edge nodes are commissioned, an edge node will lose connection with the SDM for a few seconds due to the time the SDM takes to perform the switching operation. Under this condition, "connection is unstable" logs will be raised. Connection will be re-established, however, after the dbgent switch is complete.

Prerequisites

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

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

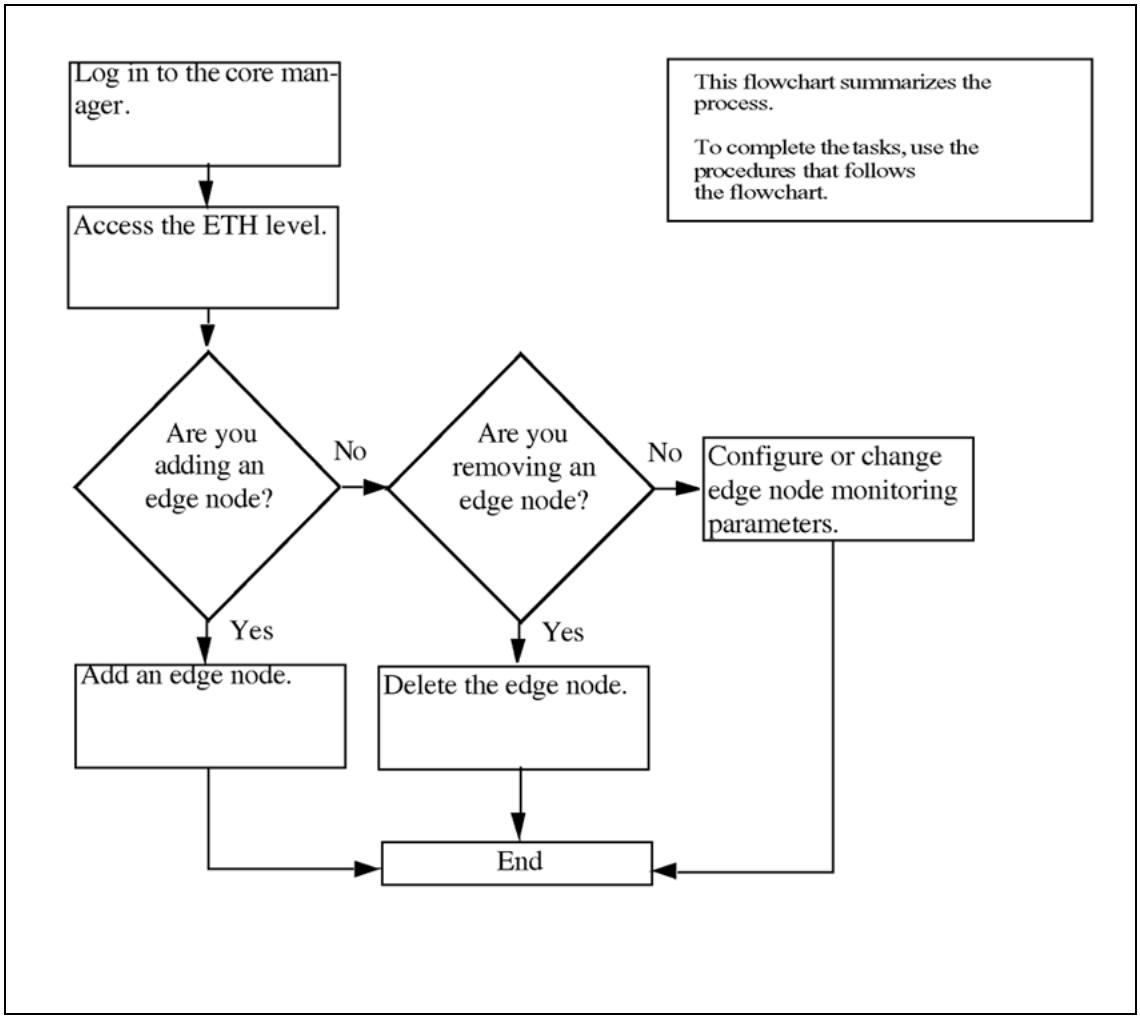
Procedures related to this procedure

Procedure	Document
Logging in to the core manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Task flow diagram

The following task flow diagram summarizes the process. To complete the tasks, use the instructions in the procedures that follow the flowchart.

Task flow for adding or removing edge nodes, or configuring edge node monitoring parameters



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

Procedures

Adding an edge node

Step	Action
	At the workstation or console
1	Log into the core manager as a user authorized to perform config-admin actions.
2	Access the ethernet (Eth) level: `sdmmtc eth`

3 Add an edge node:

```
add node
```

4 Enter the logical ethernet number for the edge node.

5 Enter a description for the edge node.

6 Enter the IP address for the edge node.

7 Confirm the add command:

```
y
```

Response:

```
Add NODE - Command complete.
```

Note: You can change the values for an edge node at any time using the Change command.

8 use this table to determine your next step.

If you want to	Do
add another edge node	go to step 3
configure the monitoring parameters for an edge node	refer to the procedure Configuring or changing edge node parameters
do neither of the above actions	you have completed this procedure

—End—

Removing an edge node

Step	Action

At the workstation or console

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

2 Access the ethernet (Eth) level by typing

```
sdmmtc eth
```

3 Remove the edge node:

```
delete node <#>
```

where

<#> is the number next to the edge node you want to delete.

4 When prompted, confirm the delete command:

y

Response:

```
Delete NODE - Command complete.
```

5 Use this table to determine your next step.

If you	Do
want to remove another edge node	go to step 3
have finished removing edge nodes	you have completed this procedure

—End—

Configuring or changing edge node parameters

Step	Action

At the workstation or console

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

2 Access the ethernet (Eth) level by typing

sdmmtc eth

3 Configure the edge node monitoring parameters:

<command>

where

<command> is:

- *Period* to specify the time interval a ping is sent (default is 1 second)
- *Failures*to specify the maximum number of failures before the link is considered failed and the active link is switched over to the other domain (default is 3 failures) or
- *Timeout* to specify the maximum time period a reply is received from a ping before the ping is considered failed (default is 1 second)

Note: If the Period value is being changed, it must be changed before the Timeout value is changed.

Example
Assuming you set the parameters as follows:

- Period = 2 seconds
- Failures = 3
- Timeout = 1 second

A ping will be sent every 2 seconds (Period). A ping reply must be received within 1 second (timeout) or the ping will be considered failed. When the number of failed pings reaches 3 (Failures), the link is considered failed and the active link is switched over to the other domain.

Note: When a ping is considered failed, a new ping is sent even if the time interval, which is 2 seconds in the example, has not yet elapsed.

4 Enter the new value and press the Enter key.

Response:
```
<command> - Command complete.
```

5 Use this table to determine your next step.

If you	Do
want to set another parameter	go to step 3
do not want to set another parameter	you have completed this procedure

—End—

Adding or removing an NTP server or peer

Purpose

Use this procedure to add or remove a Network Time Protocol (NTP) server or peer.

You can add up to three NTP servers or peers.

If you have Distributed Computing Environment (DCE) installed on your system and are deleting the last NTP server or peer, you will be prompted to set up the DCE's DTS. For this, you will need a DCE administrator password.

Prerequisites

Logging on to the CS 2000 Core Manager

You must be a user authorized to perform config-manage actions in order to perform this procedure.

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

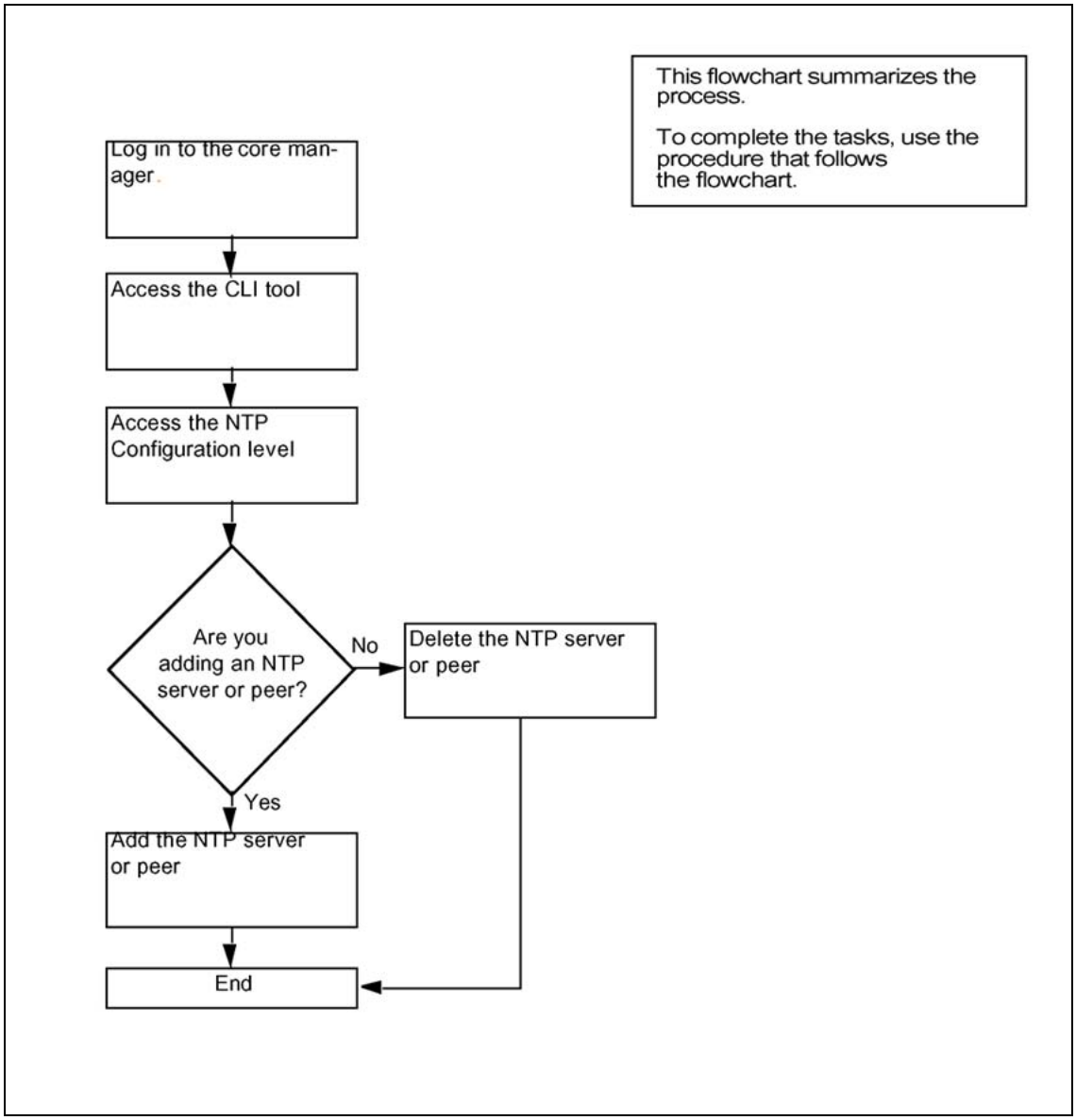
Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Task flow diagram

The following task flow diagram summarizes the software upgrade process. To complete the tasks, use the instructions in the procedures that follow the flowchart.

Task flow for adding or removing an NTP server or peer



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

Procedure

Adding or removing an NTP server or peer

Step	Action
	At the local VT100 console

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

2 Access the CLI tool

```
cli
```

3 Access the CLI configuration level:

```
<#>
```

where

`<#>` is the number next to the CLI configuration selection.

4 Access the NTP configuration level:

```
<#>
```

where

`<#>` is the number next to the Network Time Protocol configuration selection.

If you want to	Do
add an NTP server or peer	step 5
remove all NTP servers or peers	step 8
remove only a selected NTP server or peer	step 10

5 Add an NTP server or peer:

```
<#>
```

where

`<#>` is the number next to the Configure the NTP daemon selection.

6 When prompted, enter the IP address for that server or peer.

If you want to	Do
add an additional NTP server or peer	repeat this step
exit	enter `x`

You can add a maximum of three NTP servers or peers. If you attempt to add more than three, then the system will only recognize the three most recent NTP servers or peers.

A peer can act as a server.

7 When prompted, enter the hostname for the server or peer. Repeat this step until all TAG(alias) have been entered for the IP addresses previously entered.

Please do not use the IP address as an NTP hostname TAG (alias).

The TAG (alias) is not optional for the CBM.

If you want to	Do
add an NTP server or peer	step 5
exit	step 12

8 Remove all NTP servers

<#>

where

<#> is the number next to the Unconfigure the NTP daemon selection.

9 When prompted, type **y** to confirm the deletion or **n** to cancel. Go to step 12.

10 Remove only selected NTP servers or peers

<#>

where

<#> is the number next to the Remove an NTP server selection.

You can also delete an NTP server or peer using either its hostname or IP address.

11 When prompted, enter the hostname for the NTP server or peer which you want to delete.

If you want to	Do
remove an additional NTP server or peer	repeat step 11
exit	go to step 12

12 When prompted, enter **x** to exit the NTP configuration level.

13 When prompted, enter **x** to exit the CLI configuration level.

14 When prompted, enter **x** to exit the CLI tool.

15 Access the core manager RMI level to see the response.

```
sdmmtc ntp
```

16 You have completed this procedure.

—End—

Installing the FTPProxy server software

The following procedure provides instructions on how to install the FTPProxy server fileset using SWIM.

Purpose

Use this procedure to install the FTPProxy server fileset from either a tape or the core manager disk.

Prerequisites

You must have root user access to the core manager to perform this procedure.

The SWIM package provides the user interface (UI) for local core manager software installation and maintenance. You can access SWIM from the core manager maintenance interface (sdmmtc).

ATTENTION

Before you can perform an installation using SWIM, you must have the core manager base software installed on the core manager.

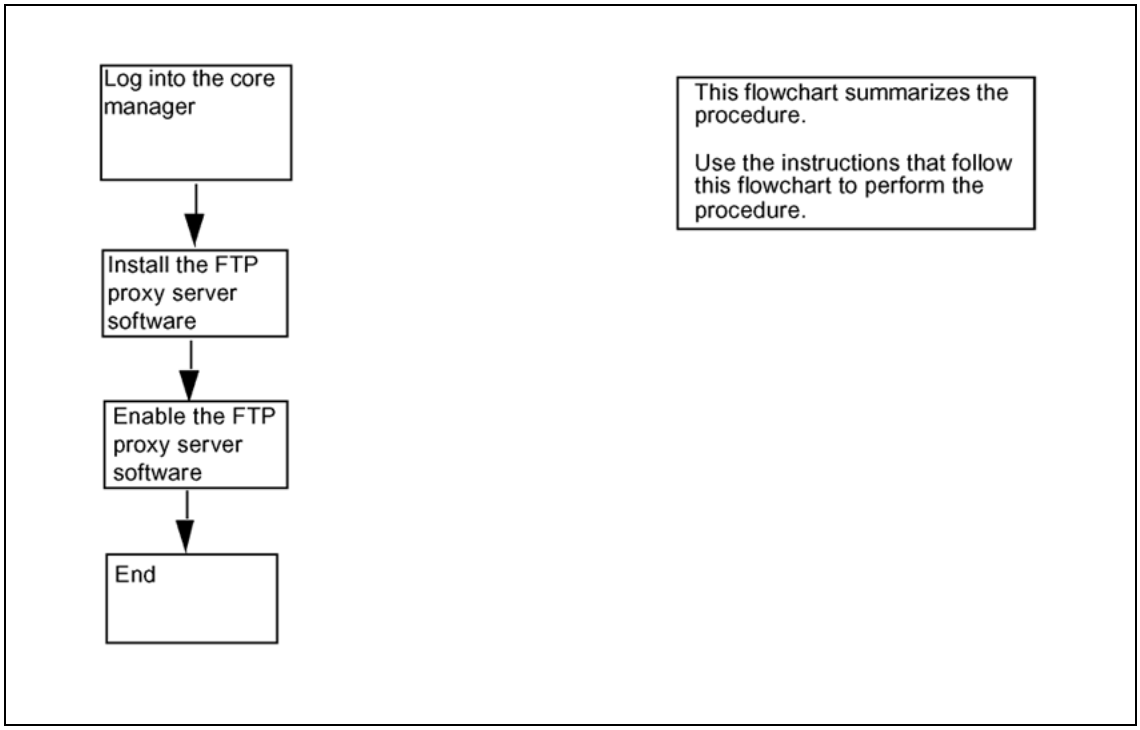
ATTENTION

Before you can perform an installation, ensure that the Secure File Transfer (SFT) application is not installed. The two applications are mutually exclusive: they cannot be on the SDM at the same time. If one application is already present, the installation of the second will fail.

Task flow diagram

The following flowchart summarizes the installation procedure for the FTP proxy server software. To complete the procedure for installing the FTP proxy server software, perform the step-action procedures that follow the flowchart.

Summary of Installing the FTPProxy server software



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

Installing the FTPProxy server software

Step	Action

At the local or remote VT100 console

1 Log into the core manager.

2 Access the maintenance interface :

```
sdmmtc
```

3 Access the SWIM level:

```
swim
```

4 Choose the FTP Proxy server fileset:

If the fileset is	Do
in a directory	step 5
on tape	step 7

5 Apply the change:

```
apply
```

6 Enter the source directory :

```
source <directory_path>
```

where

`<directory_path>` is the location of the FTPproxy server software.

Go to step 8.

7 Apply the fileset:

a. Insert the tape into the domain 0 tape drive (slot 2).

b. Type the following

```
apply 0
```

where

`0` indicates domain 0 tape drive (slot 2)

8 Install the FTP proxy server software.

a. Select the number in front of the FTPProxy fileset:

```
select <FTPProxy #>
```

b. Apply the fileset:

```
apply
yes
```

9 You have completed this procedure.

—End—

Removing an FTP proxy server application

Purpose

Use this procedure to remove an FTP proxy server when the FTP proxy application is not required on the CS 2000 Core Manager.

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

Procedure

Removing an FTP proxy server

Step	Action
	At the local or remote VT100 console
1	Log into the CS 2000 Core Manager as the maint user.
2	Access the maintenance interface: **`sdmmtc`**
3	Access the admin level: **`admin`**
4	Access the SWIM level: **`swim`**
5	Access the Details level: **`details`**
6	Select the fileset to delete: **`select <x>`** where **`<x>`** is the number next to the FTP proxy server fileset
7	Delete the fileset: **`remove`**
8	Confirm that you want to delete the fileset: **`y`** The system deletes the fileset, displaying a message when the removal is complete.

9 Exit the maintenance interface:

```
quit all
```

10 Log out from the core manager:

```
exit
```

11 You have completed this procedure.

—End—

Installing the ETA application server software on the core manager

Purpose

Use the following procedure to install a software image from a digital audio tape (DAT). This procedure applies to an initial installation of the core manager Enhanced Terminal Access (ETA) server software only.

SWIM provides the user interface for local core manager software installation and maintenance. You can access SWIM from the core manager maintenance interface.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Procedure

Installing the ETA application server software on the core manager

Step	Action
	At the local or remote VT100 console
1	Log into the core manager as a user authorized to perform config-admin actions.
2	Access the maintenance interface:

```
sdmmtc
```

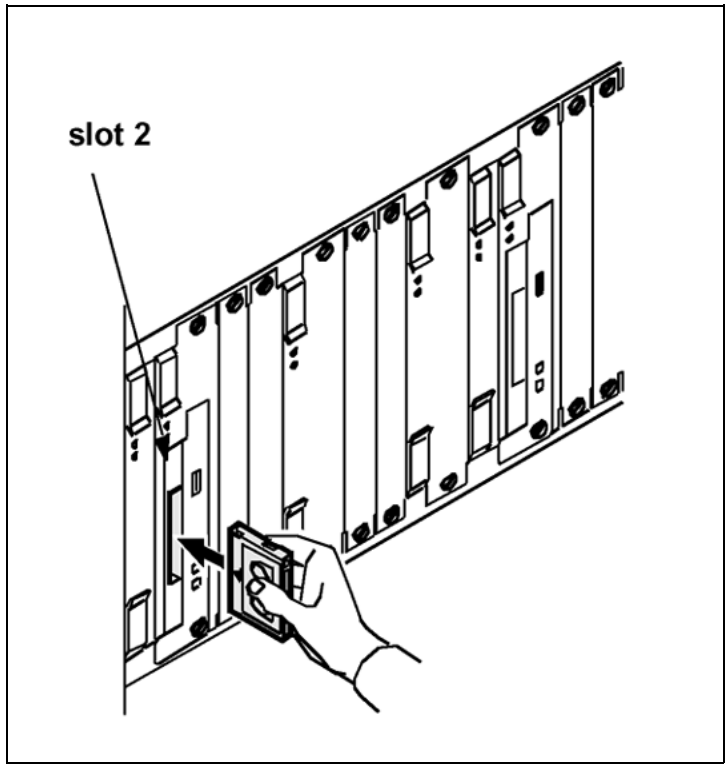
3 Access the SWIM level:

```
swim
```

4 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	insert the CS2E0006 6.x (1 of 1) tape in slot 2 as shown in the following figure, then go to step 5 ***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.
a directory	step 5

Inserting the tape into the domain 0 tape drive (slot 2)



5 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	list the filesets by typing apply 0 and pressing the Enter key
a directory	list the filesets by typing apply <directory path> and pressing the Enter key

6 Select the Enhanced Terminal Access fileset:

```
select <n>
```

where

`<n>` is the number next to the Enhanced Terminal Access fileset

7 Apply the selected fileset:

```
apply
```

8 Confirm the Apply command:

```
y
```

9 You have completed this procedure. To configure the software, refer to the procedure "Configuring the ETA application server software" (page 120).

—End—

Configuring the ETA application server software

The following procedure provides instructions on how to configure the ETA application server software using SWIM.

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

Configuring the ETA application server software

Step	Action

At the core manager:

1 Log into the core manager as the root user.

2 Access the core manager maintenance interface:

```
sdmmtc
```

The system displays the top menu level of the Maintenance interface.

3 Access the SWIM level:

```
swim
```

4 Select the Config option in the SWIM menu:

```
config
```

The system displays the Config menu, which lists the filesets available for configuration.

Example response:

```
# Fileset Description       Status
1 Enhanced Terminal Access  Unconfigured
2 Secure File Transfer      Secure and
Normal FTP Access
3 Exception Reporting       Configured
```

5 Execute the unconfigured interactive configuration scripts:

```
config <n>
```

where

<n> is the number next to Enhanced Terminal Access

If DCE has been commissioned, the following prompt appears:

```
Please enter the DCE administrator id:
```

```
[sdm_admin]
```

If DCE is	Do
commissioned	press the Enter key - you have completed this procedure
not commissioned	step 6

6 The system prompts you to enter a DCE administrator name. To accept the default DCE account (sdm_admin), press the Enter key, or enter another DCE administrator account.

Example response:

```
Enter the password for the DCE administrator sdm_admin:
```

> ***Note:*** You can also type another DCE account with administrative privileges (cell_admin).

7 Enter the DCE administrator password.

The system configures Enhanced Terminal Access and returns you to the Config menu level.

8 Exit the core manager maintenance interface:

```
quit all
```

9 Log out from the core manager:

```
exit
```

10 You have completed this procedure.

—End—

Starting the ETA server on the core manager

Purpose

The ATA and Enhanced Terminal Access (ETA) clients run on any remote workstation that is configured in the DCE cell. Along with the ETA server on the core manager, the ATA and ETA clients provide secure terminal access to the MAP/CI terminal and the core manager sessions. ATA and ETA clients cannot access the ETA server until the ETA server is installed.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Before you begin this procedure, you must complete the installation procedures described in "Configuring the ETA application server software" (page 120).

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

Procedure

Starting the ETA server on the core manager

Step	Action
	At the local or remote VT100 console
1	Log into the core manager as a user authorized to perform config-manage actions.
2	Access the maintenance interface:

```
maint:  sdmmtc
```

3 Access the application (Appl) level:

```
appl
```

4 Locate the Enhanced Terminal Access application.

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, busy it:

```
bsy <n>
```

where

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

6 Start the ETA application:

```
rts <n>
```

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 core manager. If DCE is not in service, Enhanced Terminal Access will be off-line.

7 You have completed this procedure.

—End—

Configuring a core manager in a DCE cell

Application

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. Inter-operation 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 be running on the DCE server machines.

Nortel provides NULL and NTP time providers that can be added to DCE servers. To add a provider, refer to the procedure "Adding a NULL or NTP time provider on a DCE server" (page 132).

ATTENTION
You must be a trained Distributed Computing Environment (DCE) system administrator with experience in DCE administration procedures to perform this procedure.

ATTENTION
If you use the default sdm_admin or cell_admin account, the system sends the administrative user's password in clear text across the network when you use telnet to access the core manager from another computer. Nortel recommends that you execute the command from a computer attached to the core manager console port to maintain password security.

ATTENTION
If the default sdm_admin account you are using does not exist, you can continue this procedure using the cell_admin account. You can leave this procedure to create an sdm_admin account, and return to this procedure. To create an sdm_admin account, use the Distributed Computing Environment Creating SDM administration account procedure.

ATTENTION
Nortel recommends that you configure all your core manager nodes within the same DCE cell. core manager client applications using DCE cannot communicate with core manager nodes configured in a different DCE cell.

Purpose

Perform this procedure when you want to configure or reconfigure the core manager in a DCE cell.

Use either of the following DCE accounts to perform this procedure:

- sdm_admin account (default), or any other account that is in the sdm-admin DCE group
- cell_admin account (master administrator)

If you are using the sdm_admin account, or any other account that is part of the sdm-admin group (to be referred to and used as the sdm_admin account), you must know the password created during the procedure "Creating an administration account" in the Security and Administration document. If you are using the cell_admin account, you must know the password chosen by the administrator when the cell was first commissioned.

Both the sdm_admin and the cell_admin accounts have the required privileges to make changes to the DCE cell. However, the sdm_admin account functions as a sub administrator. The sdm_admin account has limited privileges for the purpose of performing core manager-related administration tasks within the DCE cell.

Refer to the DCE Creating SDM administration account procedure for details about:

- how to create an sdm_admin account
- which activities the sdm_admin account can perform

If the default sdm_admin account you use to perform this procedure does not exist, you can use the cell_admin account instead. You can also exit this procedure and go to the DCE Creating an SDM administration account procedure to create the sdm_admin account, then return to this procedure.

Prerequisites

When you install a core manager you must configure the core manager in the DCE cell to function correctly. This procedure requires that the DCE cell be in operation.

To configure the core manager in a DCE cell, you must perform the following action:

- log on as the root user to the core manager you want to configure
- provide an account name of a DCE administrator account (sdm_admin or an equivalent account name), its password, and all other parameters required when running the "sdmconfig" program.

  Note 1: You cannot commission DCE until after you have commissioned the LAN. If you try to commission DCE before commissioning the LAN,

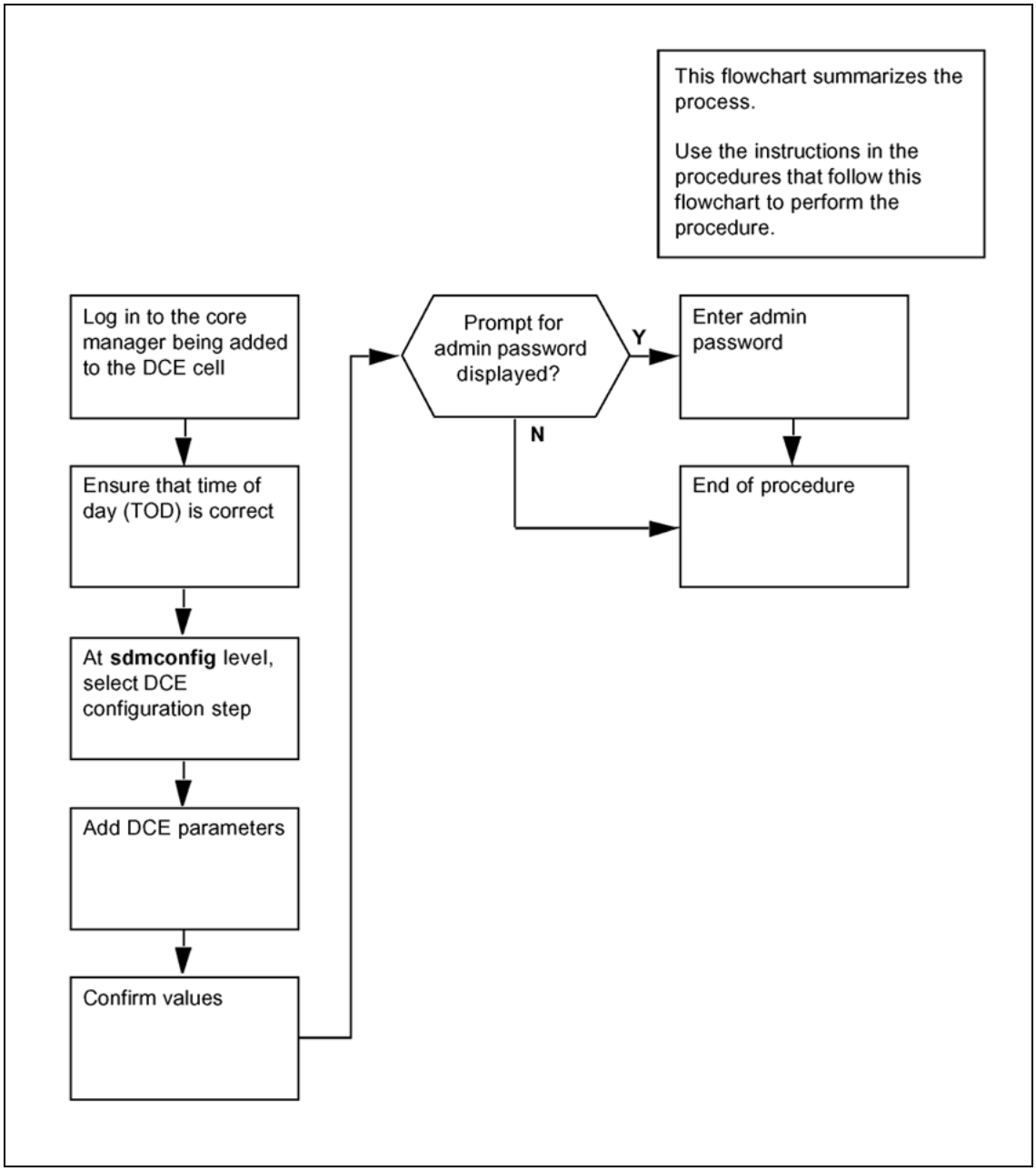
the system displays an error message. For information about LAN commissioning, refer to the procedure "Commissioning SDM-LAN connectivity".

Note 2: If you are configuring NTP with DCE on the core manager, the Distributed Time System (DTS) component of DCE will not be configured. Therefore, it is recommended that you configure NTP before you configure DCE.

Task flow diagram

The following task flow diagram provides an overview of the process. Use the instructions in the procedures that follow the flowchart to perform the task.

Task flow for Configuring a core manager in a DCE cell



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

Procedure

Configuring a core manager in a DCE cell

Step	Action

At the local or remote VT100 console

1 Log in as the root user to the core manager you are adding to the DCE cell.

2 Display the time of day (TOD) of the core manager:

```
date
```

3 Compare the TOD displayed in step 2 with the TOD obtained from a reference time signal, adjusted for the core manager time zone. A reference time signal can be obtained either from a machine with an operating NTP server or from a public time service offered by radio or telephone in your area.

After you have compared the TODs, refer to the following table to determine your next step.

If the TOD	Do
is within 5 min. of the reference time	step 5
is not within 5 min. of the reference time	step 4

4 Set the TOD of the core manager to the time provided by the reference time signal:

```
date <mm><dd><HH><MM>
```

where

<mm> = month
<dd> = day
<HH> = hour
<MM> = minute

5 Start the commissioning tool:

```
sdmconfig
```

The system displays the Commissioning Status Menu.

6 Select the DCE configuration step from the status menu:

```
step <n>
```

where

`<n>` is the menu number next to the DCE configuration option.

Response:

The system displays the DCE configuration screen.

7 The following table describes the required information for DCE commissioning parameters. Ensure that you know the information in the table, and go to step 8.

Note: The order in which the fields are prompted can vary from the order shown in the table.

Field name	Mandatory	Description
DCE cell name	Yes	
DCE administrator principal name	Yes	
Password for DCE administrator	Yes	
Hostname of the master security server	Yes	
Hostname of the master CDS server	Yes	
IP address of the master security server	Yes	
IP address of the master CDS server	No	Required only if hostname of security and CDS servers are different
LAN profile name for the core manager	Yes	The name of the DCE LAN profile that supports the part of the cell where the core manager exists. The LAN profile defines the local DTS servers that provide time synchronization for DCE nodes. For a small DCE cell, you can select the default LAN profile (lan-profile). All nodes in the cell use the same set of local DTS servers.
Alarm masters failure	Yes	
Alarm replica failures	Yes	
Minimum number of DTS servers	No	Required only if NTP is not configured

8 Begin adding DCE:

```
add
```

System response:

The system displays a prompt for each DCE parameter.

If you want to	Do
add a parameter	type the required information for the parameter, and press the Enter key. When you have entered the information for all required parameters, go to step 9.
acknowledge any information or warning messages	press the Enter key, and continue with the procedure
exit the procedure at any time	type **abort**, and press the Enter key

9 When you have entered the information for all required parameters, the system displays a message that prompts you to confirm the values.

Example system response:

```
Currently, there are no configured DCE components.
Attempting to add components: rpc sec_cl cds_cl dts_cl

          Cell name:                 sdm.ver.net
          Administrator principal:   cell_admin
          Security server hostname:  wcary2pj
          Security server IP:        47.135.213.68
          CDS Server hostname:       wcary2pj
          LAN profile:               lan-profile
          Alarm masters failure:     Y
          Alarm replica failures:    N
          Min DTS servers:           3

Proceed with these values?
Enter Y to confirm, N to reject, or E to edit:

>
```

10 Use this table to determine your next step.

If you want to	Do
confirm (proceed with) the values	go to step 11
reject the values	type **n**, and press the Enter key. To repeat the procedure, return to step 7. To exit the procedure, type **abort** or **quit all**.
edit (change) a value or values	type **e**, and press the Enter key. Change the values, and return to step 9.

11 Confirm the values:

```
y
```

If the system	Do
displays a prompt for administrator password	enter the password, press the Enter key, and go to step 12
does not display a prompt for an administrator password	step 12

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

If the system	Do
detects an abnormal condition that requires extra parameters to be entered, and displays a warning message	press the Enter key, enter the information for the extra parameters (pressing the Enter key after each entry), and return to step 9
displays other warning messages	press the Enter key
displays the message `"Add - Command complete."`	wait for the DCE status to change *from* "-" *to* ".", and go to step 13

13 You have completed this procedure.

—End—

Adding a NULL or NTP time provider on a DCE server

Purpose

Use this procedure to commission a NULL or NTP time provider for your core manager.

ATTENTION

You must be a trained Distributed Computing Environment (DCE) system administrator who knows DCE administration procedures to perform this procedure.

ATTENTION

The NULL and NTP provider tools should be added only to a system that is operating a DTS server. The tools are not required for systems that operate a DTS client. Before you can add the tools, the following fileset must be installed on the core manager: "DCE DTS Time providers for global server" (SDM_DTS_PROVIDERS.dts-19.X.X.X.tape).

ATTENTION

This procedure is valid only for machines that are running DCE 3.1 or 3.2 that are configured as DTS servers (not providers).

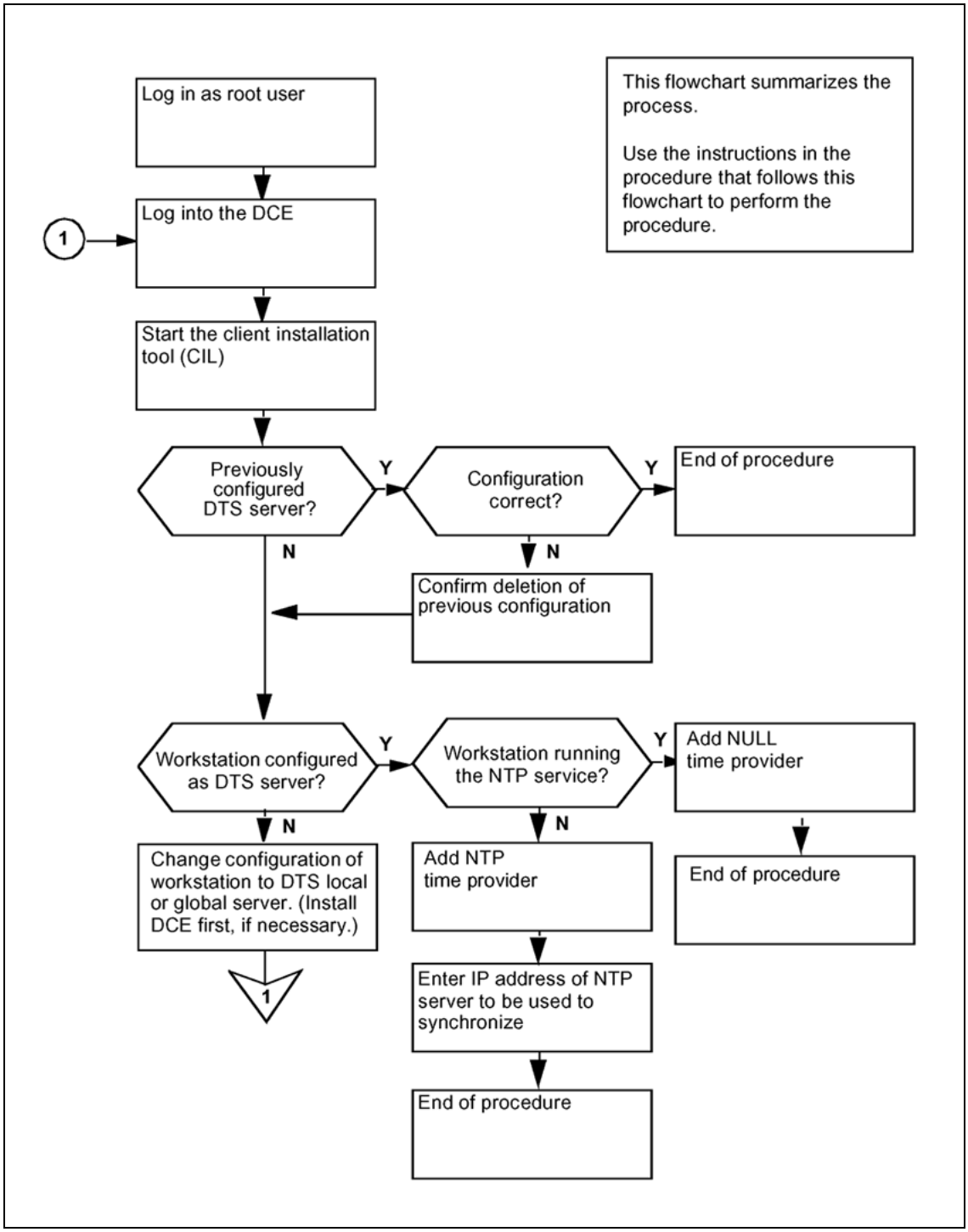
Prerequisites

Before performing this procedure, you must install the client installer and launcher (CIL). Refer to the procedure "Installing CIL on a client workstation" (page 170).

Task flow diagram

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

Task flow for Adding a NULL or an NTP time provider on a DCE server



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

Adding a NULL or an NTP provider on a DCE server

Step	Action

At the workstation where the DTS server is operating

1 Log in as the root user.

2 Log into the DCE:

```
dce_login cell_admin
```

3 Enter the cell_admin password.

4 Start the client installation tool (CIL):

```
/sdm/cil
```

Response:

The system prompts you to enter the IP address of the core manager DTS Provider fileset

5 At the prompt, enter

```
<ip_address>
```

where

<ip_address> is the address of the core manager where the DTS Provider fileset is installed

Response:

The system displays the list of client filesets on the core manager.

6 Select the DTS Provider fileset:

```
select <n>
```

where

<n> is the number of the DTS Provider fileset to be added

7 Apply the selected fileset:

```
apply
```

Response:

The system displays the IBM License Service agreement and limitations and the following prompt.

```
Do you agree with the above limitations, and do you
have a valid license to run IBM Distributed Computing
Environment for Solaris Base Services on this machine?
[Y/N]
```

8 Confirm the acceptance of the IBM License Service agreement:

```
y
```

Response:

The system determines if a DTS server was previously configured on the workstation, and displays the appropriate message.

If the system displays	Do
a message that starts with "A DTS time provider was previously configured..."	step 9
any other message	step 11

9 The system displays the details of the current configuration for the DTS time provider, including the type or provider (NULL or NTP) and any relevant parameters, and prompts you to erase the previous DTS (DCE) server configuration. After you have examined the details of the current configuration, use the following table to determine your next step.

If the configuration is	Do
correct	type **n**, press the Enter key, and go to step 10
incorrect, or if you are unsure	type **y**, and go to step 11

10 The system displays the following response:

```
No modifications made to DTS time provider
configuration.

SDM Client software installation done.
```

Go to step 18.

11 The system determines whether the workstation is configured as a DTS global or local server, and displays the appropriate message. Use the following table to determine your next step.

If the system displays a message that starts with...	Do
"This machine is running a DTS server..."	step 12

If the system displays a message that starts with...	Do
"This machine is running a DTS client..."	type **n**, and press the Enter key. Using DCE configuration commands, change the DTS configuration of this machine to a DTS local or global server, and return to step 2.
"This machine isn't running any DTS software at the moment..."	type **n**, and press the Enter key. Install and configure DCE on the workstation. Configure DTS to be a global or local server, and return to step 2.

12 The system determines whether NTP is configured and operational on the workstation, and displays the appropriate message. Use the following table to determine your next step.

If the system displays a message that starts with...	Do
"The NTP daemon (xntpd) is currently running on this machine..."	step 13
"Select the type of DTS time provide you want to configure..."	step 15

13 The system displays the following prompt:

```
The NTP daemon (xntpd) is currently running on this machine.
It appears that the daemon is working properly.
The command 'ntpq -p' shows at least one server that has a
good stratum and an offset of less than 10 seconds.
The NTP DTS time provider (dts_ntp_provider) cannot co-exist
with an NTP daemon, but the NULL DTS time provider
(dts_null_provider) can, and is recommended.

Do you want to proceed with the installation of NULL DTS
time provider [Y/N]?
```

14 To confirm the installation of the NULL time provider, enter

y

Response:

```
Installation of NULL DTS time provider completed
successfully.

SDM Client software installation done.
```

Go to step 18.

15 The system displays the following prompt:

```
Select the type of DTS time provider that you want
to configure:
1 - NTP (recommended), provides time synchronization for DCE
by contacting a remote NTP server. You will need to provide
by the hostname or address of the NTP server later.
2 - NULL, provides time synchronization for DCE by
using the local clock of this machine as the reference.
Should only be used if the local clock is synchronized
to a reference signal via some mechanism. Otherwise, never
setup more than one NULL time provider in a cell, nor put
machines that are synchronized via NTP in that cell.
```

16 To select an NTP time provider, enter

1

Response:

```
Enter the hostname or IP address of the NTP server that
will be used to synchronize, or "abort" to exit:
```

17 Enter

<ip_address>

where

<ip_address> is the address of the NTP server with which you want to synchronize

Response:

```
Installation of NTP DTS time provider completed
successfully.

SDM Client software installation done.
```

18 You have completed this procedure.

—End—

Configuring or reconfiguring a node within a DCE cell

Purpose

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.

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 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.

ATTENTION
You must be a trained Distributed Computing Environment (DCE) system administrator to perform this procedure.

ATTENTION
This procedure does not apply if you are configuring a DCE master server. To configure a DCE master server, refer to your DCE vendor's documentation.

Use this procedure to configure a new node or to reconfigure an existing node within a DCE cell. This procedure updates the pe_site file for each client or server within a DCE cell. The pe_site file contains the IP addresses and other binding information for both master server and backup server.

This procedure also replicates the CDS directories that a core manager application needs from the master server to the backup server.

Prerequisites

ATTENTION

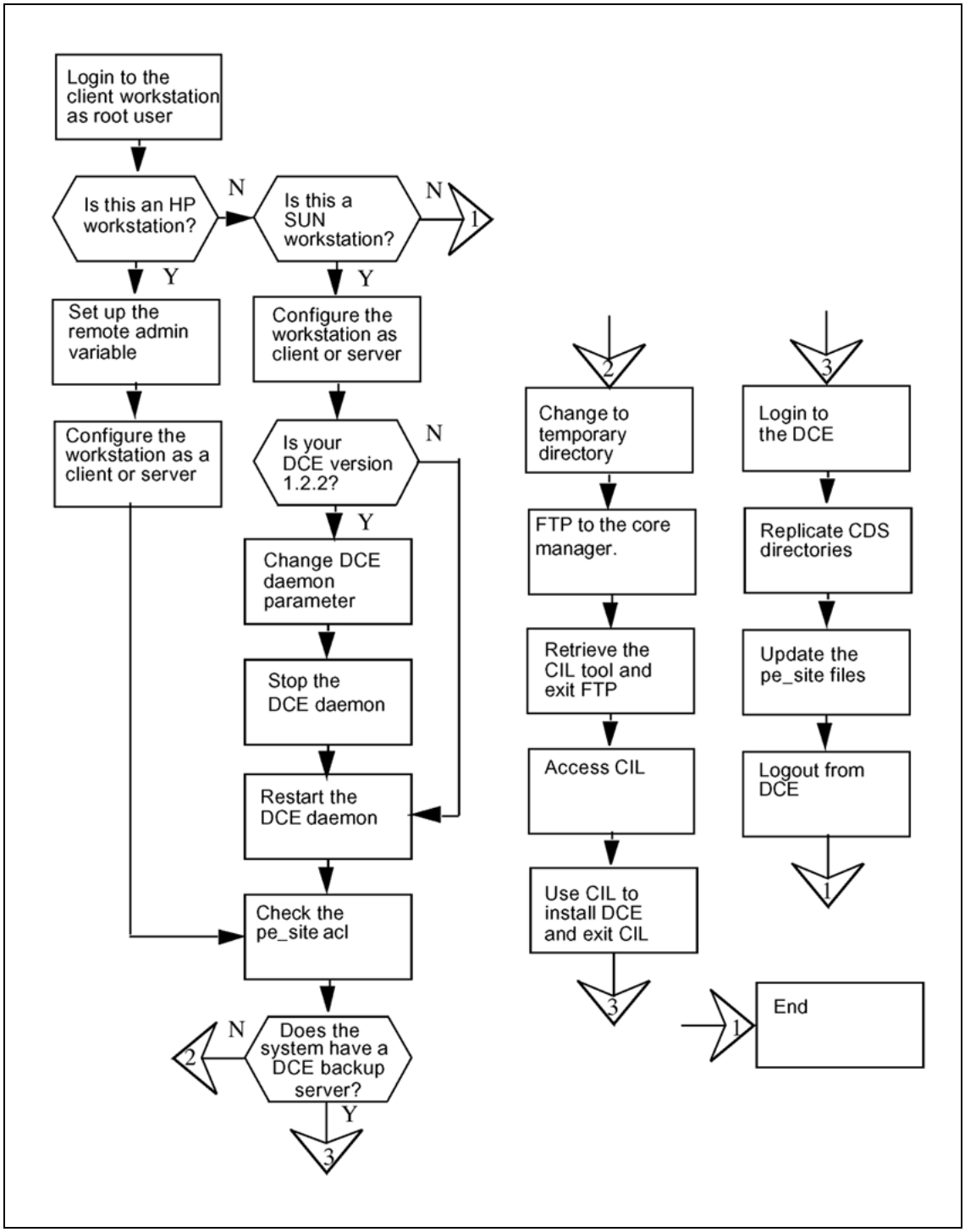
This procedure can only be performed if your operating system is HP-UX or SunOS. If you are using a different operating system, do not attempt to perform this procedure.

If your operating system is not HP-UX or SunOS, contact your next level of support.

Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedures that follow the flowchart to perform the tasks.

Task flow for configuring or reconfiguring a node within a DCE cell



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

Procedures

Configuring or reconfiguring a node within a DCE cell

Step	Action

At the client workstation

1 Login to the client workstation as the root user.

2 Identify the operating system on the workstation:

```
uname
```

Example response:

```
HP-UX
```

3 Use the following table to determine your next step.

If your O/S is	Do
HP-UX	step 4
SunOS	step 9

4 Determine your login shell:

```
finger root
```

Example response:

```
Login name: root              In real life:
000-Admin (0000)
Directory: /users/root Shell: /bin/csh
On since Jul 29 09:20:37 on pts/0 from bmerh7b
45 minutes Idle Time
No unread mail
No Plan.
```

5 Use the following table to determine your next step.

If the shell you are running is	Do
shell = csh	step 6
shell = ksh or sh	step 7

6 Set up the remote administration capability:

```
setenv REMOTE_ADMIN y
```

Go to step 8.

7 Set up the remote administration capability:

```
export REMOTE_ADMIN=y
```

8 Follow your vendor's instruction to configure the HP workstation as a DCE client or server within the DCE cell.

Go to step 15.

9 Follow your vendor's instructions to configure the SUN workstation as a DCE client or server within the DCE cell.

10 Use the following table to determine your next step.

If the DCE version you are using is	Do
DCE 1.1	step 11
DCE 1.2.2	step 12

11 Modify the DCE daemon startup option. Use a text editor to edit the file setup_state located in the /opt/dcelocal/etc/ directory. Change the line startup_dced='' to startup_dced='-b -x' and save the file.

Go to step 13.

12 Modify the DCE daemon startup option. Use a text editor to edit the file cfgarg.dat located in the /opt/dcelocal/etc/ directory. Add **-r** to the end of the line starting with " `dced:` ": for example, `dced: -b -r -t1440`. Save the file.

13 Stop the DCE daemon:

```
/etc/init.d/dce stop
```

DCE 1.2.2 Example response:

```
Gathering current configuration information...
Stop of DCE host, wmers06t, will now begin.
Stopping the DTS client...
The DTS client was stopped successfully.
Stopping the Directory client...
The Directory client was stopped successfully.
Stopping the Security client...
The Security client was stopped successfully.
Stopping RPC...
RPC was stopped successfully.
Gathering component state information...
           Component Summary for Host: wmers06t
     Component      Configuration State   Running State
Security client         Configured          Not Running
RPC                     Configured          Not Running
Directory client        Configured          Not Running
DTS client              Configured          Not Running
The component summary is complete.
Stop of DCE Host, wmers06t, was successful.
Stop completed successfully.
```

14 Start the DCE daemon:

```
/etc/init.d/dce start
```

DCE 1.2.2 Example response:

```
Gathering current configuration information...
Start of DCE host, wmers06t, will now begin.
Starting RPC...
RPC was started successfully.
Starting the Security client...
The Security client was started successfully.
Starting the Directory client...
Contacted the directory server.
Waiting up to 60 minutes for DCED registration to be
functional.
The Directory client was started successfully.
Starting the DTS client...
The DTS client was started successfully.
           Component Summary for Host: wmers06t
     Component      Configuration State   Running State
Security client         Configured           Running
RPC                     Configured           Running
Directory client        Configured           Running
DTS client              Configured           Running
The component summary is complete.
Start of DCE Host, wmers06t, was successful.
Start completed successfully.
```

15 Start the DCE control program (dcecp):

```
dcecp
```

16 Check the pe_site acl at the prompt:

```
dcecp> acl show /.:/$_h/config/hostdata/pe_site
```

Example response:

```
{unauthenticated ---r-}
{user hosts/bmerye6d/self cdprw}
{group subsys/dce/dced-admin -dprw}
{any_other ---r-}
```

17 Use the following table to determine your next step.

If the line "group sub-sys/dce/ dced-admin..."	Do
did not show on the display	step 18
is shown on the display	step 19

18 Add dced-admin acl to pe_site:

```
dcecp> acl modify / .
```

```
:/$_h/config/hostdata/pe_site -add {group subsys/dce/d
ced-adm}
```

19 Check the number of DCE backup servers:

```
dcecp> registry catalog
```

Example response:

```
/.../sdmver.bnr.ca/subsys/dce/sec/bmerye6d
/.../sdmver.bnr.ca/subsys/dce/sec/bmerha86
```

Note: Each line represents one DCE server that is currently configured to your system.

20 Use the following table to determine your next step.

If the number of DCE backup servers on the system is	Do
greater than 1	step 21
1	step 43

21 Determine if the DCE tool box exists:

```
ls -l /sdm/bin/replicate_cds_dirs
```

22 Use the following table to determine your next step.

If the DCE tool box is	Do
not present	step 23
present	step 34

23 Change to the temporary directory:

```
cd /tmp
```

Note: You can change to any directory as long as it is a directory where you can download new files.

24 Open a connection to a core manager that has at least SDMN0011 software installed. Open a file transfer protocol (FTP) connection:

```
ftp <ip-address>
```

where

<ip-address> is the IP address of the core manager.

25 Log in to the core manager as an anonymous user:

```
Name:  anonymous
```

26 The system prompts you to enter a password. Press the Enter key to continue the procedure.

27 Retrieve the CIL program:

```
ftp> get cil
```

28 Quit the connection to the core manager:

```
ftp> quit
```

29 Make the CIL program executable:

```
chmod +x cil
```

30 Start the CIL tool:

```
./cil
```

Response:

```
            SDM CLIENT SOFTWARE INSTALLATION
Enter the IP address or hostname of the SDM that you
want to download the client software from.
SDM's Address:
```

31 At the CIL menu, connect to the core manager:

```
cil> <sdm_name>
```

where

<sdm_name> is the IP address or the host name of the core manager.

32 Select the DCE tools fileset to install on the client workstation:

```
cil> select <n>
```

where

<n> is the entry number of the DCE tools fileset on the list.

Note: To deselect any fileset, select the fileset a second time. To deselect all filesets, enter select none.

33 Install the DCE tools fileset:

```
cil> apply
```

The CIL tool automatically closes after it installs the DCE tools fileset

34 Log in to the DCE using the userID of the administrator:

```
dce_login <administrator_name>
```

where

<administrator_name> is the user name of the DCE administrator.

35 Enter the administrator password.

36 Access the /sdm/bin directory:

```
cd /sdm/bin
```

37 Create the cds_cache_wan entry on the hostdata profile:

```
./create_cds_cache_wan_hostdata
```

Response:

```
cds_cache_wan host data entry created.
Returning dced to normal mode.
```

38 Update the pe_site:

```
./update_pe_site
```

Response:

Gathering information. Data retrieved from DCE security registry database, proceeding... Security registry pe_site data update is complete.

39 Replicate CDS directories:

```
./replicate_cds_dirs
```

Response:

```
The directories from master CDS server/clearinghouse
"/.../sdm/ver.bnr.ca/bmerye6d will be replicated to the
following replicas:
"/.../sdmver.bnr.ca/bmerya86_ch"
Do you want to continue?  [y]
```

40 Confirm the command:

```
y
```

Response:

```
Directory /.:/hosts has been replicated in replica CDS
bmerha86_ch
Directory /.:/subsys 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 completed
```

41 Log out of DCE:

```
exit
```

42 Log out of the client workstation:

```
exit
```

43 You have completed this procedure.

—End—

Installing the SFT server software

There are two filesets for the Secure File Transfer (SFT) application: the server fileset, and the client fileset.

The following procedure provides instructions on how to install the SFT server fileset using SWIM.

Purpose

Use this procedure to install the SFT server fileset from either a digital audio tape (DAT) or from a core manager hard disk drive.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

The following procedure applies to an initial installation of the SFT fileset only.

The SWIM package provides the user interface (UI) for local CS 2000 Core Manager software installation and maintenance. You can access SWIM from the CS 2000 Core Manager maintenance interface (sdmmtc).

ATTENTION

Before you can perform an installation using SWIM, you must have the base software installed on the CS 2000 Core Manager.

ATTENTION

If you use the DCE-based SFT application, make sure that the CS 2000 Core Manager is configured in the DCE cell before performing this procedure. Refer to the procedure "Configuring a core manager in a DCE cell" (page 124).

To add the SFT server, you must have a DCE account with administrative privileges.

ATTENTION

Risk of revealing the administrative user password.
If you use telnet to access the core manager remotely, and use the default sdm_admin or cell_admin "master administrator" account to add the SFT server, the system sends the password of the administrative user in clear text across the network. To avoid this security risk, Nortel recommends that you execute the command from a terminal attached to the core manager console port.

The DCE administrator account can create a sub-administrator account with privileges to add only core manager servers. You can use the sub-administrator account to log in to DCE to change the SFT server to DCE mode.

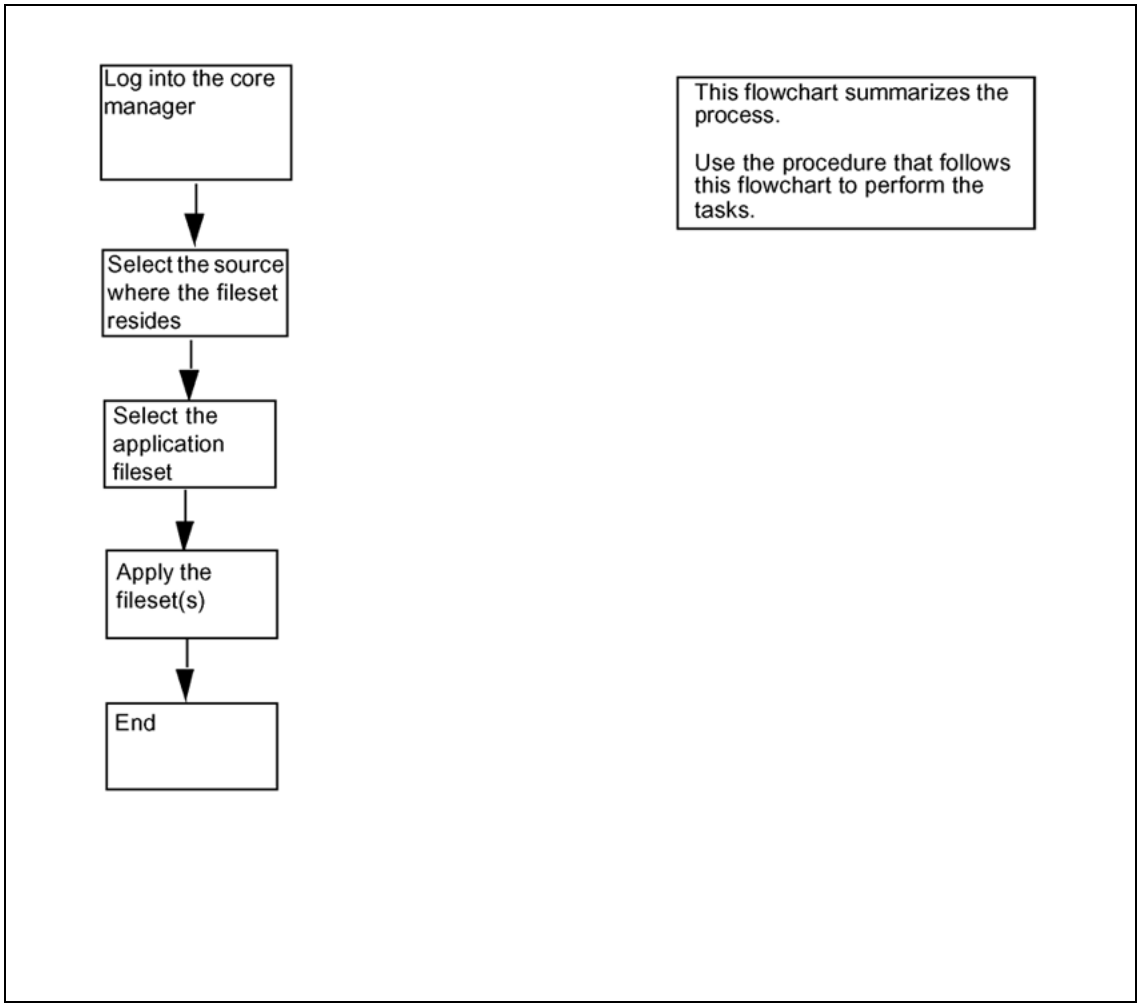
The sub-administrator account requires the following privileges:

- quota to create principals
- add permission for the core manager server organization
- add permission for the sdm-servers-using-cds group
- insert and modify access control list (ACL) permissions on the /.:/subsys/NT/SDM CDS directory

Task flow diagram

The following task flow diagram summarizes the installation process for the SFT server software. To complete the tasks in the installation process, use the instructions in the procedures that follow the flowchart.

Task flow for Installing the SFT server software



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

Procedure

Installing the SFT server software

Step	Action
	At the local or remote VT100 console
1	Log into the core manager as a user authorized to perform config-admin actions.
2	Access the maintenance interface: `sdmmtc`

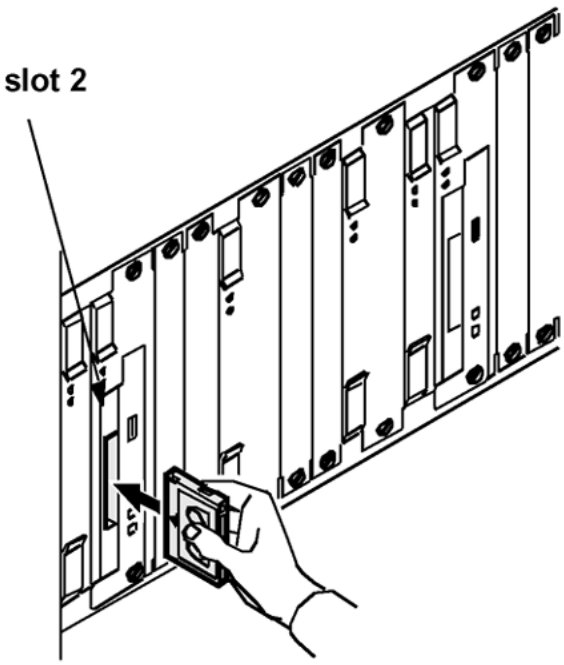
3 Access the SWIM level:

```
swim
```

4 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	insert the CS2E0006 6.x (1 of 1) tape in slot 2 as shown in the following figure, then go to step 5 ***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.
a directory	step 5

Inserting the tape into the domain 0 tape drive (slot 2)



5 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	list the filesets by typing apply 0 and pressing the Enter key
a directory	list the filesets by typing apply <directory path> and pressing the Enter key

6 Select the SFT fileset:

```
select <n>
```

where

<n> is the number next to the SFT fileset

7 Apply the selected fileset:

```
apply
```

8 Confirm the Apply command:

```
y
```

9 You have completed this procedure.

—End—

Configuring the SFT server application software

CAUTION
Risk of revealing the administrative user password
If you use telnet to access the core manager remotely, and use the default sdm_admin or cell_admin "master administrator" account to configure the SFT server to DCE mode, the system sends the password of the administrative user in clear text across the network. To avoid this security risk, Nortel recommends that you execute the command from a terminal attached to the SDM console port.

ATTENTION

For security reasons, anonymous FTP is turned off by default. Should you require anonymous FTP for a given purpose, use this procedure to enable anonymous FTP access.

If the CS 2000 Core Manager supports a CS 2000, configure the SFT server application for secure access. Using a non-secure mode can compromise the security of the CS 2000 Core Manager.

If the CS 2000 Core Manager supports a CS 2000 Compact, configure the SFT server application for anonymous access. The CS 2000 - Compact requires boot information on the CS 2000 Core Manager. Using another mode of access will cause the CS 2000 - Compact to continuously reboot.

Purpose

The following procedure provides instructions on how to configure the secure file transfer (SFT) server application software using SWIM. Perform this procedure only if the core manager did not configure the software when you applied the fileset using the procedure Installing the SFT server software.

When configuring SFT, you can enable or disable the following FTP options on the SFT server:

- anonymous FTP access to the core manager (*Anon*)
- normal FTP access to the core manager and Core (*Normal*)
- DCE-secured FTP access to the core manager and Core (*Secured*)

Anonymous FTP

Anonymous FTP access allows client workstations to access the core manager by logging in as *anonymous*, or *ftp*. The client workstation only has access to the core manager, and to limited directories and software.

If you do not have DCE installed on your network, and you are confident with your current security, you can use the anonymous FTP mode.

Anonymous FTP access is enabled by default on the core manager.

Normal FTP

Normal FTP access allows client workstations to access the core manager and the CM using the user names other than *anonymous* or *ftp*. The password is required for the login.

If you do not have DCE installed on your network, and you are confident with your current security, you can use the normal FTP mode.

DCE-secured FTP

DCE-secured FTP access allows client workstations to access the core manager and CM using the SFT client software in a DCE-secure environment.

If you have DCE installed on your network, you can take advantage of the login encryption, and use the secure access mode.

Configuring FTP options

Each option can be enabled (**Y**) or disabled (**N**) independently of the other options. The following table lists the possible combinations of options for SFT FTP configuration.

Possible combinations of options for SFT FTP

FTP Configuration	Enabled FTP option(s)	Disabled FTP option(s)
`Anon:Y;Normal:Y;Secured:Y`	Anonymous Normal Secured	
`Anon:Y;Normal:Y;Secured:N`	Anonymous Normal	Secured
`Anon:Y;Normal:N;Secured:N`	Anonymous	Secured Normal
`Anon:N;Normal:N;Secured:N`		Secured Anonymous Normal
`Anon:N;Normal:N;Secured:Y`	Secured	Anonymous Normal
`Anon:N;Normal:Y;Secured:Y`	Normal Secured	Anonymous

FTP Configuration	Enabled FTP optio n(s)	Disabled FTP optio n(s)
`Anon:Y;Normal:N;Secured:Y`	Anonymous Secured	Normal
`Anon:N;Normal:Y;Secured:N`	Normal	Anonymous Secured

When you set SFT access on the core manager, you are configuring all FTP type interaction with the core manager. SFT in secure access mode provides a secure operating environment. Anonymous or normal FTP access provides standard FTP access, which is insecure, to the core manager. To avoid sending login, password, and files unsecured over the network, enable *secured* mode and use the SFT client.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

To configure the SFT server to DCE mode, you must have a DCE account with administrative privileges. This restriction does not apply if you do not use DCE mode.

To perform this procedure, you must first install the core manager platform maintenance software and the SFT software package.

ATTENTION

If you use the sdm_admin account to perform this procedure, and the sdm_admin account does not exist, you can use the cell_admin account instead. You can also exit this procedure, and go to the procedure "Creating a DCE user" to create an sdm_admin account, then return to this procedure.

The sdm_admin and cell_admin accounts have the required privileges to make changes to the DCE cell. However, the sdm_admin account functions as a sub-administrator account with limited privileges. The sdm_admin account only performs administrative tasks related to the core manager within the DCE cell.

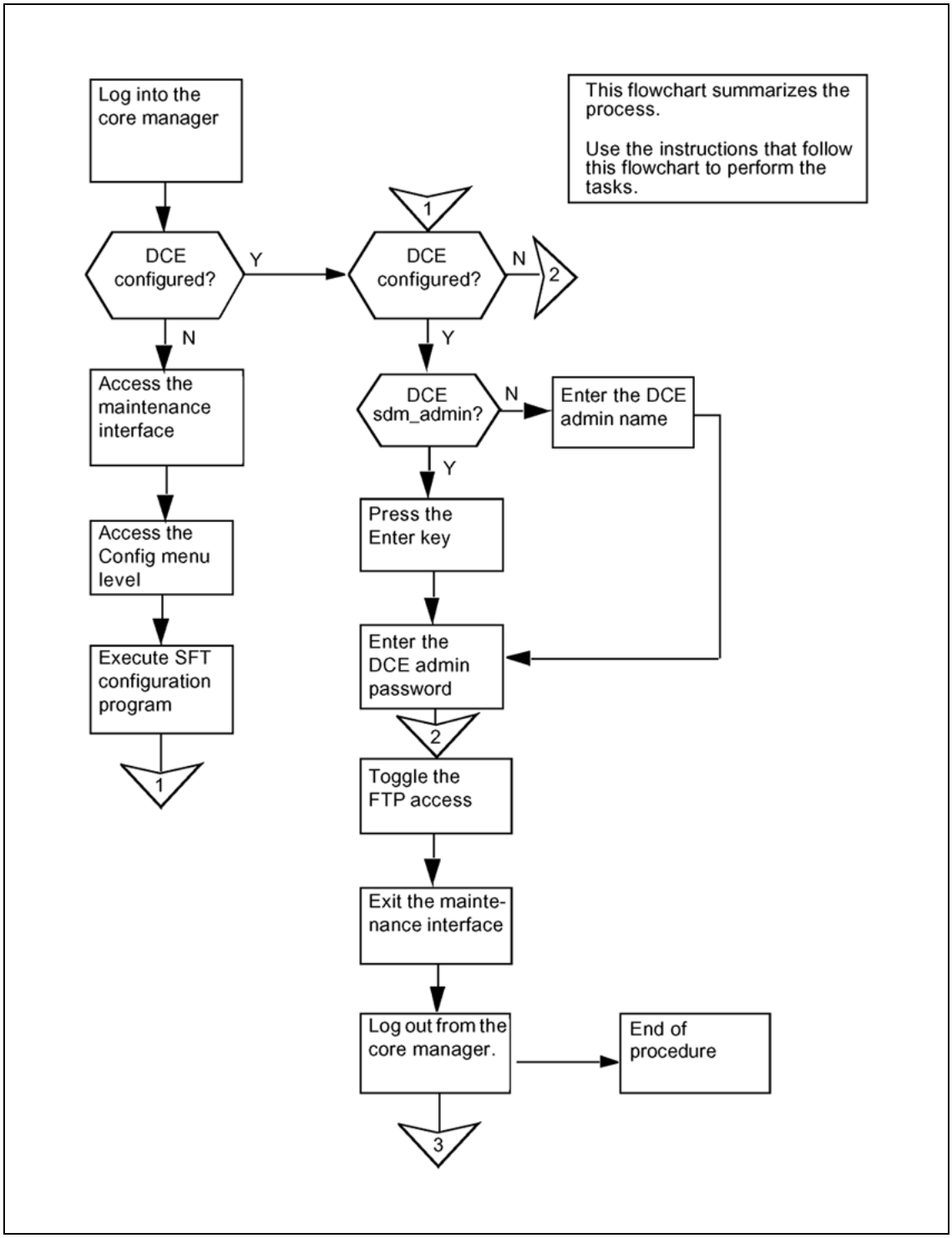
The sub-administrator account requires the following privileges:

- quota to create principals
- the ability to add permission for the core manager server organization
- the ability to add permission for the sdm-servers-using-cds group
- the ability to insert and modify access control list (ACL) permissions on the /.:/subsys/NT/SDM CDS directory

Task flow diagram

The following task flow diagram summarizes this process. Use the procedures that follow the flowchart to complete the tasks.

Task flow for Configuring the SFT server application software



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

Procedure

Configuring the SFT server application software

Step	Action

At any workstation or console

CAUTION
Risk of revealing the administrative user password
f you use telnet to access the core manager remotely, and use the default sdm_admin or cell_admin "master administrator" account to configure the SFT server to DCE mode, the system sends the password of the administrative user in clear text across the network. To avoid this security risk, Nortel recommends that you execute the command from a terminal attached to the core manager console port.

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

2 Access the SWIM level of the maintenance interface:

```
sdmmtc swim
```

Response

The system displays the top menu level of the maintenance interface.

3 Select the Config option from the SWIM menu:

```
config
```

Response

The system displays the Config menu that lists the filesets available for installation and the SFT status.

Example of response:

```
Filter: OFF

#   Fileset Description          Status
-------------------------------------------------
1   Enhanced Terminal Access     Configured

2   OM Delivery                  Configured

3   SDM Billing Application      Configured

4   Secure File Transfer         Anon:N;Normal:Y;Secure:Y

          Configuration programs: 1 to 4 of 4
```

If DCE is	Do
commissioned	step 5
not commissioned	step 7

4 Execute the unconfigured interactive configuration scripts:

`config <n>`

where

`<n>` is the number of the fileset you want to configure.

5 When prompted to enter a DCE administrator name, press the Enter key to accept the default DCE account (sdm_admin), or enter another DCE administrator account.

Example response:

```
Enter the password for the DCE administrator sdm_admin:
```

Note: You can also type another DCE account with administrative privileges (cell_admin), as described at the beginning of this procedure.

6 When prompted, enter the DCE administrator password.

Example response:

```
                        SECURE FILE TRANSFER ACCESS

Type the corresponding # to toggle the FTP access.

Type "Commit" to apply the configurations shown in the "New" column.

Type "Quit" to exit.

WARNING:Changing the SFT access will cause any current transfers to be interrupted.

#    FTP access                                  Current          New
-------------------------------------------------------------------------
1    Anonymous FTP access to the SDM             DISABLED         ENABLED
2    Normal FTP access to the SDM and CM         ENABLED          DISABLED
3    DCE-secured FTP access to the SDM and CM    ENABLED          ENABLED

SFT config >
```

Note: If you do not have DCE installed on your core manager, the system only displays options 1 and 2 on the terminal. Option 3 is not available.

7 Toggle the FTP access:

`<n>`

where

`<n>` is the number beside the FTP access in the list

When you type the number, the corresponding value in the "New" column will be toggled to indicate the changes that you made. The number can be typed multiple times.

Note: If the SFT application is either manually busy (ManB) or offline (Offl), the system displays a warning message on the terminal. The message indicates that the core manager will restart the application to change the SFT mode. Continue this procedure by typing **y**.

If you want to	Do
apply the changes	type **commit**, press the Enter key, and go to step 8
discard the changes	type **quit**, press the Enter key, and go to step 8

8 Exit the maintenance interface:

`quit all`

9 Log out from the core manager:

`exit`

10 You have completed this procedure.

—End—

Configuring the SFT client

Purpose

Use these procedures to configure the Secure File Transfer (SFT) client software.

Configuring the SFT client is a three-stage process:

- creating a DCE user
- setting an ERA value for the core manager userID
- setting the SFT permission

Prerequisites

You must have a Distributed Computing Environment (DCE) user account in order to access SFT and perform this procedure. If you do not have a DCE user account, refer to the procedure "Creating a DCE user" in the Security and Administration document.

ATTENTION

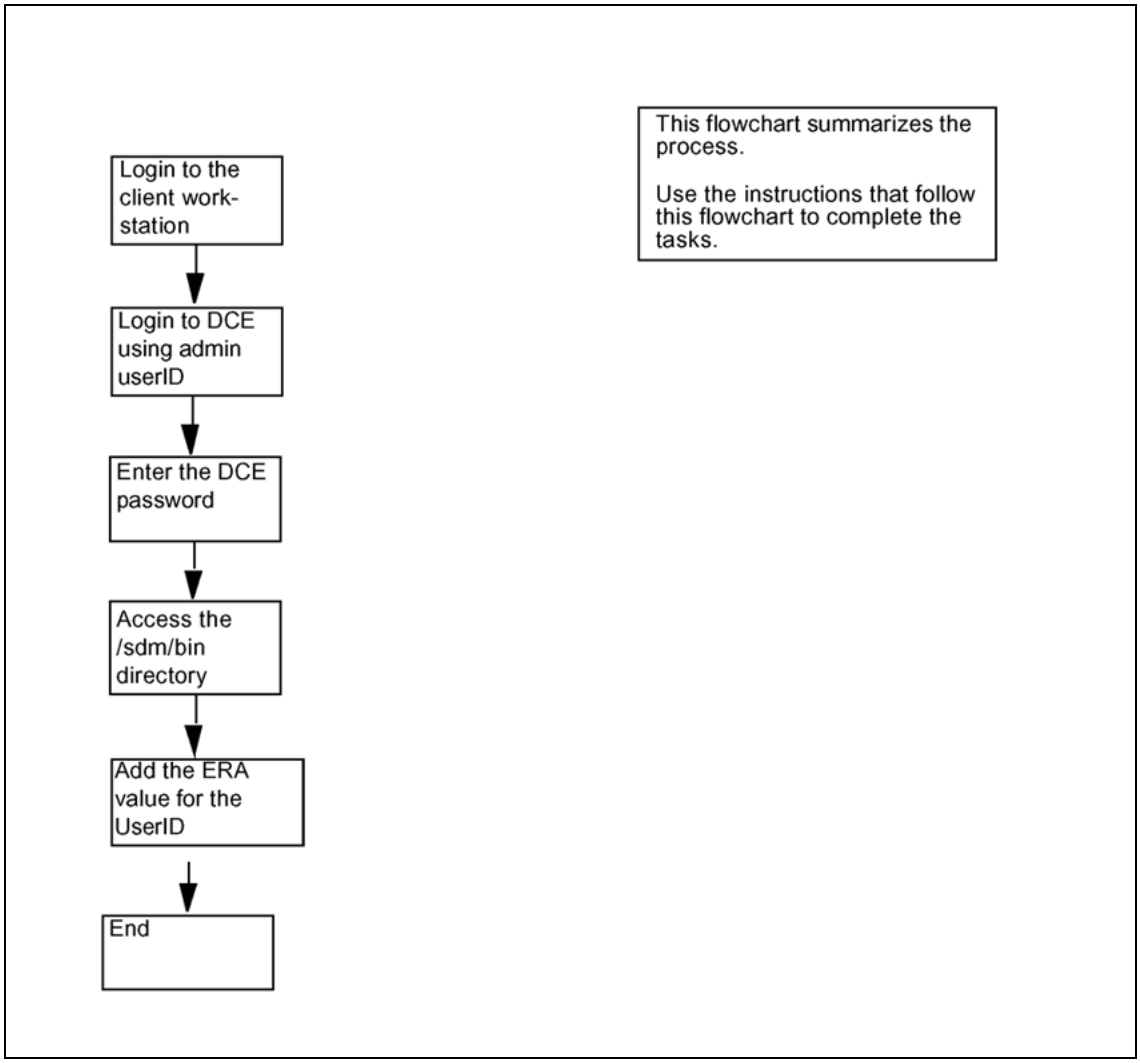
The DCE administrator must create and configure the DCE user accounts before a user can access the SFT servers using the SFT clients. If you are using SFT in FTP (non-DCE) mode, ignore this section.

Task flow diagrams

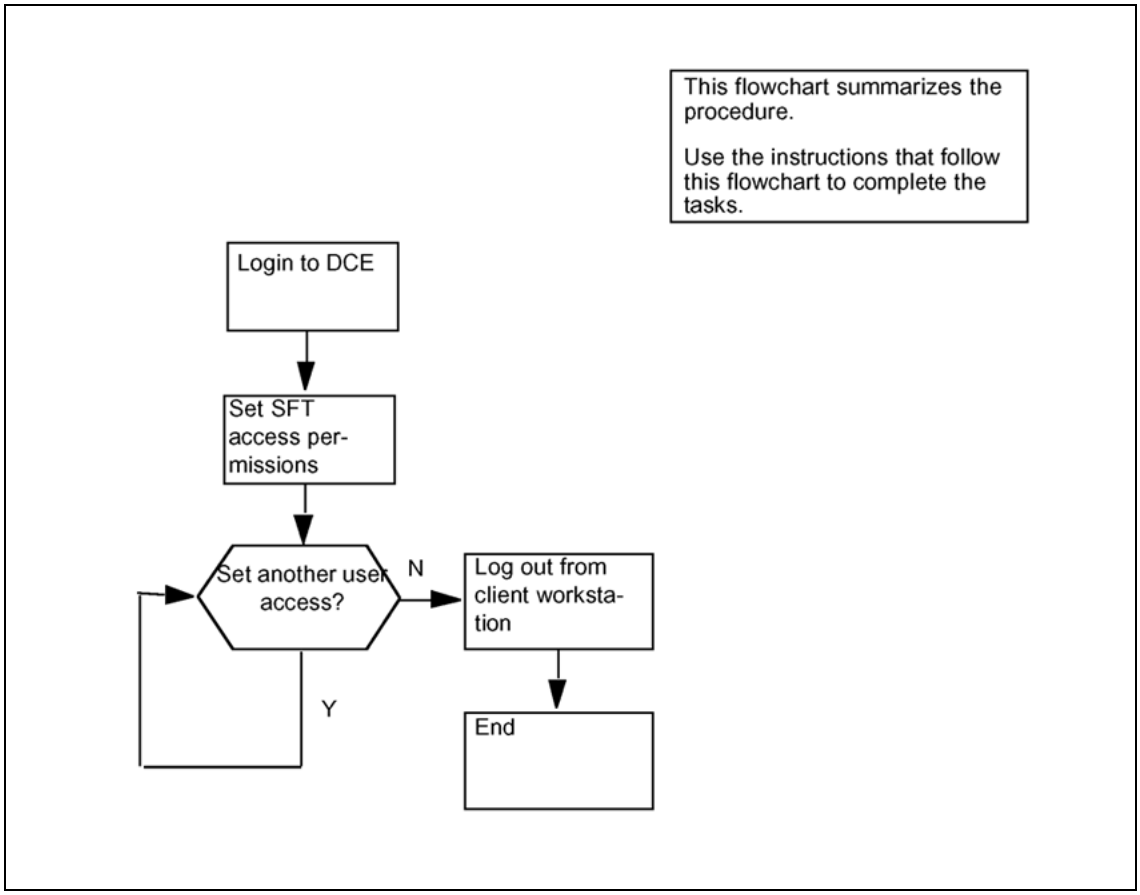
The following task flow diagrams summarize the process. Use the instructions in the procedures that follow the flow charts to complete the tasks.

- setting an ERA value for a core manager userID
- setting the SFT access permissions

Task flow for Setting an ERA value for the core manager userID



Task flow for Setting the SFT access permission



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

Procedures

Setting an ERA value

To set an ERA value for the SFT client core manager userID, use the add_sdm_userid command. When an SFT client accesses the core manager, the SFT server obtains the ERA value for that client core manager userID, and uses it to connect the client to the core manager.

Setting an ERA value for the core manager userID

Step	Action
	At the client workstation:
1	Log in to the client workstation.
2	Log in to DCE using the userID of the administrator:

dce_login <administrator_name>

where

<administrator_name> is the userID for the administrator account that you are using.

3 When prompted, enter the administrator password.

4 Access the /sdm/bin directory:

cd /sdm/bin

5 Add the ERA value for the core manager userID:

./add_sdm_userid <principal_name> <sdm_userid>

where

<principal_name> is the principal name of the DCE user account.
<sdm_userid> is the core manager userID.

Note: The core manager userID must correspond to an existing core manager UNIX account. This account must reside on all of the core manager nodes that you need to access. You cannot use SFT to access the core manager without this core manager UNIX account.

6 You have completed this procedure.

—End—

Setting the SFT access permissions

ATTENTION
The default permission is "none". If you do not perform this procedure, the user will not have access to SFT.

Setting the SFT access permissions

Step	Action

At a UNIX prompt on the client workstation

1 Log in to DCE as the DCE administrator:

dce_login <administrator_name>

where

<administrator_name> is the userID for the administrator account that you are using.

2 When prompted, enter the administrator password.

3 Access the /sdm/bin directory:

```
cd /sdm/bin
```

4 Set the SFT client access permissions for the user:

```
./set_sft_access <DCE_principal> <SFT_permission>
<type_of_access>
```

where

<DCE_principal> is the DCE userID whose access permissions you are changing
<SFT_permission> is the access permission level for the user
<type_of_access> is *none* where access is not permitted to the SFT services (default value), *sdm_only* where access is permitted to the core manager, or *sdm_cm*, where access is permitted to both the core manager and the CM

5 Use this table to determine your next step.

If you	Do
need to set SFT access for another user	step 4
do not need to set SFT access for another user	step 6

6 Log out from the client workstation:

```
exit
```

7 You have completed this procedure.

—End—

Decommissioning X.25 ports

Purpose

Use this procedure to decommission one or both X.25 ports on an UMFIO/X25 (NTRX50NN) or SYNC X25 (NTRX50FY) module.

Prerequisites

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

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

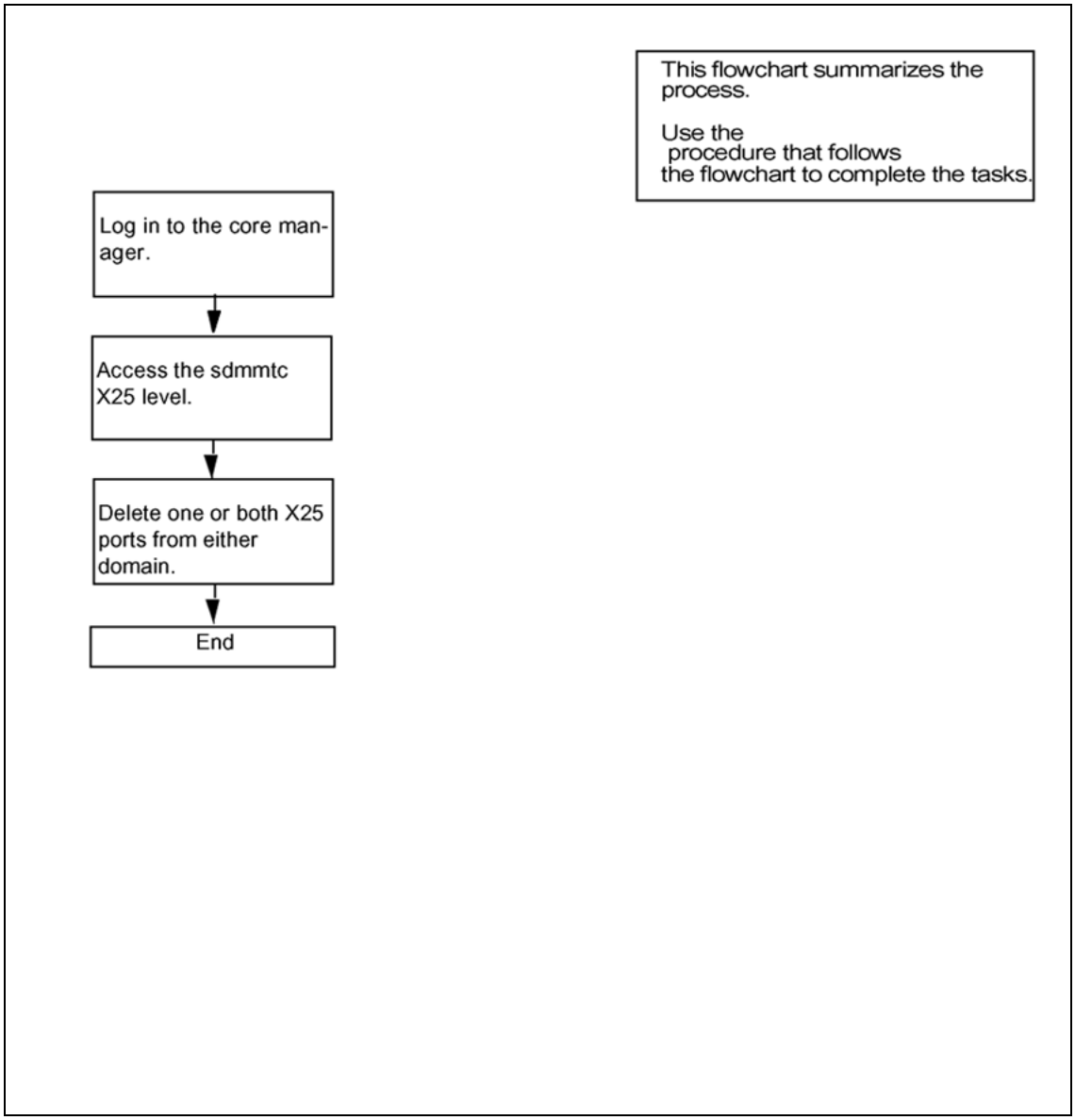
Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Task flow diagram

The following diagram summarizes the process. Use the instructions in the procedure that follows the flowchart to complete the tasks.

Task flow for Decommissioning X.25 ports



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

Procedure

Decommissioning X.25 ports

Step	Action
	At the local VT100 console

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

2 Access the X.25 level:

```
sdmmtc x25
```

3 Delete one or both X.25 ports from either domain:

```
delete <parameters>
```

where

<parameters> is the domain number of the X.25 module (0 or 1), and the port number of the X.25 module when decommissioning a single port (0 or 1) - see examples below.

Example input for both ports:

```
delete 0
```

Example input for one port:

```
delete 0 1
```

Example response:

```
This action will delete the X25 configuration of domain
0 port 1.  The X25 daemon needs to be restarted for
this activity to take effect.
Do you wish to proceed?
Please confirm ('YES', 'Y', 'NO', 'N')
```

4 When prompted, confirm that you want to delete the specified X25 configuration:

```
Y
```

Example response:

```
Delete 0 1 - Command submitted.
```

Once the delete command is complete, the port or ports you decommissioned will show a status of "OffL -" (offline)

5 You have completed this procedure.

—End—

Installing CIL on a client workstation

Purpose

Use this procedure to install the client installer and launcher (CIL) tool on a client workstation for the first time. Repeat the procedure for each client workstation.

ATTENTION

The Secure File Transfer (SFT) client software allows you to access SFT servers running in Distributed Computing Environment (DCE) mode. If you have configured all of your servers to File Transfer Protocol (FTP) mode, use standard FTP client software, and ignore this section.

Prerequisites

You must have the following information in order to perform this procedure:

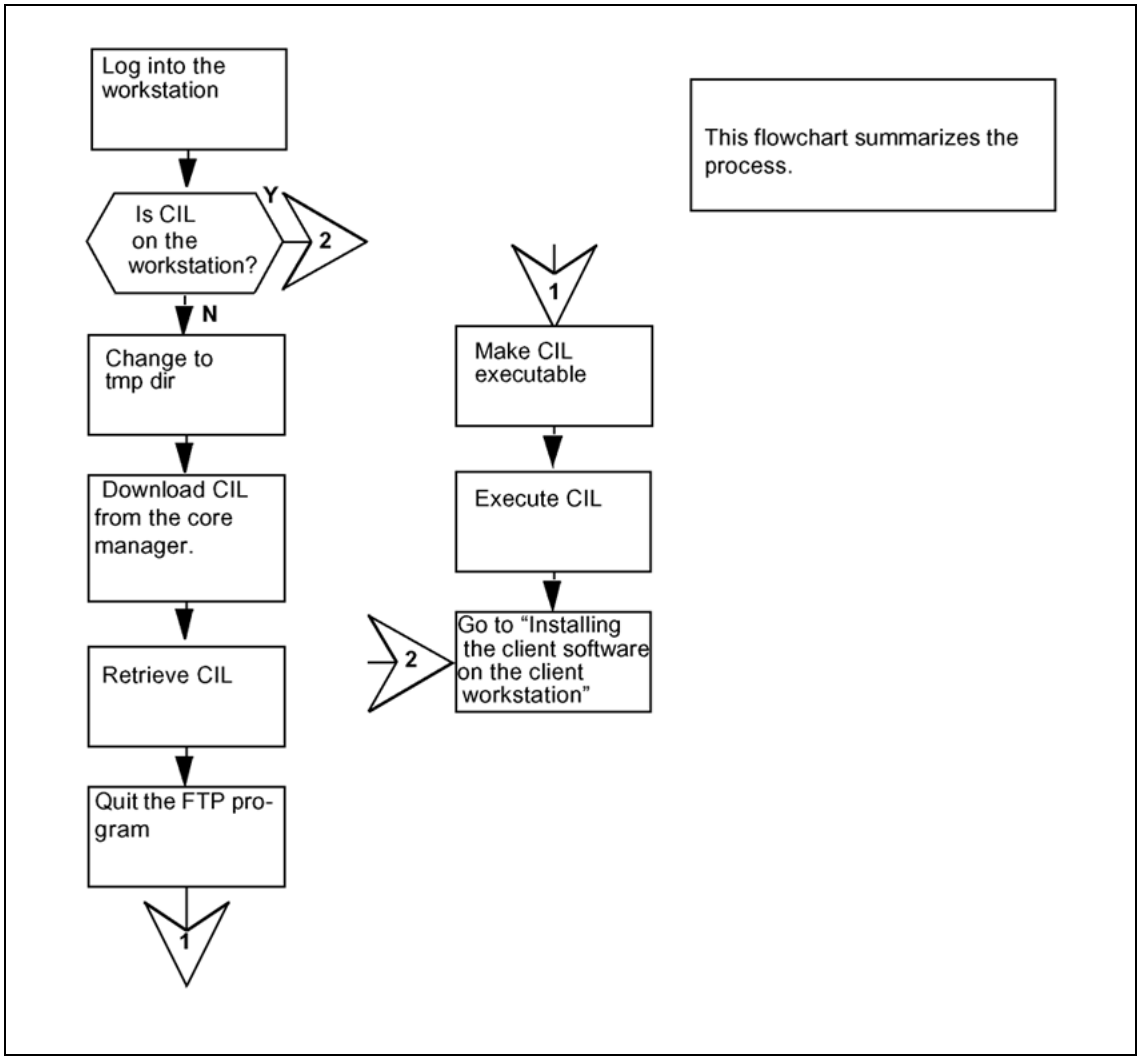
- the platform of the client workstations
- the internet protocol (IP) address of the client workstations
- the client software fileset names

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

Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Task flow for installing CIL on a client workstation



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

Procedure

Installing CIL on a client workstation

Step	Action
	At the local or remote VT100 console

CAUTION
Risk of revealing the administrative user password
If you use telnet to access the client workstation remotely, and use the default sdm_admin or cell_admin account to execute the DCE control program (dcecp) commands, the system sends the administrative user password in clear text across the network. To avoid this risk, Nortel recommends that you execute the commands from a terminal attached to the workstation console port.

1 Log into the client workstation.

2 Change to the temporary directory:

```
cd /tmp
```

Note: You can change to any directory as long as it is a directory where you can download new files.

3 Open a file transfer protocol (FTP) connection to core manager:

```
ftp <ip-address>
```

where

`<ip-address>` is the IP address of the core manager.

4 Log into the core manager as an anonymous user:

```
Name:  ftp
```

5 When prompted for a password, press the Enter key to continue the procedure.

6 Retrieve the CIL program:

```
ftp> get cil
```

7 Quit the connection to the core manager:

```
ftp> quit
```

8 Make the CIL program executable:

```
chmod +x cil
```

9 You have completed this procedure. Proceed to "Installing client software on a client workstation" (page 176).

—End—

Installing the Base Maintenance Interface software

Purpose

The following procedure provides instructions on how to install the Base Maintenance Interface software on the core manager.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Procedure

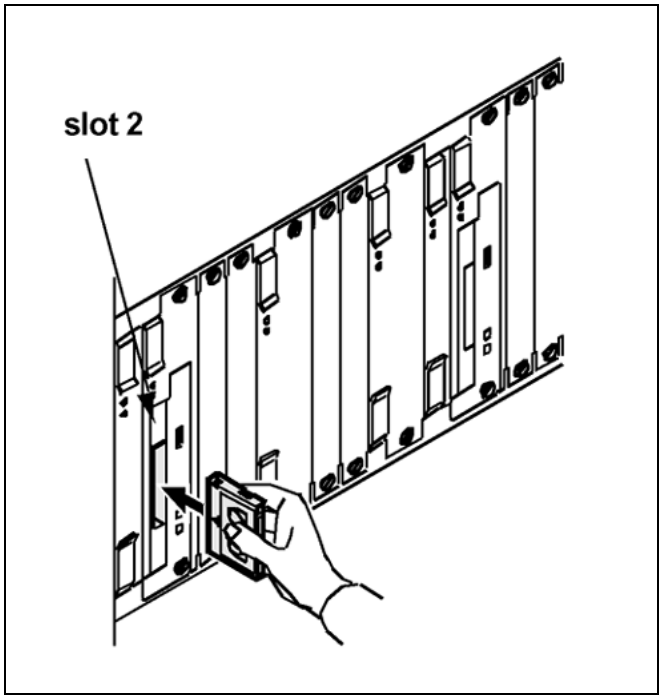
Installing the Base Maintenance Interface software

Step	Action
	At the local or remote VT100 console
1	Log into the core manager as a user authorized to perform config-admin actions.
2	Access the maintenance interface level: `sdmmtc`
3	Access the SWIM level: `swim`

4 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	insert the CS2E0006 6.x (1 of 1) tape in slot 2 as shown in the following figure, then go to step 5 ***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.
a directory	step 5

Inserting the tape into the domain 0 tape drive (slot 2)



5 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	list the filesets: `apply 0`
a directory	list the filesets: `apply <directory path>`

6 Select the SDM Base Maintenance Interface fileset:

select <n>

where

<n> is the number next to the SDM Base Maintenance Interface fileset

7 Apply the selected fileset:

apply

8 Confirm the Apply command:

y

9 Press the Enter key again to continue.

10 Access the Application level and verify the installation:

appl

Example response:

```
# Application                                  State
1 Log Delivery Service                           .
2 OM Access Service                              .
3 Table Access Service                           .
4 Exception Reporting                            .
5 ObjectStore Database Svc                       .
6 OSS Comms Svcs                                 .
7 OSS and Application Svcs                       .
8 Secure File Transfer                           .
9 Enhanced Terminal Access                       .
10 Base Maintenance Interface                    .

                    Applications showing: 1 to 10 of 15
```

In this example, the Appl level lists the SDM Base Maintenance Interface as fileset number 10. The "." value for the State column indicates that the application was automatically put in service (InSv).

11 Exit the maintenance interface:

quit all

12 You have completed this procedure.

—End—

Installing client software on a client workstation

Purpose

Use this procedure to install client software on the client workstation using the client installer and launcher (CIL) tool.

Prerequisites

Make sure you install the CIL tool on the client workstation before you install the client software. Refer to the procedure "Installing CIL on a client workstation" (page 170).

ATTENTION

The Client Common Resources fileset must be installed before installing the client filesets.

Procedure

Perform this procedure when you are installing client software on the client workstation for the first time, or installing the latest version of the client software on the client workstation.

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

Installing client software on a client workstation

Step	Action
	At the client workstation
1	Access the tmp directory where the CIL tool exists: **`cd /tmp`**

2	Invoke CIL:
	`./cil`
	Response
	`SDM CLIENT SOFTWARE INSTALLATION`
	`Enter the IP address or hostname of the SDM that you want to download the client software from.`
	`SDM's Address:`

3	When prompted, connect to the core manager: **`SDM's Address: <sdm_name>`** where

<sdm_name> is the IP address or the host name of the core manager

Example response

```
       SDM CLIENT SOFTWARE INSTALLATION
After you enter 'Apply', the selected filesets are
FTPed from the SDM to the /tmp directory.  The filesets
are then installed into the /sdm directory.  Type
'Help' for a list of commands.  Type 'Quit' to exit
this program.
Client software source: the SDM at bmerye6b
    # Fileset Name
    1 ata_client_17.0.8.0.tar.Z
    2 sft_client_17.0.8.0.tar.Z
    3 eta_client_17.0.8.0.tar.Z
    4 clientcommon_17.0.8.0.tar.Z
    5 logdelivery_client_17.0.8.0.tar.Z
                    Client Software: 1 to 5 of 5
cil>
```

4 Use the following table to determine your next step.

If the Client Common Resources fileset is	Do
not installed	step 5
installed	step 7

5 Select the Client Common Resources fileset:

cil> select <n>

where

<n> is the number next to the Client Common Resources fileset

Note: To deselect any filesets, select the fileset a second time. To deselect all filesets, type *select none*.

6 Install the selected fileset:

cil> apply

7 Select the filesets to install on the client workstation:

cil> select <n>

where

<n> is the number next to the fileset you want to install.

Note: To deselect any filesets, select the fileset a second time. To deselect all filesets, type *select none*.

8 Install the selected fileset:

```
cil> apply
```

9 You have completed this procedure.

—End—

Installing the logreceiver tool on a client workstation

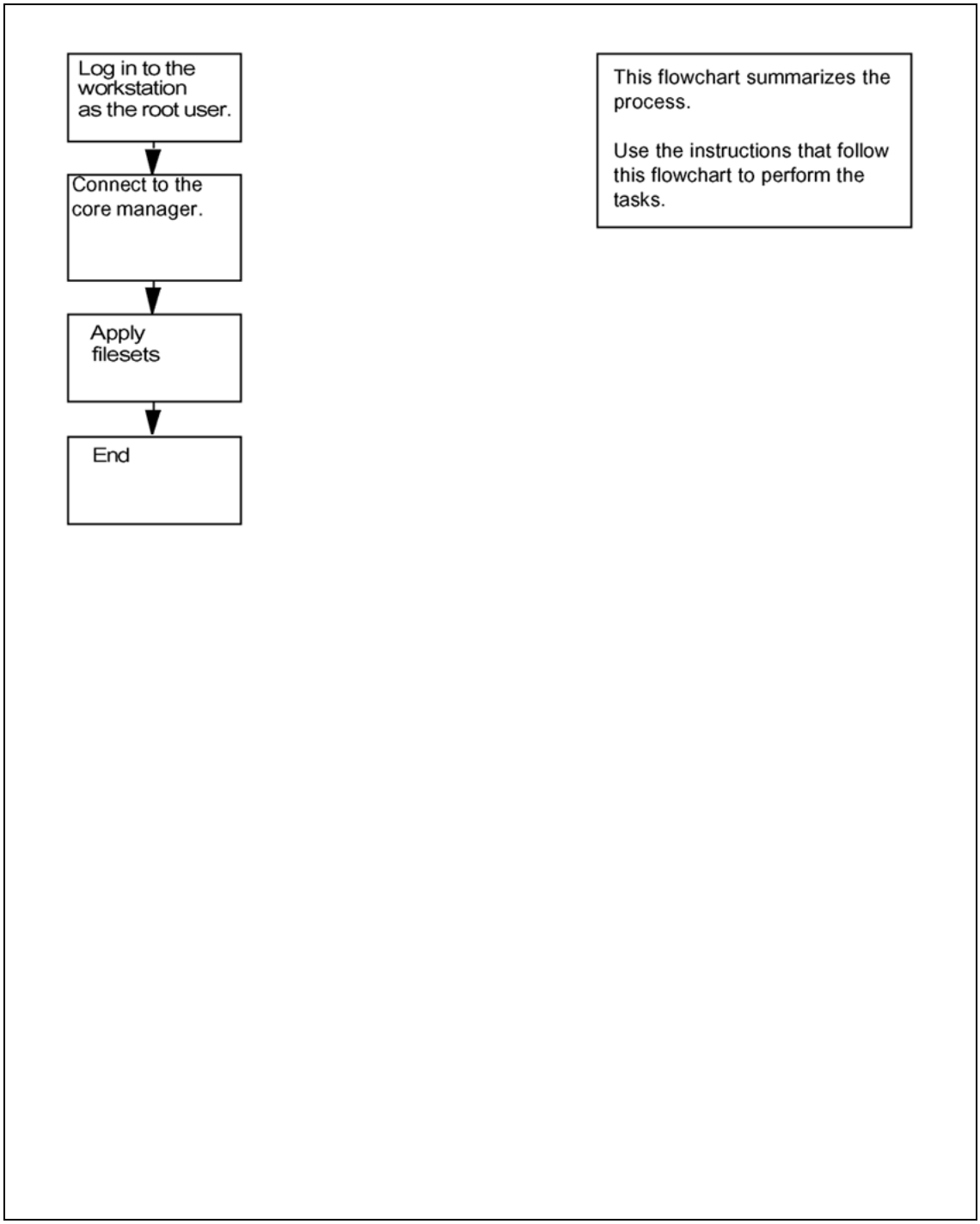
Purpose

Use this procedure to install the logreceiver tool on a client workstation. The procedure accesses the logreceiver software stored on the core manager to which the workstation can connect, and installs it in a specified directory location on the workstation.

Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Task flow for Installing the logreceiver tool on a client workstation



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

Procedure

Installing the logreceiver tool on a client workstation

Step	Action

At the local or remote VT100 console

CAUTION
Risk of revealing the administrative user password
If you use telnet to access the client workstation remotely, and use the default sdm_admin or cell_admin account to execute the DCE control program (dcecp) commands, the system sends the administrative user password in clear text across the network. To avoid this risk, Nortel recommends that you execute the commands from a terminal attached to the workstation console port.

1 Log in to the client workstation as the root user.

2 Access the tmp directory where the CIL tool exists:

```
cd /tmp
```

3 Make the CIL program executable:

```
chmod +x cil
```

4 Invoke CIL:

```
./cil
```

Response

```
            SDM CLIENT SOFTWARE INSTALLATION
Enter the IP address or hostname of the SDM that you
want to download the client software from.
SDM's Address:
```

5 At the CIL menu, connect to the core manager:

```
SDM's Address: <sdm_name>
```

where

<sdm_name> is the IP address or the host name of the core manager.

Response

```
       SDM CLIENT SOFTWARE INSTALLATION
After you enter 'Apply', the selected filesets are
FTPed from the SDM to the /tmp directory.  The filesets
are then installed into the /sdm directory.  Type
```

```
'Help' for a list of commands.  Type 'Quit' to exit
this program.
Client software source: the SDM at bmerye6b
    # Fileset Name
    1 ata_client_17.0.8.0.tar.Z
    2 sft_client_17.0.8.0.tar.Z
    3 eta_client_17.0.8.0.tar.Z
    4 clientcommon_17.0.8.0.tar.Z
    5 logdelivery_client_17.0.8.0.tar.Z
                    Client Software: 1 to 5 of 5
```

If the Client Common Resources fileset is	Do
not installed	step 6
installed	step 8

6 Select the Client Common Resources fileset:

cil> select <n>

where

<n> is the number next to the Client Common Resources fileset

7 Install the selected fileset:

cil> apply

8 Select the logdelivery_client fileset:

cil> select <n>

where

<n> is the number next to the logdelivery_client fileset on the list.

Note: To deselect any filesets, select the fileset a second time. To deselect all filesets, type *select none*.

9 Install the selected fileset:

cil> apply

10 Exit the CIL tool:

cil> quit

11 You have completed this procedure.

—End—

Installing and configuring OM Delivery software

This procedure provides instructions on how to install and configure the OM Delivery (OMD) application. It is assumed that the core manager platform and AIX operating system have already been installed.

If you are installing the OM Delivery application for the first time, ensure that the OM Access and Table Access applications are installed and in service on your core manager before executing this procedure.

Use the following procedure to install or upgrade the OMD application.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Procedure

Installing and configuring OM Delivery software

Step	Action
	At the local or remote VT100 console
1	Log into the core manager as a user authorized to perform config-admin actions.
2	Access the maintenance interface by typing `sdmmtc`

and pressing the Enter key.

3 Access the SWIM level by typing

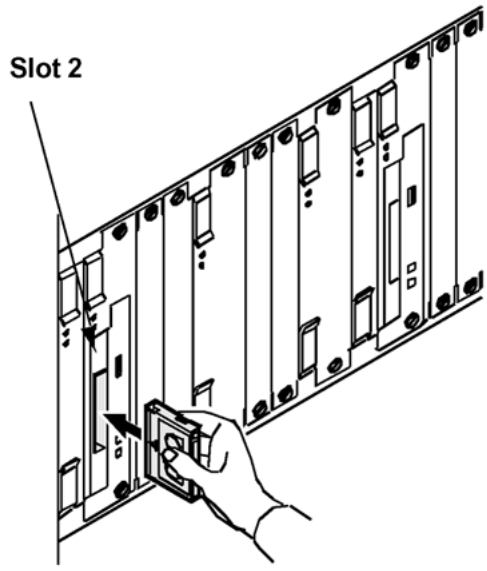
```
swim
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	insert the CS2E0006 6.x (1 of 1) tape in slot 2 as shown in the following figure, then go to step 5 ***Note:*** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.
a directory	step 5

Inserting the tape into the domain 0 tape drive (slot 2)



5 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	list the filesets by typing apply 0 and pressing the Enter key
a directory	list the filesets by typing apply <directory path> and pressing the Enter key

6 Select the OM Delivery fileset by typing

`select <n>`

and press the Enter key.

where

`<n>` is the number next to the OM Delivery fileset

7 Apply the selected (highlighted) fileset by typing

`apply`

and pressing the Enter key.

8 Confirm the Apply command by typing

`y`

and pressing the Enter key.

9 Use the following table to determine your next step.

If the application	Do
installed with no errors	step 10
installed with errors or failed to install	record any error information, and contact your next level of support

10 Return to the SWIM level by typing

`quit`

and pressing the Enter key.

11 Access the Config level by typing

`config`

and pressing the Enter key.

12 Begin configuration for OM Delivery by typing

`config <n>`

and pressing the Enter key.

where

<n> is the number next to the OM Delivery fileset

Response:

```
Are the MDM and SDM integrated?  [y/n]:
```

13 When prompted, indicate the MDM and SDM are not integrated by typing

n

and pressing the Enter key.

14 Use the following table to determine your next step.

If you are configuring OM Delivery for	Do
a PT-AAL1 or UA-AAL1 office	type y, press the Enter key, and continue with step 15
any other office	type n, press the Enter key, and go to step 19

15 Configure OM Delivery as follows:

a. When prompted, enter the IP address of the first MDM (for example, 47.70.176.226), and press the Enter key.

b. When prompted, enter the host name of the first MDM (for example, bpves001), and press the Enter key.

c. When prompted, enter the IP address of the second MDM (for example, 47.149.48.175), and press the Enter key.

d. When prompted, enter the host name of the second MDM (for example, bpves923), and press the Enter key.

e. When prompted, enter the port for 5-minute PM data from the appropriate PMSP running on the MDM (for example, 1646), and press the Enter key.

f. When prompted, enter the port for 30-minute PM data running on the appropriate PMSP running on the MDM (for example, 1647), and press the Enter key.

The system prompts you to indicate whether you want to use custom connection retry settings.

g. Use the following table to determine your next step.

If you	Do
want to use custom connection retry settings	type y, press Enter, and continue with step 16
do not want to use custom connection retry settings	type n, press Enter, and go to step 17

16 Enter your retry settings as follows:

Note: Retry setting values are in seconds. Values higher than 300 seconds are not recommended as they may adversely affect recovery time.

a. When prompted, enter the first connection retry interval (for example 2), and press the Enter key.

b. When prompted, enter the number of retry attempts at that interval (for example 10), and press the Enter key.

c. When prompted, enter the second connection retry interval (for example 10), and press the Enter key.

d. When prompted, enter the number of retry attempts at that interval (for example 40), and press the Enter key.

e. When prompted, enter the third connection retry interval (for example 60), and press the Enter key.

17 Use the following table to determine your next step.

If the data is	Do
correct	type y, and go to step 19
not correct	type n, and go to step 18

18 Use the following table to determine your next step.

If you	Do
want to restart the configuration process	type y, and return to step 15
do not want to restart the configuration process	type n, and go to step 19

19 Exit the maintenance interface by typing

```
quit all
```

and pressing the Enter key.

20 You have completed this procedure.

—End—

Configuring outbound connection security for OMDD

Purpose

Secure outbound file transfer of OMs is provided through the OpenSSH SFTP (secure file transfer protocol) client. The SFTP client protects all data, including sensitive users' passwords, by encrypting the data before it leaves the core manager and decrypting the data after it arrives at the downstream OSS destination. The SFTP client also provides data integrity checking to ensure that the data has not been tampered with during the transfer.

Both password-based authentication and key-based (public key) authentication are supported for secure outbound file transfers using the OpenSSH SFTP.

Prerequisites

The following prerequisites apply to the outbound connection security feature:

- An SSH sftp server (SFTP server subsystem) that is compatible with the OpenSSH sftp client must be running on the downstream Operations Support System (OSS) in order for the OMDD to transfer data with the OpenSSH sftp client.
- OpenSSH software, version 3.7.1p2 or later, and any dependent software must be installed on the core manager in order for SFTPW (Secure File Transfer Protocol wrapper) protocol for outbound file transfer to be used. There is no explicit check performed by the OMDD software to determine whether this package or fileset is installed when the SFTPW is being configured. Thus, if the OMDD SFTPW application fails to find the sftp program, an SFTPW alarm is raised and the application terminates any transfer event it is attempting to perform.
- For the CBM, this secure outbound transfer capability depends on the OpenSSH packages as well as NTutil.
- For the SDM and CS 2000 Core Manager, the secure outbound transfer capability depends on the SDM_OpenSSH.base fileset, which must be installed manually, and the SDM_BASE.util fileset.
- The initial host key acceptance of the downstream processor should be performed manually in order for the SFTPW to be used for file transfer from the core manager. The .ssh/known_hosts file in the maint home directory is edited by SSH software to include the host key. After this is completed, sftp can be used to send files to the downstream OSS. This step must be performed for each downstream destination prior to schedule tuple configuration for SFTPW.

You must have the root user ID and password to perform this procedure.

Limitations and restrictions

The following limitations and restrictions apply to the secure outbound file transfer capability:

- Secure outbound file transfer (SFTPW) cannot re-send ClosedSent files when ClosedSent files already exist on the target directory in the downstream system. Therefore, it is important that existing ClosedSent (or processed) files at the downstream system be either moved to another directory or re-named before an attempt is made to re-send ClosedSent files from the core manager to the downstream system.
- Automatic dumping of the public key file on the remote system is not supported. Users have to manually dump the contents of the public key file into the user's authorization file on the remote system.

  If the remote system is running OpenSSH server, the public key should be appended to .ssh/authorized_keys or .ssh/authorized_keys2 file.
- The user SHELL (cshrc or bash) startup script at the downstream system must not contain ANY echo or print statements which will interfere the handshaking between sftp client and sftp-server. The symptom is that the sftp session terminated pre-maturely and the message "Received message too long <a long num> is printed".
-

Procedure

To configure secure data transfer to a downstream OSS destination, it is necessary to first accept the known host key for the downstream OSS destination. Steps 1 through 10 of this procedure enable you to perform this task. This task must be performed whenever the destination downstream OSS is rebooted or whenever the SFTPD server on the OSS is restarted.

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

Configuring outbound connection security for OMDD

Step	Action
	At the PC or UNIX workstation
1	Establish a telnet connection to the core manager by completing the following substeps. a. Open a terminal window that is VT100 compatible. b. Log onto the core manager from the terminal window prompt:

telnet <ip_address>

where

<ip_address> is the IP address of the core manager

c. When prompted, enter your user ID and password.

d. Change to the root user. Type

su - root

and press the Enter key.

e. When prompted, enter the root password.

2 Change directory to the maint home directory:

cd ~maint

3 Look in the maint directory for the ".ssh" directory:

ls -lad .ssh

If	Do
the .ssh file does not exist	step 4
the .ssh file does exist	step 10

4 Create the .ssh directory:

mkdir .ssh

5 Change the .ssh directory ownership:

chown maint:maint .ssh

6 Change the permissions associated with the .ssh directory:

chmod u+rwx .ssh

7 Change to the maint user:

su maint

8 Run the ssh client to the downstream OSS destination by providing a "maint" user name and IP address for the ssh client, by performing the following steps:

a. Type

ssh -l maint <nn.nn.nn.nn>

where

<nn.nn.nn.nn> is the IP address of the ssh client

Example of response

The authenticity of host Ô10.10.10.10’ can’t be established.

RSA key fingerprint is 3a:d5:d7:6e:ee:6b:45:fc:b9:0b:92:a7:1c:d8:f1:be.

Are you sure you want to continue connecting (yes/no)?

b. Type

```
yes
```

Example of response

Warning: Permanently added Ô10.10.10.10’ (RSA) to the list of known hosts.

9 Press ctrl + C to terminate the program.

10 Exit the telnet session:

```
exit
```

11 Configure the outbound file transfer destination for secure data transfer, using password-based authentication or key-based authentication.

For the procedure on how to configure an outbound file transfer destination, refer to the chapter "Adding a file transfer destination" in the CBM 850 Performance Management book, NN10361-711.

12

13 You have completed this procedure.

—End—

Troubleshooting

Possible error scenarios that may occur when you are performing this procedure and the steps to perform in addressing these problems are listed in the following:

- Connection refused

  This error causes a "Down" status for the SSH Collector Status parameter.

  Example

  Error : ssh; connect to host <hostname/hostip> port 22:
  Connection refused
  Connection closed.

To resolve this problem:

— Verify that the host machine is on the network.

— Verify that the SSH server on the host machine is running and that the configuration is correct (such as, the port number and fingerprint).

- SSH not found

  This error is caused by the ssh not being installed on the core manager.

  Example

  Error: /bin/ksh: ssh: not found.

  To resolve this problem:

  — Verify that the OpenSSH package is installed on the system.

  If your core manager is an AIX-based SDM or CS 2000 Core Manager, you can verify whether the OpenSSH package is installed by checking for the package at the SWIM level of the sdmmtc user interface.

  If the package is not installed, contact your Nortel service representative for assistance in installing the OpenSSH package provided by Nortel.

  You should not install the OpenSSH package downloaded from the web unless you are instructed to do so by your Nortel service representative.

- known_hosts file cannot be datafilled

  This error is caused by the non-existence of, or incorrect permissions for, the /home/maint/.ssh (AIX-based SDM) or /cbmdata/users/maint/.ssh (CBM) directory.

  To resolve this problem:

  — Verify that you are logged in as the root user and that you switched user (su) to the maint user.

  — Verify that the directory /home/maint/.ssh (AIX-based SDM) or /cbmdata/users/maint/.ssh (CBM) is present and has read/write permissions set for the maint user. If the directory doesn't exist, create it.

  — Verify that the correct IP address is used for host key acceptance.

- SSH server's host key has changed

  If the server's host key has changed, the client will notify you that the connection cannot proceed until the server's host key is deleted from the known_hosts file using a text editor. Before performing this task, you must contact the system administrator of the SSH server to ensure that the server operation will not be compromised.

To resolve this problem:

— Try to create an ssh connection to a different machine. If you receive an error message about a changed or incorrect public key, it is probably due to the host changing its public key. Edit the file /home/maint/.ssh/known_hosts using a text editor and delete any line containing the name of that host.

— Try to create an ssh connection to that host again and then accept a new public key for the host.

- SSH warns about "man-in-the-middle attack"

  This problem is caused either by someone eavesdropping on your connection or by the host key having been changed.

  To resolve this problem:

  — Contact your system administrator to determine whether the host key has been changed or whether the ip address of the client has been changed.

  — Edit the file /home/maint/.ssh/known_hosts using a text editor and delete any line containing the name of that host.

  — Datafill the known_host keys with new information.

- sftp session terminated pre-maturely with the message "Received message too long <a long num>"

  Ensure that the user SHELL (cshrc or bash) startup script at the downstream system does not contain any echo or print statements which will interfere the handshaking between sftp client and sftp-server.

Creating the backup user ID on the core for SBRM

Purpose

This procedure enables you to create the user ID on the core to enable the operation of the Synchronous Backup Restore Manager (SBRM). The types of operations that can be performed by this user are:

- set dump_restore_in_progress field in ofcstd table
- start image dump
- ability to run itocci command set

This procedure should be performed before you first perform the procedure, "Configuring core access for SBRM".

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

Procedure

Creating the backup user ID on the core for SBRM

Step	Action
	At the CI prompt on the core
1	Enter the following command: **`permit <backupuser> <backupuser_pswd> 4 10000 english all`** where **`<backupuser>`** is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login **`<backupuser_pswd>`** is the password for the <backupuser> user you are creating, which can be up to 16 characters in length **`4`** is the priority **`10000`** is the stack size **`english`** the language setting **`all`** is the privilege setting If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length. If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log into the core manually with this user first. The core will prompt you to change the password at the

first login after the login is permitted. Change the password and then perform the procedure, "Configuring core access for SBRM" using the <backupuser> user you have created and the changed password.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in "Configuring core access for SBRM" to ensure that the password for the <backupuser> user.

2 You have completed this procedure.

—End—

Configuring core access for SBRM through the CS 2000 Core Manager

Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

Note 1: Perform the procedure,"Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM" (page 200) before you perform this procedure for the first time.

Note 2: This procedure should be performed to whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

Prerequisites

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

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

Procedures related to this procedure

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

Procedures

Configuring core access for SBRM through the CS 2000 Core Manager

Step	Action
	At the CS 2000 Core Manager
1	Log into the core manager with the login ID and password for a user authorized to perform config-admin actions.

2 Use the following table to determine your next step.

If	Do
you wish to perform this procedure on the command line	step 3
you wish to perform this procedure through SDMMTC (SDM maintenance interface)	step 5

3 At the command line prompt, change directory to the directory containing appropriate configuration script:

```
cd /opt/nortel/bkresmgr/cbm/scripts
```

4 Run the configuration script:

```
./bkmgr_config.sh
```

Go to step 7.

5 Access the config level of the SDM maintenance interface:

```
# sdmmtc config
```

6 From the list of filesets that displays, select the Succession Provisioning Data Sync Manager fileset (Backup Restore Manager fileset, SDM_BKM.bkm) and then type **config**.

7 As the configuration script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, "Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM" (page 200)

8 As the script continues to run, you are then prompted for the user you entered (in step 7). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, "Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM" (page 200)

9 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.

10 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.

11 You have completed this procedure.

—End—

Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM

Purpose

This procedure enables you to configure the bkmgrusr user ID and password in order for the Synchronous Backup Restore Manager (SBRM) to communicate with the Device Backup Restore Manager (DBRM) on the CS 2000 Core Manager.

Note: This procedure applies only to the CS 2000 Core Manager running on an AIX platform. The procedure does not apply to the Core and Billing Manager (CBM) running on an SSPFS-based server.

Prerequisites

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

Procedure

Configuring the bkmgrusr user ID and password for communication with SBRM

Step	Action

At your workstation

1 Log into the CS 2000 Core Manager on which the DBRM is installed as a user authorized to perform config-admin actions.

2 Create the user, "bkmgrusr":

```
mkuser bkmgrusr
```

3 Create the groups, "emsmtc", "emsadm", and "emsrw":

```
mkgroup emsmtc

mkgroup emsadm

mkgroup emsrw
```

4 Add the bkmgrusr user to the primary group, "maint", and to secondary groups, "emsmtc", "emsadm", "emsrw":

```
chuser pgrp=maint groups=emsmtc,emsadm,emsrw
home=/export/home/bkmgrusr admin=true shell=/bin/ksh
bkmgrusr
```

Note: Although it may be unclear from the command syntax shown above, this command is entered on a single line. Therefore, when you enter this command, ensure that there is a space between emsrw and home, and that there is a space between ksh and bkmgrusr

5 Confirm that the bkmgrusr user has been added to the required groups in step 4:

```
groups bkmgrusr
```

The system will display the groups that are associated with the bkmgrusr user.

6 Set the password for the bkmgrusr user:

```
passwd bkmgrusr
```

Note: The bkmgrusr user is disabled until this step is performed.

7 Log out of the CS 2000 Core Manager and then log back in as "bkmgrusr".

When the system prompts you, change the password for the bkmgrusr user.

8 Change to the home directory and create the ".ssh" directory:

```
cd /export/home/bkmgrusr

mkdir .ssh

chmod 700 .ssh
```

9 You have completed this procedure.

—End—

Removing an ETA server

Purpose

Use this procedure to remove an Enhanced Terminal Access (ETA) server. When the ETA application is not required on the core manager, you must release the resources that were claimed by the application server.

ATTENTION

You can use either the sdm_admin or the cell_admin account to perform this procedure. If you use the default sdm_admin account to perform this procedure, and the default account does not exist, you can use the cell_admin account instead. You can also exit the procedure, go to the DCE Creating a DCE user procedure to create an sdm_admin account, then return to this procedure.

CAUTION

Risk of revealing the administrative user password

If you use telnet to access the core manager remotely, and use the default sdm_admin or cell_admin account to execute the DCE control program (dcecp) commands, the administrative user password is sent in clear text across the network. To avoid this potential security risk, Nortel recommends that you execute the commands from a terminal physically attached to the core manager console port.

You can also use this procedure to clear problems with an application server. It might be necessary to remove an ETA server from the DCE cell, then recreate the server using the config command under the SWIM menu. For information on server installation, refer to the procedure "Configuring the ETA application server software" (page 120).

Problems with an application server can include:

- the server identifies a mismatch resulting from a change to the switch Common Language Location Identifier (CLLI)
- the server cannot authenticate itself because of key tab problems. This may occur if the core manager data files are restored from a backup tape
- the server is unable to authenticate itself because its password has expired. This may occur if the server is OffL or ManB for an extended period of time.

Removing an ETA server is a two-stage process:

- remove the ETA server from the DCE cell, then
- remove the ETA server from the core manager

Prerequisites

To perform this procedure, you must have a DCE account with administrative privileges and root user access to the core manager.

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

Procedures

Removing an ETA server from a DCE cell

Step	Action

At the local or remote VT100 console

1 Log into the core manager as the root user.

2 Log into DCE:

```
dce_login <DCE_admin_user>
```

where

`DCE_admin_user` is the administrator userID.

3 Enter your DCE password, and press the Enter key.

4 Invoke the DCE control program (dcecp):

```
dcecp
```

5 List the key tables in the core manager:

```
dcecp> key catalog -simplename
```

6 Use the following table to determine your next step.

If the list	Do
contains the eta key table	step 7
contains the eta key table	step 12

7 List the principals that are supported by the key table:

```
dcecp> key list eta
```

8 Ensure the list from the command executed in step 7 contains entries that follow the format: /.../cell name/sdm/clli/principal name.

where

`cell name` is the cell in which the core manager resides.

clli is the Common Language Location Identifier (CLLI) of the switch to which the core manager is connected.
principal name is the userID of the server.

9 Determine whether the principal name of all members in the list is the same, and that it corresponds to the eta-server.

If all principal names are	Do
identical	step 11
not identical	step 10

10 Remove the entries for the principal in the key table:

```
dcecp>key remove eta -member /.../ <cell_name>
/sdm/ <clli> /eta-server
```

where

cell_name is the cell in which the core manager resides
clli is the Common Language Location Identifier (CLLI) of the switch to which the core manager is connected.

11 Delete the key table:

```
dcecp> key delete eta
```

12 Remove the principal for the core manager application server:

```
dcecp> principal delete sdm/ <clli> /eta-server
```

where

clli is the CLLI of the switch to which the core manager is connected.

13 Exit dcecp:

```
dcecp> exit
```

14 Log out from DCE:

```
exit
```

15 You have completed this procedure. To remove the ETA server and client filesets from the core manager, use the procedure "Removing an ETA server from a core manager" (page 205).

—End—

Removing an ETA server from a core manager

Step	Action
	At the local or remote VT100 console
1	Ensure that you are logged into the core manager as the root user.
2	Access the maintenance interface: **`sdmmtc`**
3	Access the admin level: **`admin`**
4	Access the SWIM level: **`swim`**
5	Access the Details level: **`details`**
6	Select the filesets to delete: **`select <x> <y> <z>`** where **`x`** is the number next to the ETA fileset **`y`** is the number next to the ETA client fileset **`z`** is the number next to the ATA client fileset.
7	Delete the filesets: **`remove`**
8	Confirm that you want to delete the filesets: **`y`** ***Note:*** You will need to re-install the filesets from the DAT if you wish to use the ETA server at a later date. The system deletes the filesets, displaying a message when the removal is complete.
9	Exit the maintenance interface: **`quit all`**
10	Log out from the core manager: **`exit`**
11	You have completed this procedure.

—End—

Installing the CMFT on a client workstation

Purpose

Use this procedure to install the Command Module File Transfer script (CMFT) on a client workstation.

Application

This procedure copies the CMFT from the Command Module (CM) to a specified directory on the client workstation, typically /sdm/bin. The CMFT script allows you to use SCFT (SSH Core File Transfer) to transfer files to and from the CM.

SCFT is described in the "OpenSSH Overview" section in *CBM 850 Accounting*, NN10363-811

Prerequisites

Logging on to the CS 2000 Core Manager

All users are authorized to perform this procedure.

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

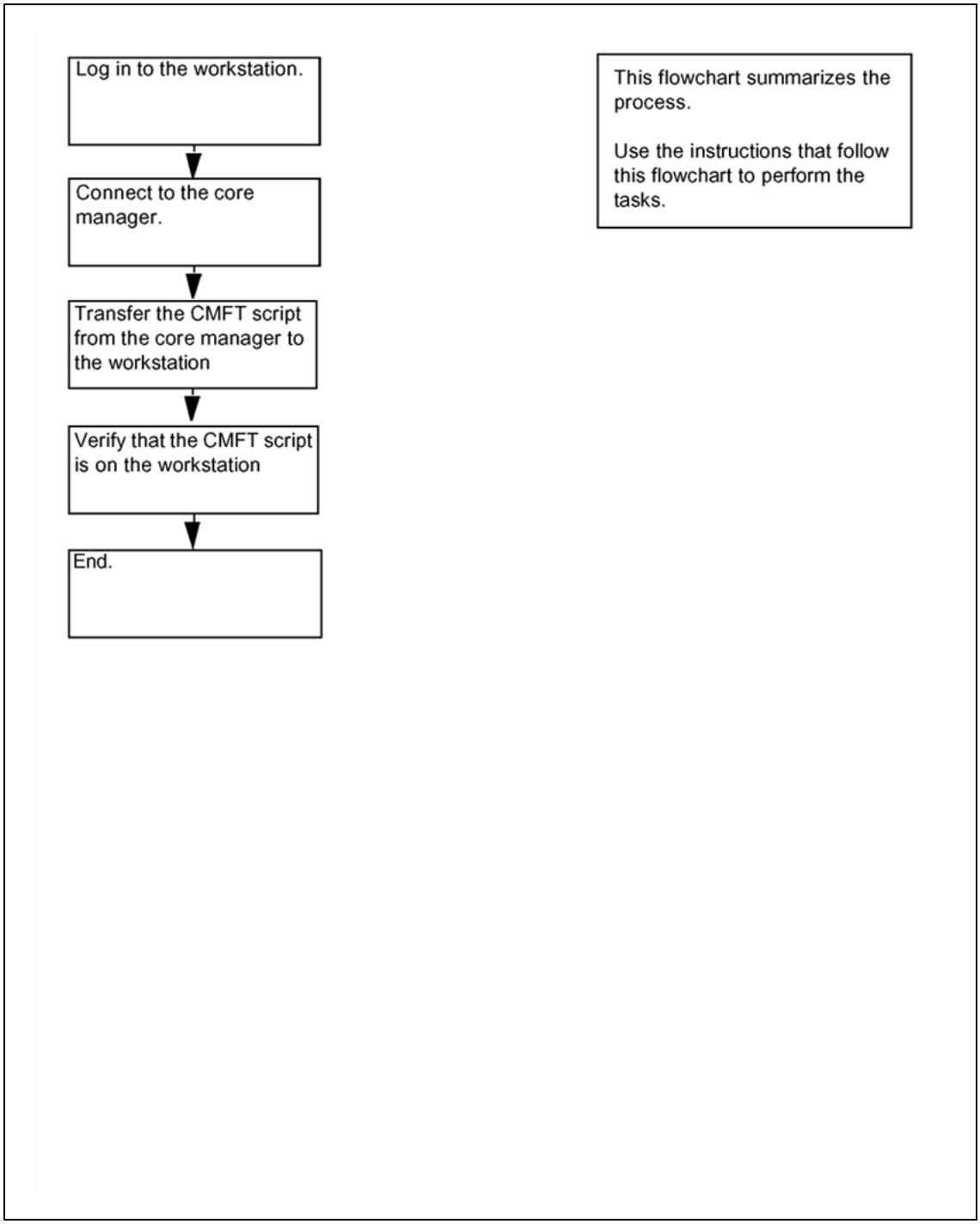
Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying information about a user or role group	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Task flow for installing the CMFT on a client workstation



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

Procedure

Installing the CMFT on a client workstation

Step	Action
	At the local or remote VT100 console
1	Log in to the client workstation.
2	Get the CMFT script from the core manager: **`scp <your user ID>@ <coremanager_ip_address> :/sdm/scft/cmft.`** where **`<coremanager_ip_address>`** is the core manager node name or ip address
3	Verify that you have successfully transferred the CMFT script **`ls -l cmft`** The client workstation displays the CMFT script.
4	Set the ownership and permissions of the CMFT script to 755: **`chmod 755 cfmt`**
5	You have completed this procedure.

—End—

Removing SCFT

Purpose

Use this procedure to remove SCFT (SSH Core File Transfer). SCFT allows you to use secure FTP to access the Core.

Prerequisites

Logging on to the CS 2000 Core Manager

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

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

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

Procedure

Removing SCFT

Step	Action

At the local or remote VT100 console

1 Log into the core manager. Refer to "Prerequisites" (page 210) for details.

2 Access the maintenance interface:

```
sdmmtc
```

3 Access the admin level:

```
admin
```

4 Access the SWIM level:

```
swim
```

5 Access the Details level:

```
details
```

6 Select the fileset to delete:

select <x>

where

<x> is the number next to the SCFT fileset

7 Delete the fileset:

remove

8 Confirm that you want to delete the fileset:

y

The system deletes the fileset, displaying a message when the removal is complete.

9 Exit the maintenance interface:

quit all

10 Log out from the core manager:

exit

11 You have completed this procedure.

—End—

Removing a core manager from a DCE cell

Purpose

ATTENTION
You must be a trained Distributed Computing Environment (DCE) system administrator who knows DCE administration procedures to perform this procedure.

ATTENTION
Do not decommission DCE if your system is configured with any DCE-dependent application, such as ETA, ATA, SFT, or GR740 Pass Through.

ATTENTION
If you use the default cell_admin "master administrator" account (full removal only), the system sends the password of the administrative user in clear text across the network when you use telnet to access the core manager from another computer. Nortel recommends that you execute the command from a computer attached to the core manager console port to maintain password security.

If you are taking the core manager out of service permanently, you must remove the core manager from the DCE cell. You can remove the core manager from the DCE cell if there is a DCE error that you cannot fix by other methods.

Prerequisites

To perform this procedure, you must know the password created with the DCE cell to use the cell_admin DCE account (principal). The cell_admin DCE account has the required privileges to make changes to the DCE cell.

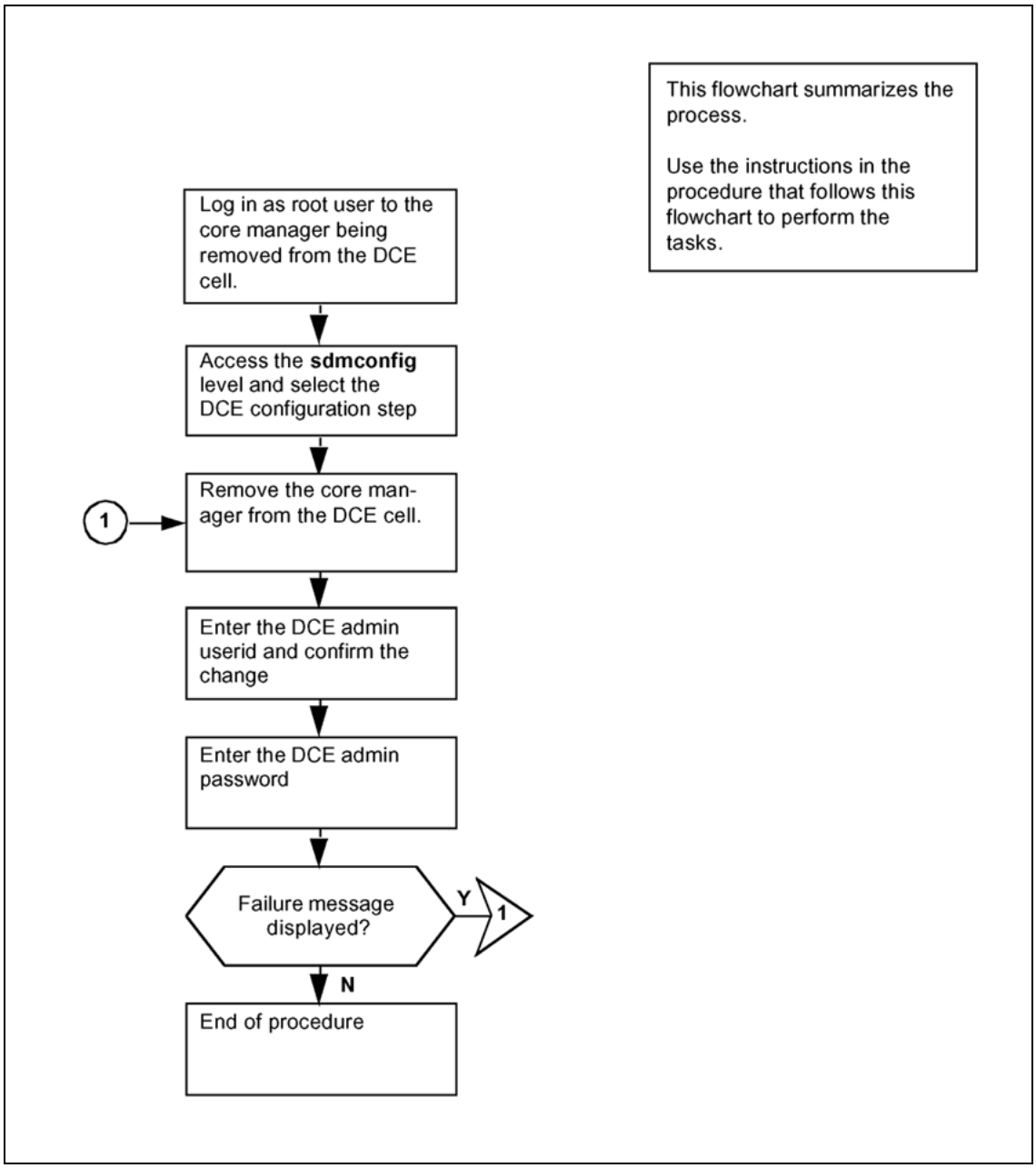
The cell_admin principal can also create a sub administrator account (default is sdm_admin) with limited privileges for the purpose of maintaining core managers in the DCE cell. If you decide to create a sub administrator account, refer to the DCE procedure "Creating SDM administration account".

CAUTION
Possible failure to remove DCE
You cannot use the sdm_admin account to remove DCE from a core manager configured by the cell_admin account. The sdm_admin account does not have the privilege to remove the DCE. Use the cell_admin account to remove DCE under failure conditions.

Task flow diagram

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

Task flow for removing a core manager from a DCE cell



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

Procedure

Removing a core manager from a DCE cell

Step	Action

At the local or remote VT100 console

1 Log in as root user to the core manager that you are removing from the DCE cell.

2 Start the commissioning tool:

```
sdmconfig
```

Response:

The system displays the Commissioning Status Menu.

3 Select the DCE configuration step from the status menu:

```
step <n>
```

where

`<n>` is the menu number next to the DCE configuration option

Response:

The system displays the DCE configuration screen.

4 Delete DCE:

```
delete
```

Response:

The system displays a prompt for you to enter the DCE administrator userid.

5 Enter the DCE administrator **userid**.

Response:

The system displays a prompt for you to confirm the deletion of DCE.

6 Confirm the deletion:

```
y
```

Response:

The system displays a response for you to enter the DCE administrator password.

7 Enter the DCE administrator password.

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

If the system	Do
detects an abnormal condition, and displays a failure message	Under certain fault conditions it may be necessary to enter the delete command more than once to completely remove DCE. As long as the error message changes compared to the previous attempt, go to step 4.
displays other warning messages	press the Enter key
displays the message `"Delete - Command completed."`	wait for the DCE status to change from "." to "-", and go to step 9

9 You have completed this procedure.

—End—

Removing an SFT server

Purpose

Use this procedure to remove a Secure File Transfer (SFT) server. When the SFT application is not required on the core manager, you must release the resources that were claimed by the application server.

Removing an SFT server is a two-stage process:

- remove the SFT server from the DCE cell
- remove the SFT server from the core manager.

You can also use this procedure to clear problems with an application server. It might be necessary to remove an SFT server from the DCE cell, then recreate the server using the config command under the SWIM menu. For information on server installation, refer to Installing the SFT server software.

Problems with an application server can include the following:

- the server identifies a mismatch resulting from a change to the switch Common Language Location Identifier (CLLI)
- the server cannot authenticate itself because of key tab problems. This may occur if the core manager data files are restored from a backup tape
- the server is unable to authenticate itself because its password has expired. This may occur if the server is OffL or ManB for an extended period of time.

ATTENTION

You can use either the sdm_admin or the cell_admin account to perform this procedure. If you use the default sdm_admin account to perform this procedure, and the default account does not exist, you can use the cell_admin account instead. You can also exit the procedure, go to the DCE "Creating a DCE user" procedure to create an sdm_admin account, then return to this procedure after you have created an sdm_admin account.

CAUTION

Risk of revealing the administrative user password

If you use telnet to access the core manager remotely, and use the default sdm_admin or cell_admin account to execute the DCE control program (dcecp) commands, the administrative user password is sent in clear text across the network. To avoid this potential security risk, Nortel recommends that you execute the commands from a terminal physically attached to the core manager console port.

Prerequisites

To perform this procedure, you must have a DCE account with administrative privileges and root user access to the core manager.

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

Removing an SFT server

Step	Action

At the local or remote VT100 console

1 Log into the core manager as the root user.

2 Log into DCE using the administrator userID:

```
dce_login <DCE_admin_user>
```

where

DCE_admin_user is the administrator userID.

3 Enter your DCE password.

4 Invoke the DCE control program (dcecp):

```
dcecp
```

5 List the key tables in the core manager:

```
dcecp> key catalog -simplename
```

6 Determine whether the key table list contains a key table called eta.

If the list	Do
contains the sft key table	step 7
does not contains the sft key table	step 12

7 List the principals that are supported by the key table:

```
dcecp>key list sft
```

8 The list from the command executed in step 7 must contain entries that follow the format: /.../cell name/sdm/clli/principal name.

where

cell name is the cell in which the core manager resides.
clli is the Common Language Location Identifier (CLLI) of the switch to which the core manager is connected.
principal name is the userID of the server.

9 Determine whether the principal name of all members in the list is the same, and that it corresponds to the sft-server.

If all principal names are	Do
identical	step 11
not identical	step 10

10 Remove the entries for the principal in the key table:

```
dcecp> key remove sft -member /.../<cell_name>
/sdm/<clli>/sft-server
```

where

cell_name is the cell in which the core manager resides
clli is the Common Language Location Identifier (CLLI) of the switch to which the core manager is connected.

11 Delete the key table:

```
dcecp> key delete sft
```

12 Remove the principal for the core manager application server:

```
dcecp> principal delete sdm/<clli>/sft-server
```

where

clli is the CLLI of the switch to which the core manager is connected.

13 Exit dcecp:

```
dcecp> exit
```

14 Log out from DCE:

```
exit
```

15 Access the maintenance interface:

```
sdmmtc
```

16 Access the SWIM level:

```
swim
```

17 Select the filesets to delete:

```
select <x> <y>
```

where

x is the number next to the SFT fileset
y is the number next to the SFT client fileset

18 Delete the filesets:

```
8 or remove
```

19 Confirm that you want to delete the filesets:

```
y
```

The system deletes the filesets, displaying a message when the removal is complete.

Note: You will need to re-install the filesets from the DAT if you wish to use the SFT server at a later date.

20 Exit from the maintenance interface:

```
quit all
```

21 Log out from the core manager:

```
exit
```

22 You have completed this procedure.

—End—

Restricting the SFT port range

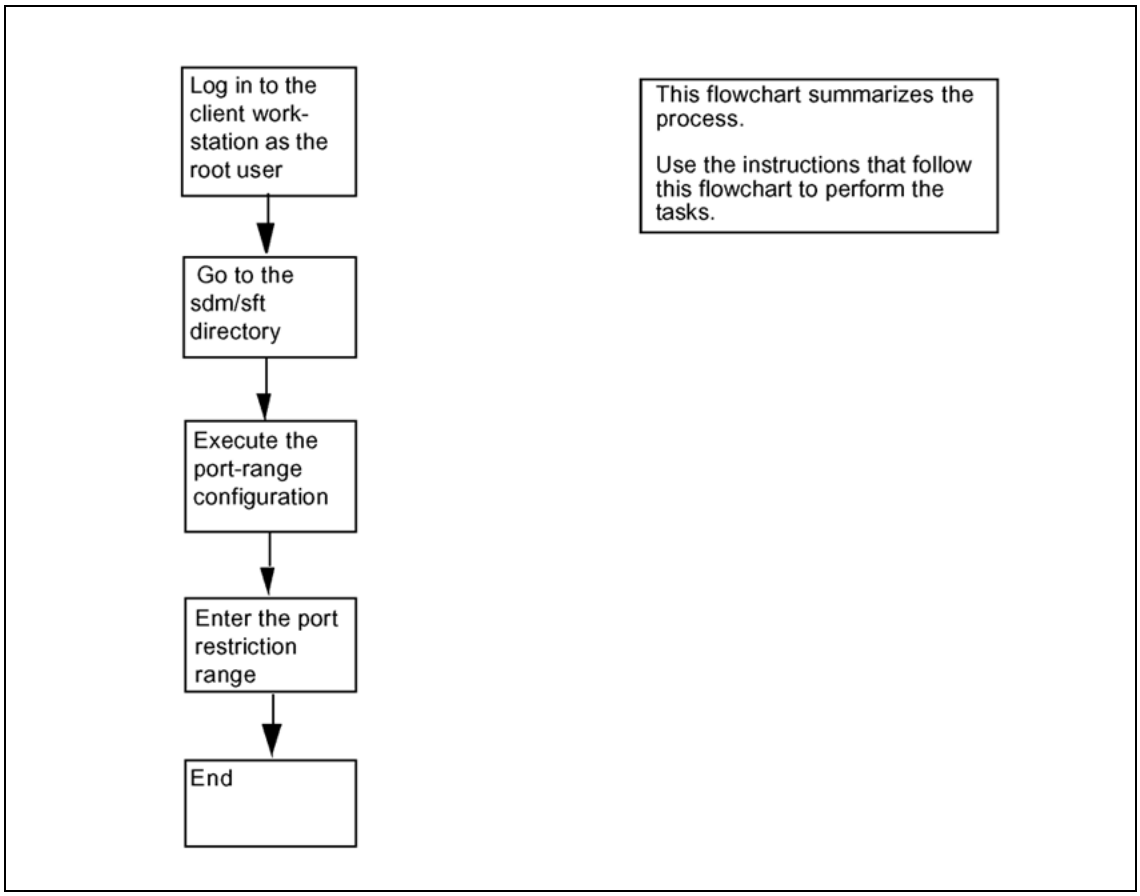
Purpose

Use the following procedure to restrict the Secure File Transfer (SFT) client reverse connection ports on the client workstation.

Task flow diagram

The following task flow diagram summarizes the process for restricting the port range. To complete the specific tasks, perform the procedures that follow the flowchart.

Task flow for restricting the SFT port range



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

Procedure

Restricting the SFT port range

Step	Action

At the local or remote VT100 console:

1 Log in to the client workstation as the root user.

2 Change to the SFT directory:

```
cd /sdm/bin
```

3 Execute the port range configuration script:

```
./sft_port_range
```

Response

```
      SECURE FILE TRANSFER PORT RANGE CONFIGURATION
This configuration script allows you to restrict the
SFT Client reverse connection ports on the client
workstation.
The current port restriction range for the SFT Client
is:
      Range start: -
      Range end:   -
      (no port restriction range)
Set a new port restriction range by typing two numbers
(and pressing [Enter]) which represent the start and
end of the port restriction range.  To remove the port
restriction, type 'None' and press [Enter].  To quit
this program, type 'Quit' and press [Enter].
Port restriction range:
```

4 Enter the port restriction range:

```
Port restriction range: <a> <b>
```

where

a is the start of the range of ports (must be greater than 1024).
b is the end of the range of ports (must be less than 32 000).

Note 1: These values are not range checked. Make sure that these values range from 1024 to 32 000. Enter the lower value first.

Note 2: The range size is determined by the maximum number of simultaneous instances of the SFT client program that are expected to run on the machine where the client is installed. Nortel recommends a range of at least 20 ports (b-a >= 20).

5 Exit the program:

```
exit
```

6 You have completed this procedure.

—End—

Configuring the core manager to communicate with a call agent

Purpose

This procedure describes how to add or change the Ethernet and LANCOMM IP addresses on the core manager to communicate with a call agent. It assumes that the latest software release is already installed on the core manager.

Prerequisites

The table IPNETWRK must contain the LANCOMM stack IP address.

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

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

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

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

Procedure

Configuring the core manager to communicate with a call agent

Step	Action
	At the core manager
1	Login to the core manager as a user authorized to perform config-admin actions.
2	Access the Maintenance level of the maintenance interface: `sdmmtc mtc`

3 Verify the state of the core manager under SDM in the top banner.

If the core manager is	Do
Offl or ManB	step 6
InSv or ISTb	step 4
SysB	contact your next level of support

4 Busy the core manager:

```
bsy
```

5 Confirm the busy command:

```
y
```

6 Access the Core level:

```
core
```

7 Use the following table to determine your next step.

If you are	Do
configuring the core manager for the first time	step 9
reconfiguring the core manager	step 8

8 Begin the change process:

```
change
```

Go to step 11.

9 Begin the add process:

```
add
```

10 When prompted, select the Ethernet communication path:

```
2
```

11 When prompted, enter the active ethernet IP address.

12 When prompted, enter the core's IPNETWORK IP address.

13 Confirm the action:

```
y
```

If	Do
you are ready to return the core manager to service	step 14
you need to perform other tasks on the core manager	step 17

14 Access the maintenance level:

```
mtc
```

15 Return the core manager to service:

```
rts
```

16 Verify that the core connectivity goes into service (indicated by a dot [.] under the State header).

If the core connectivity	Do
goes into service	step 17
does not go into service	contact your next level of support

17 You have completed this procedure.

—End—

Deleting a file system on a core manager

Purpose

Use this procedure if you want to delete a file system that you previously defined on the core manager.

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

Procedure

Deleting a file system on a core manager

Step	Action
	At the local VT100 console
1	Log on to the core manager using the root user ID and password.
2	Access the root directory: `cd /`
	CAUTION The following command will stop all processes that have open files in the designated file system (that is, in <file_system_name>).
3	Delete the file system: `removelv -k <file_system_name>` where `<file_system_name>` is the name of the file system that you want to delete ***Note:*** The file system name must always begin with a forward slash (/).
4	If you cannot remove the file system, contact your next level of support.
5	You have completed this procedure.

—End—

Changing remote and local console connections with O-I

Purpose

Use the procedures in this section to change remote and local console connections with O-I.

Procedures

ATTENTION

All AC devices connected to the SDM must be powered by CO protected power and meet all DMS Isolated System Grounding (ISG) requirements. Specifically, no direct connections from VDUs or other AC-powered devices to SDM EIA ports are allowed. All SDM customers are advised to review the AC power source on all devices connected to the SDM serial ports, to review EIA connections between devices and serial ports, and to comply with the guidelines set fore by the DMS Isolated System Ground (ISG) requirements (NTP 297-1001-156).

Failure to follow this instruction can result in the SDM rebooting if devices are connected, and they take a power spike.

ATTENTION

When connecting a console (VDU) to the SDM, the SDM console should be powered down before the cable is connected to the SP0/1 port. (This step also applies when connecting a MODEM to the SDM SP0/1 ports.) Ensure that the SDM console is powered off and unplugged. Connect one end of the NTRX5094 cable to the serial port of the SDM console. At the rear of the SDM main chassis, connect the other end of the NTRX5094 cable to port P0 in Slot 6 Rear. Once this connection is in place, power up the SDM console.

Failure to follow this procedure can introduce a noise spike on the SP0/1 port, which may cause the SDM to reboot.

Refer to the following table to determine which procedure you should use to change console connections with O-I.

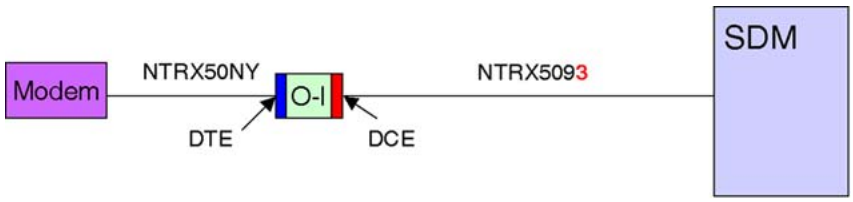
If you want to	Do
change from a remote to a local console connection	the procedure "Changing from a remote to a local console connection with O-I" (page 228)
change from a local to a remote console connection	the procedure "Changing from a local to a remote console connection with O-I" (page 229)

Changing from a remote to a local console connection with O-I

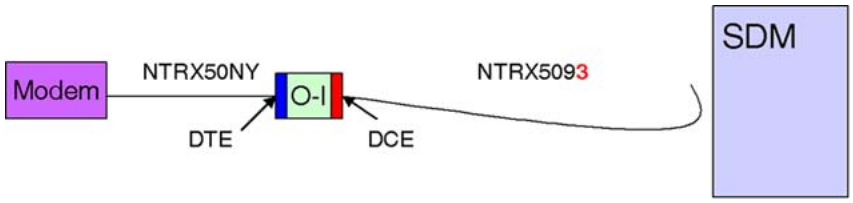
Step	Action

At the core manager

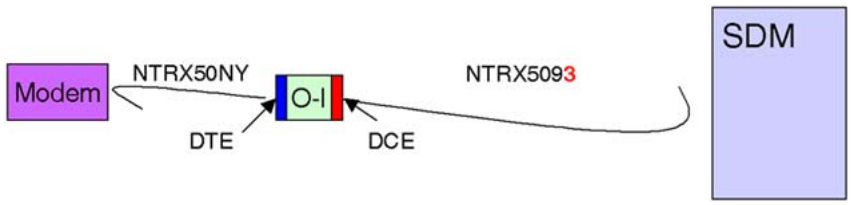
1 The following figure shows an existing remote console connection. Be sure that you are familiar with the configuration, then go to step 2.



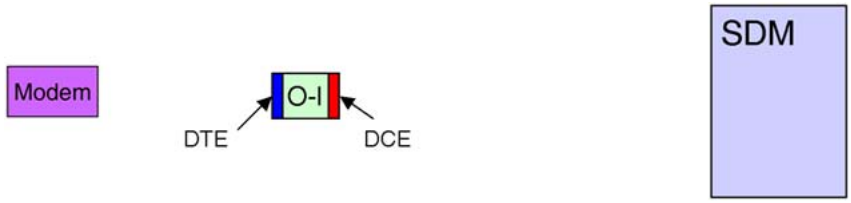
2 Disconnect the NTRX5093 from SP0.



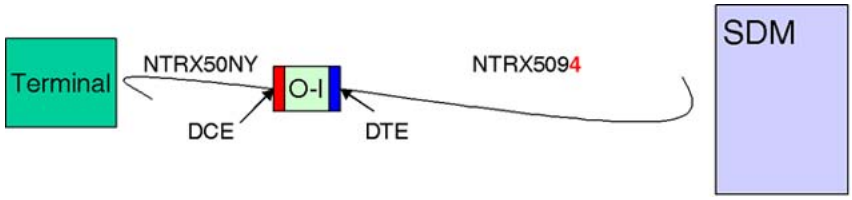
3 Disconnect the NTRX50NY from the modem.



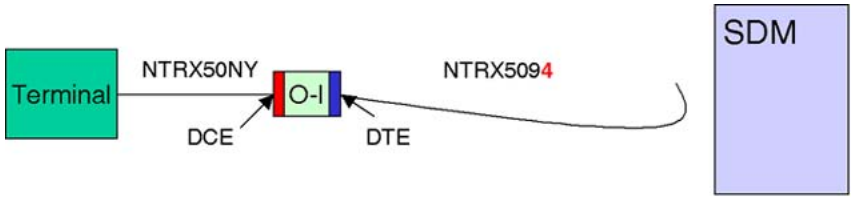
4 Disconnect NTRX50NY from the DTE side of the O-I, and NTRX5093 from the DCE side of the O-I.



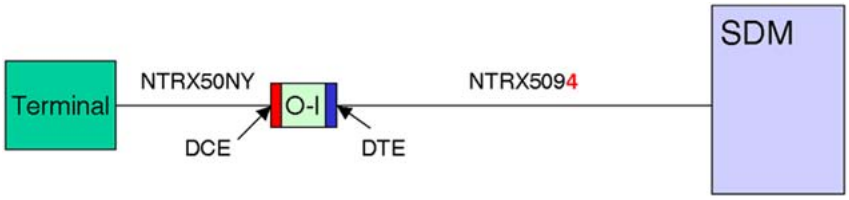
5 Connect the NTRX50NY to the DCE side of the O-I. Connect the NTRX5094 to the DTE side of the O-I.



6 Connect the NTRX50NY to the terminal.



7 Connect the NTRX5094 to SP0.



8 You have completed this procedure.

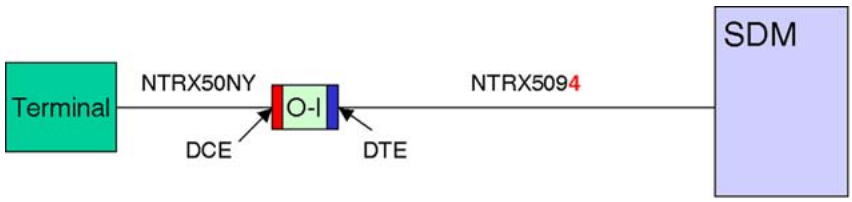
—End—

Changing from a local to a remote console connection with O-I

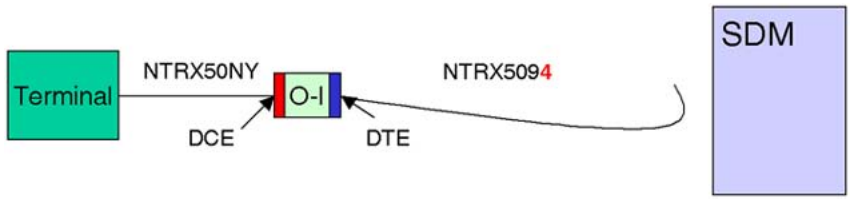
Step	Action

At the core manager

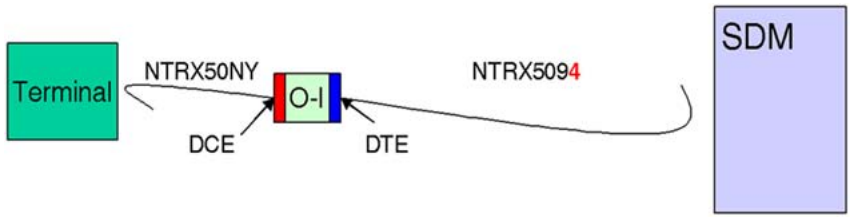
1 The following figure shows an existing local console connection. Be sure that you are familiar with the configuration, then go to step 2.



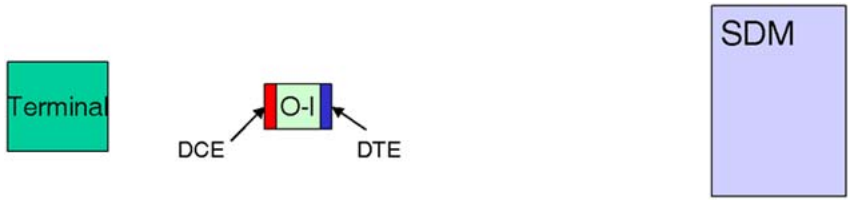
2 Disconnect the NTRX5094 from the SP0.



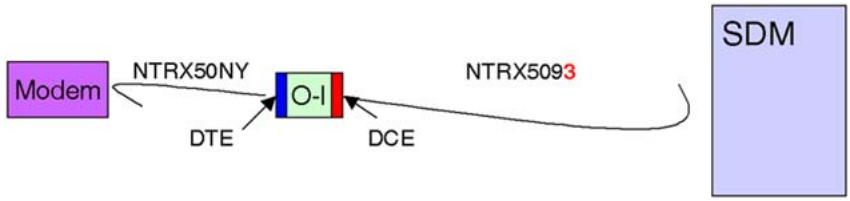
3 Disconnect the NTRX50NY from the terminal.



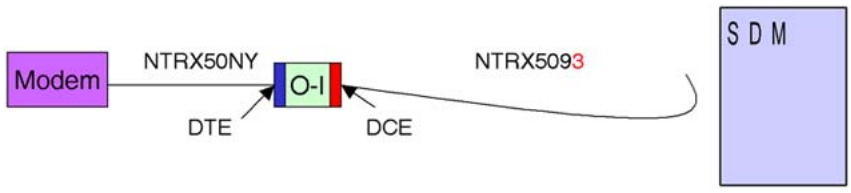
4 Disconnect NTRX50NY from the DCE side of the O-I and NTRX5094 from the DTE side of the O-I.



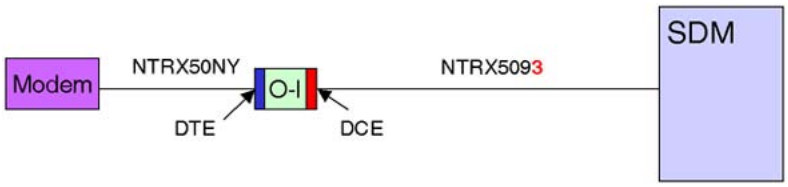
5 Connect the NTRX50NY to the DTE side of the O-I. Connect the NTRX5093 (SDM modem cable) to the DCE side of the O-I.



6 Connect the NTRX50NY to the modem.



7 Connect the NTRX5093 to SP0.



8 You have completed this procedure.

—End—

Configuring a terminal or modem connection to port SP-0

Purpose

Use this procedure to configure a terminal or modem for connection to port SP-0.

CAUTION
If the device connected to the SP-0 port is not configured properly, it could result in a system that does not reboot properly.

CAUTION
Due to the nature of the failure if these devices are configured improperly, Nortel recommends that you take immediate action and review the devices connected to the SDM SP-0 port.

Procedure

Configuring a terminal or modem connection to port SP-0

Step	Action

At your system

1 Use the following table to determine your next step.

If	Do
you have a terminal connected to the SP-0 port	step 2
you have a modem connected to the SP-0 port	step 5

2 If the terminal is powered up (for example, a VDU with or without dual connectors), ensure that echo is disabled and that it is not in XOFF mode while software flow control is enabled.

3 Ensure that the terminal is configured properly, according to the settings shown below:

- 9600 baud
- 8 bit
- no parity

- 1 stop bit
- Xon/Xoff control (or no Xon on some terminals)
- no local echo
- jump scroll
- id vt100
- no new line
- F3=Cancel
- F5=Break
- F10=Exit
- F11=Esc

Note 1: Consult the vendor documentation for these settings.

Note 2: To ensure that the terminal is not in Xoff mode, log into the SDM through port SP-0 whenever you need to issue a shutdown or reboot command.

Note 3: For multi-input terminal, ensure that any unexpected system events are handled correctly by keeping the SDM selected.

4 Go to step 8

5 Ensure that the modem is configured properly:

a. Connect a VT-100 terminal to the GDC modem with the temporary RS-232 cable.

Note: The commands that follow must be issued to the modem from a terminal connected to the modem. Therefore, use a temporary cable with RS-232 connectors on both ends.

b. Issue the following "AT" commands to the modem in the order shown. Before starting, refer to the notes at the end of this command list.

```
AT&F0
AT\T7
AT&R2
AT&C1
ATE0
AT%K1
ATQ1
```

```
AT&W0

AT&Y
```

Note 1: The commands must be issued in the order shown above. If a mistake is made, re-issue all of the commands starting from the first command in the list.

Note 2: Although the GDC modem that is shipped with the SDM supports all of the commands shown above, some modems do not. If you encounter errors on commands other than "ATE0" (the command to disable echo), those errors can be ignored.

Note 3: After the command "ATQ1" is entered, the modem goes into quiet mode and does not acknowledge the reception of AT commands with an "OK". Continue entering the commands, regardless.

6 Remove the temporary RS-232 cable from the modem.

7 Re-connect the NTRX5093 cable to the modem, to port SP-0.

8 You have completed this procedure.

—End—

Upgrading the CS 2000 SAM21 Manager GUI client application

Application

Use this procedure to upgrade the CS 2000 SAM21 manager graphical user interface (GUI) client application to the latest software release.

Prerequisites

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

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

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

The CS 2000 SAM21 manager server must have the same software version as the client version to which you are upgrading. The CS 2000 SAM21 manager is a client/server application. The client runs on a Sun SPARC workstation, and the server runs on the CS 2000 Core Manager.

For SN07, the following requirements must be met to upgrade the client:

- The CS 2000 SAM21 Manager client requires a Sun SPARC workstation. The workstation must run (at a minimum) the Solaris 2.7 operating system. The CS 2000 SAM21 Manager is also supported on the Solaris 2.8 operating system. For optimum performance, Nortel recommends you have a Sun Ultra10 with 512 Mbyte of DRAM and 70 Mbyte or higher of available disk space.
- The latest versions of the following patch IDs are required for Solaris 2.7 systems:
  - Patch 106300
  - Patch 106327
  - Patch 106541
  - Patch 106950
  - Patch 106980

— Patch 107081

— Patch 107226

— Patch 107226

— Patch 107544

— Patch 107636

— Patch 107656

— Patch 107702

— Patch 108374

The latest versions of the following patch IDs are required for Solaris 2.8 systems:

— Patch 108652

— Patch 108921

— Patch 108940

For further details see Sun's Solaris Java patch page at: http://java.sun.com/j2se/1.3/install-solaris-patches.html

Patches can be retrieved from Sun's Patchfinder at: http://sun-solve.sun.com

- The latest SAM21 client software version must be installed.
- The CS 2000 SAM21 Manager client application requires the client machine to be configured in a pluggable authentication module (PAM) framework.

Procedure

ATTENTION

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

Step	Action

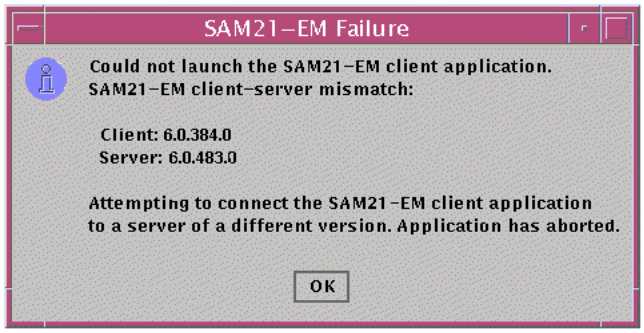
At the Client Workstation

1 Log onto the client workstation as a user authorized to perform config-admin actions.

Note: For all upgrades, the client software must be upgraded to match the server software before it is started.

If an attempt was made to launch the CS 2000 SAM21 Manager client application (by typing: >sdm/bin/sam21gui), the user will receive a mismatch error. See the following "Mismatch error" (page 237) figure for an example of the error message. A mismatch error indicates that the client machine must be upgraded to match the version of the manager running on the CS 2000 Core Manager. This error message only occurs for MNCL or maintenance release upgrades.

Mismatch error



2 If a previous manager client has been installed, verify the client machine is still using the old version of the manager software:

```
/sdm/bin/sam21gui -version
```

The resulting version number indicates that you have not yet upgraded the client to match the server.

3 Access the directory where the Client Installer and Launcher (CIL) tool is to be located after the FTP operation:

```
cd /tmp
```

4 Connect to the CS 2000 Core Manager using file transfer protocol (FTP):

```
ftp <ipaddress>
```

where

ipaddress is the IP address of the CS 2000 Core Manager

5 Log on the CS 2000 Core Manager as an anonymous user:

```
Name:ftp
```

6 When prompted for a password, ignore the prompt and press the Enter key to continue the procedure.

7 Get the Client Installer and Launcher tool (CIL):

```
ftp> get cil
```

8 Quit the ftp connection to the CS 2000 Core Manager:

```
ftp> quit
```

9 Make the CIL program executable:

```
chmod 755 cil
```

10 Execute the CIL program:

```
./cil
```

The system responds

```
       SDM CLIENT SOFTWARE INSTALLATION
Enter the IP address or hostname of the SDM that you
want to download the client software from.
SDM's Address:
```

11 At the CIL menu, connect to the CS 2000 Core Manager:

```
SDM's Address: <ipaddress>
```

where

ip_address is the IP address or the host name of the CS 2000 Core Manager.

12 Select the CS 2000 Core Manager fileset to upgrade the client workstation:

```
cil> select <#>
```

where

#
is the number of the CS 2000 Core Manager fileset.
An example of the fileset is snm_sam21_client_7.0.xxx.n.tar.Z where xxx represents the latest version and n represents the MNCL version.

13 Install the selected fileset:

```
cil> apply
```

14 Enter the IP address of the server when prompted for it by typing the IP address at the prompt and pressing the Enter key.

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

—End—

Performing a full restore of the software from S-tape

Purpose

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

Prerequisites

ATTENTION

You must be a trained AIX system administrator who is authorized to perform config-admin actions 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 recommends that you use tape drive DAT0 to perform this procedure.

You must be authorized to perform config-admin actions at a local VT100 console to perform this procedure.

Procedures

Follow the procedures outlined in "Performing a full restore of the software from S-tape" in *CS 2000 Core Management Fault Management*, NN10082-911.

Removing CS 2000 Core Manager application filesets

Purpose

Use this procedure to remove application filesets that reside on the CS 2000 Core Manager.

You can display the list of application filesets available on the CS 2000 Core Manager at the DETAILS level of the maintenance interface, including the version and status of each application fileset. An application fileset can be in one of the following states:

- APPLIED—the CS 2000 Core Manager is using the software. If a previous version of the fileset exists in the archived state, the applied fileset can be removed. In that case, the previous version is restored.
- ARCHIVED -— a backup version of the fileset is available and can be restored.
- FAILED— the fileset failed and must be reinstalled before use.
- OBSOLETED—the fileset is no longer active

Prerequisites

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

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

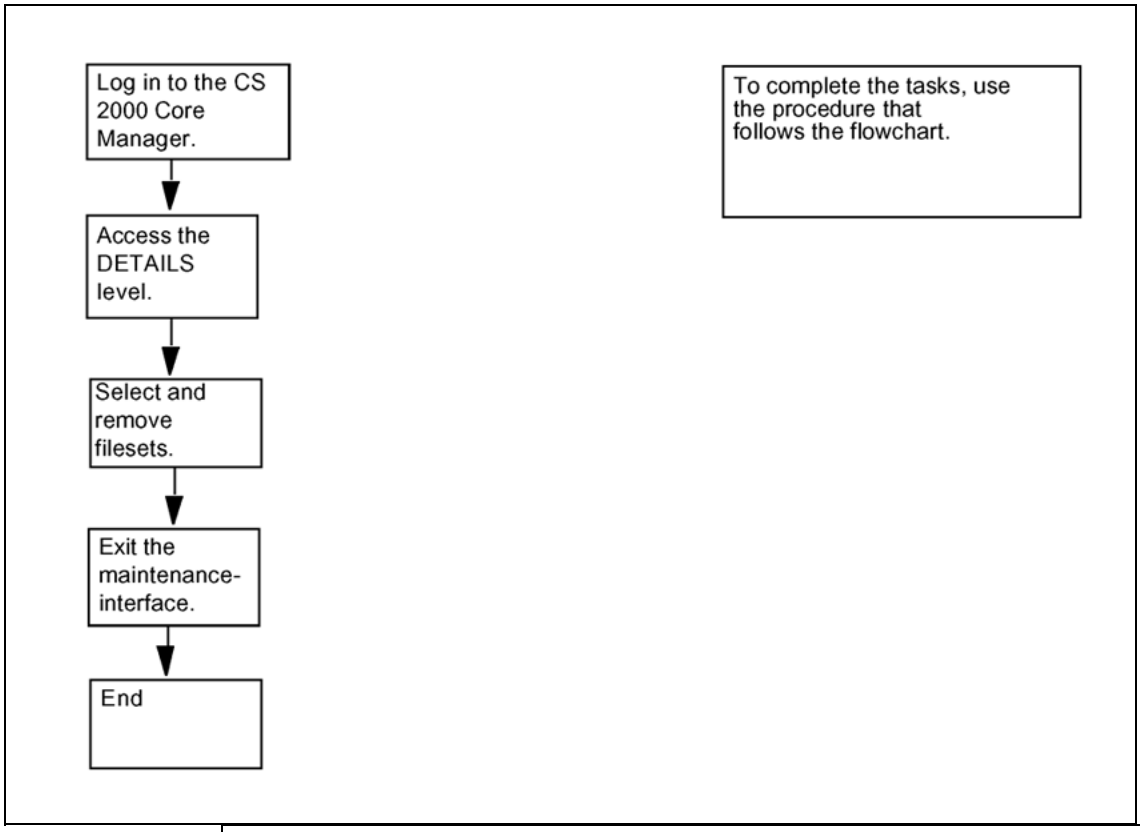
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Procedure

The following task flow diagram summarizes the process. To complete the tasks, use the instructions in the procedure that follows the flowchart.

Task flow for Removing application filesets



ATTENTION

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

Removing application filesets

Step	Action

At the local or remote VT100 console:

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

2 Access the DETAILS level of the maintenance interface:

```
sdmmtc details
```

3 Remove one or more filesets:

```
remove <#>
```

where

`<#>` is the number next to the fileset you want to remove

Note: To remove multiple filesets at one time, specify as many fileset numbers as you want, without using commas to separate them.

4 When prompted, confirm the remove command:

```
Y
```

5 Exit the maintenance interface:

```
quit all
```

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

—End—

Upgrading the CPU controller modules

Purpose

Use this procedure to upgrade the CPU controller modules independently from a CS 2000 Core Manager software upgrade. Refer to "Hardware Baseline" in *Upgrading the CS 2000 Core Manager*, NN10060-461, for a list of the CPU modules that are supported by this upgrade procedure.

ATTENTION

Upgrading a pair of CPUs can require two to four hours of a maintenance window to complete.

CAUTION

This activity causes a service disruption

This hardware upgrade requires the complete shutdown of the CS 2000 Core Manager and all its applications including the CS 2000 Core Manager billing Application. Ensure that adequate backup space is available on the core before continuing with this procedure.

Prerequisites

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

You must determine the amount of backup space needed during the hardware upgrade. Refer to section "Disk space requirements in "Preparing for SBA installation and configuration" in *CS 2000 Core Manager Accounting*, NN10126-811. To set up the backup space, refer to "Configuring the SBA on the core" in *CS 2000 Core Manager Accounting*, NN10126-811.

ATTENTION

Perform a system image backup before you upgrade the CPUs. Refer to the procedure "Creating system image backup tapes (S-tapes) manually" in the *CS 2000 Core Manager Security and Administration*, NN10170-611.

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

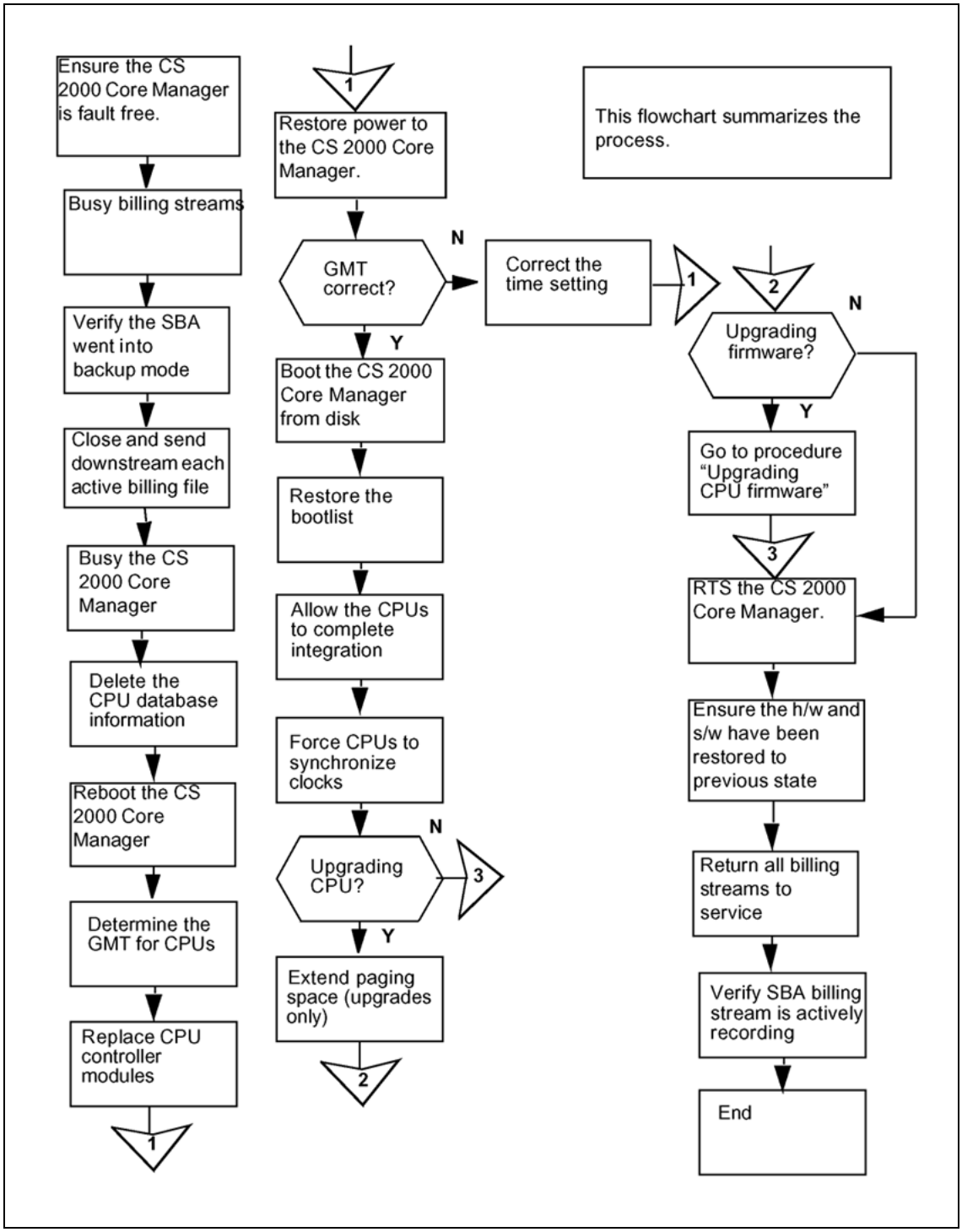
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Procedure

The following task flow diagram provides an overview of the upgrade process. Use the instructions in the procedures that follow the flowchart to complete the tasks.

Task flow for Upgrading the CPU controller modules



Procedure

ATTENTION

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

ATTENTION

Verify the keystrokes that are required to perform a "Break" on your VT100 console. If necessary, consult your site system administrator for assistance.

Upgrading the CPU controller modules

Step	Action

At the MAP display

1 Ensure that you have configured adequate backup space and performed a system image backup.

2 Ensure that the CS 2000 Core Manager hardware and software applications are fault-free, or that known faults are investigated and acceptable.

Any alarms that recur after a CPU upgrade must be investigated, and any new alarms must be resolved without delay. If this does not occur, contact your next level of support.

3 Busy all billing streams on the core. Post the required billing stream:

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

where

<stream> is the name of the billing stream

4 Busy the posted stream:

```
bsy
```

5 Repeat steps 3 to 4 for each configured billing stream.

6 For each configured billing stream, verify that at least one backup file exists on at least one of the configured backup volumes.

Display the names of the backup volumes configured for the specified billing stream:

```
mapci;mtc;appl;sdmbil;conf view <stream>
```

where

<stream> is the name of the billing stream

7 Verify that an SBA backup file exists on at least one of the displayed backup volumes:

```
diskut;lf <backup_volume>
```

where

`<backup_volume>` is the name of the selected backup volume

Note: The name of each backup file is prefixed with the word BACK.

8 Repeat steps 6 and 7 for each billing stream.

At the local or remote VT100 console

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

10 Close and send downstream all unprocessed billing files. Refer to *CS 2000 Core Manager Accounting*, NN10126-811 and use the following table to determine your specific method.

Task	File transfer mode	Procedure to use in *CS 2000 Core Manager Accounting*, NN10126-811
Close billing files	All	"Closing billing files"
Send billing files downstream	Outbound file transfer (OFT)	"Sending billing files from disk"
	Inbound file transfer (IFT)	"Retrieving billing files for a stream set to inbound file transfer"
	Real-time billing (RTB)	"Sending billing files from disk"
	Automatic file transfer (AFT)	No manual action is required. Wait for SBA to deliver pending billing files to the downstream destination. There must be no more than one pending file for each AFT session. Use the following commands to query AFT sessions: billmtc, appl, aft, aftconfg, list. To verify which billing files for each session are still pending, enter the following commands: billmtc, appl, aft,query <session_name>.

11 To display the details about a stream, refer to the procedure "Listing billing streams" in the Accounting document. To list all files currently stored in a stream, refer to procedure "Listing billing files" in *CS 2000 Core Manager Accounting,* NN10126-811.

12 If you are unable to send billing files to a downstream destination and you want to proceed with the upgrade, back up the billing files to a DAT tape. If required, refer to procedure "Copying billing files to tape (backup)" in *CS 2000 Core Manager Accounting,* NN10126-811.

13 If you need to restore the billing files from tape and you have AFT or IFT configuration, contact your next level of support for instructions. For any other configuration, you can send the billing files from tape using the procedure "Sending billing files from tape" in *CS 2000 Core Manager Accounting,* NN10126-811.

At the MAP display

14 Access the CS 2000 Core Manager level of the MAP display:

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

Example response:

```
SDM InSv
```

15 Busy the CS 2000 Core Manager:

```
bsy
```

Example response:

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

16 Confirm the busy command:

```
y
```

Example response:

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

At the local or remote VT100 console

17 Log in to the CS 2000 Core Manager as a user authorized to perform config-admin actions.

18 List information for the root volume group (rootvg):

```
lsvg -p rootvg
```

Example response

```
root vg:
```

```
PV NAME  PV STATE  TOTAL PPs  FREE PPs
FREE DISTRIBUTION
hdisk0   active    1013       499
       175..31..00..125
                                        ..168
hdisk7   active    1013       499
       170..137..00..00
                                        ..192
```

19 Record the names of the hard disks (physical volumes) that provide rootvg storage on the CS 2000 Core Manager. (In the example shown in step 18, the hard disks are hdisk0 and hdisk7.)

20 Delete the CS 2000 Core Manager configuration database information for the CPU controller modules currently installed on the system:

```
ftcpuclean
```

21 Shut down the CS 2000 Core Manager and initiate a reboot:

```
shutdown -Fr
```

Note: The message: COLD start, appears within approximately 2 minutes.

22 Interrupt the boot process when the COLD start message appears by pressing the Break key.

Example response

```
FX-Bug>
```

23 Determine the current Greenwich Mean Time (GMT) setting on the existing CPU controller modules:

```
FX-Bug> time
```

Example response:

```
FRI NOV 16 18:41:49:00
```

Note: The time setting is the correct GMT setting. It does not necessarily reflect your site's local date and time.

24 Record the date and time response.

If you are using local time to set the GMT on the new CPU controller modules, use the response in step 23 to calculate the number of hours that your local time differs from GMT.

At the modular supervisory panel (MSP)

25 Interrupt power to the CS 2000 Core Manager by turning off the MSP breakers, located at the front of the MSP, which supply power

to the CS 2000 Core Manager. Proceed according to the chassis structure of your system.

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

At the front of the CS 2000 Core Manager

26 Replace the CPU controller modules using the procedure "Replacing a CPU controller module during an upgrade". When complete, return here, and continue with step 27.

At the MSP

27 Restore power to the CS 2000 Core Manager by turning on the MSP breakers. Proceed according to the chassis structure of your system.

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

When power is restored, both LEDs on the CPU controller modules turn on briefly, then turn off. This action is normal and indicates that the module is seated correctly, is receiving power, and has passed its self tests.

At the local or remote VT100 console

ATTENTION
Verify the keystrokes that are required to perform a "Break" on your VT100 console.

28 Interrupt the boot process when the COLD start message appears by pressing the Break key.

Note: The COLD start message appears within approximately 5 minutes.

29 If the following message appears after you press the Break key: `Break detected; Self test/boots about to begin; press <Break> anytime to abort all`, press the Break key again after the prompt to stop the self/boot process.

Example response:

```
FX-Bug>
```

30 Determine the current Greenwich Mean Time (GMT) setting on the new CPU controller modules:

```
FX-Bug> time
```

Example response:

```
FRI NOV 16 18:41:49:00
```

31 Determine if the GMT setting for the new CPU controller modules is correct.

If the GMT setting is	Do
incorrect	step 32
correct	step 33

CAUTION
Potential loss of service

Ensure that the GMT setting on the new CPU controller modules is later than the setting on the previous modules (recorded in step 24). Do not reboot the system if the GMT setting is earlier than the time of the shutdown. This action can corrupt the system configuration and status information.

32 Correct the time setting to the current GMT:

```
FX-bug> set <mmddyyhhmm>
```

where

mm is the numeric month of the year (01 to 12)
dd is the numeric day of the month (01 to 31)
yy is the last two digits of the current year (00 to 99)
hh is the current hour (01-12)
mm is the current minute (00 to 59)

33 Ensure that the environment parameters are set to the default values:

```
FX-bug> env;d
```

Example response:

```
Update with Auto-Configuration Defaults
Update Non-Volatile RAM (Y/N)?
```

34 Enter Y to confirm the NVRAM update.

Example response:

```
Reset Local System (CPU) (Y/N)?
```

35 Enter Y to reset the system.

36 Interrupt the reboot process by pressing the Break key.

Example response:

```
FX-bug>
```

37 Boot the CS 2000 Core Manager from disk:

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

Note: During this time, the CPU firmware is automatically upgraded.

If you	Do
return to the FX-bug prompt again	step 38
do not return to the FX-bug prompt again	step 39

38 Boot the CS 2000 Core Manager again:

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

39 At the login prompt, log in to the CS 2000 Core Manager a user authorized to perform config-admin actions.

40 Restore the bootlist:

```
bootlist -m normal <hdisk_x> <hdisk_y>
```

where

<hdisk_x> and <hdisk_y> are the two physical disks that provide rootvg storage, as recorded in step 19.

41 Check the CPU firmware for the CPU in domain 0:

```
ftbugver -l CPU-0
```

Note: The "**-l**" is a lower-case L.

42 Check the CPU firmware for the CPU in domain 1:

```
ftbugver -l CPU-2
```

Note: The "**-l**" is a lower-case L.

43 Access the maintenance interface:

```
sdmmtc
```

44 Access the hardware level:

```
hw
```

45 Check the CPU integration status:

```
querysdm flt
```

46 Once the CPU controller modules have been integrated, exit the maintenance level:

```
quit all
```

47 Force each CPU controller module to assume mastership to synchronize their clocks:

```
ftctl -switch
```

Repeat the command for the other CPU controller module.

48 Proceed according to whether you have upgraded or downgraded a module.

If you have	Do
upgraded a module	step 49
downgraded a module	step 53

49 View the current paging space to ensure that it is twice the memory size of the CPU:

```
lsps -a
```

Example response:

```
Page Space   Physical Volume   Volume Group   Size %Used  Active Auto  Type
hd6          hdisk0           rootvg         512MB   1    yes    yes   lv
```

This response is an example of the paging space for a 256-MByte CPU controller module. In the example, the Size column, which represents the memory size, indicates 512MB. This is twice the size of the CPU.

If the paging space is	Do
twice the size of the CPU	step 53
not twice the size of the CPU	step 50

50 Increase the paging space:

```
sdmconfig cpu
```

The paging space is now reset at twice the memory size of the CPU.

51 Verify the paging space has been increased:

```
lsps -a
```

Example response:

```
Page Space   Physical Volume   Volume Group   Size %Used   Active Auto Type
hd6          hdisk0            rootvg       1024MB 1       yes    yes   lv
```

This response is an example of the paging space for a 512-MByte CPU controller module. In the previous example, the Size column, which represents the memory size, shows a 1024MB paging size, which is twice the size of the CPU.

52 Use the following table to determine your next step.

If	Do
If the paging space did not increase	repeat steps 50 and 51. If, after repeating these steps the paging space still does not increase, contact your next level of support.
If the paging space did increase	step 53

At the MAP display

53 Access the SDM level of the MAP display:

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

Example response:

```
SDM ManB
```

54 Return the CS 2000 Core Manager to service:

```
rts
```

The system responds:

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

The system automatically returns all modules to service.

55 Ensure the CS 2000 Core Manager hardware and software applications have been restored to the previous in-service state (before the upgrade).

56 Investigate any CS 2000 Core Manager or CM alarms not recorded in pre-checks. For any alarms that cannot be resolved, contact your next level of support.

57 Return all billing streams to service. For each billing stream, complete steps 58 through 54.

58 Post the required billing stream:

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

where

<stream> is the name of the billing stream

59 Return the posted stream to service:

```
rts
```

60 Post each billing stream again (see step 58) and make sure that each stream is in-service (InSv).

61 Verify that billing is collecting records:

```
query <stream_name>
```

where

<stream_name> is the name of the billing stream, for example, ama.

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

If the number of records	Do
increased from the first query command (billing is working)	step 62
did not increase from the first query command (billing is not working)	contact your next level of support

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

—End—

Upgrading the CPU firmware

Purpose

Use this procedure to upgrade the CPU firmware after you have upgraded the CPU controller module, you must check the version of the firmware. If the CPUs do not have the current firmware version, you must perform a firmware upgrade. You can also perform this procedure at any time in order to check the status of the CPU firmware.

Prerequisites

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

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

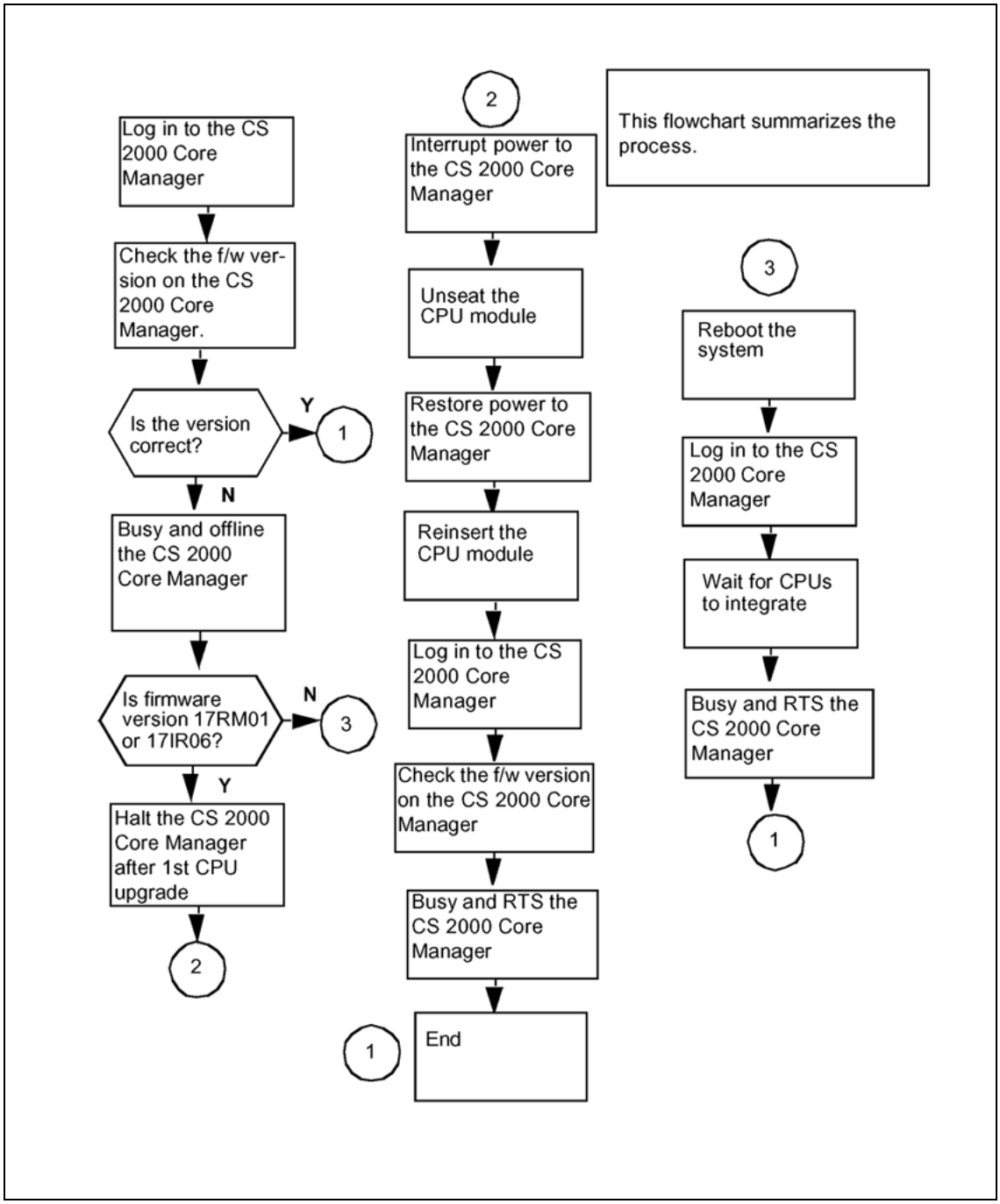
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Procedure

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Task flow for upgrading the CPU firmware



Procedure

ATTENTION

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

Upgrading the CPU firmware

Step	Action

At the CS 2000 Core Manager local VT100 console

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

2 Run the firmware process:

```
sdmfirmware
```

The system runs through the process and indicates whether a firmware upgrade is required. Record the current firmware version.

If the firmware	Do
needs to be upgraded	step 3
does not need to be upgraded	step 31

At the MAP

3 Access the SDM level:

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

4 Busy the CS 2000 Core Manager:

```
bsy
```

5 Confirm the busy command:

```
y
```

6 Take the CS 2000 Core Manager offline:

```
offl
```

At the CS 2000 Core Manager local VT100 console

7 Proceed with the firmware upgrade by pressing the Enter key.

If the firmware version noted in step 2	Do
is 17RM01	step 16
is not 17RM01	step 8

8 Print the instructions displayed on the system, so that you can execute them after the system has rebooted. Also note the CPU number.

9 Press the Enter key to reboot the system, and wait for the FX-Bug prompt.

10 At the FX-Bug prompt, enter:

```
FX-Bug> switch <cpu> ;h
```

where

`<cpu>` is the CPU number (0 or 2) from step 8

11 Boot the system:

```
FX-Bug> gevboot
```

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

At the CS 2000 Core Manager VT100 console

13 Run the firmware process:

```
sdmfirmware
```

14 Wait for the CPU modules to integrate.

15 Press the Enter key to continue, and go to step 33.

At the CS 2000 Core Manager VT100 console

16 Before you halt the CS 2000 Core Manager, record the CPU that the system has directed you to pull.

The system prompts you to halt the CS 2000 Core Manager after the firmware upgrade on one CPU is complete. The system also indicates that you must pull the CPU after the halt is complete.

17 Halt the CS 2000 Core Manager by pressing the Enter key.

18 Wait for the halt to complete before continuing the procedure.

If	Do
the system does not halt	step 19
halts	step 22

19 Halt the CS 2000 Core Manager again. Interrupt the reboot process to access the FX-Bug prompt by pressing the Break or Esc key several times.

20 When the CS 2000 Core Manager is at the FX-Bug prompt, interrupt the power to the CS 2000 Core Manager.

21 Under some circumstances, the CS 2000 Core Manager reboots and does not halt. If this happens, wait for the reboot to complete, log into the CS 2000 Core Manager, and halt the SDM again.

At the MSP

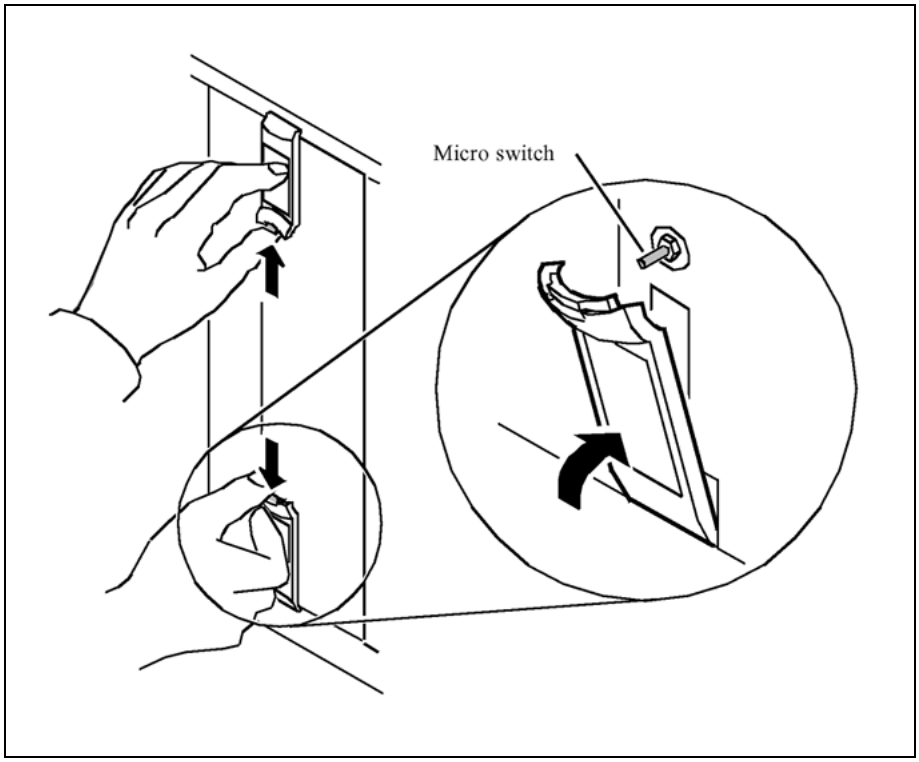
22 Interrupt power to the CS 2000 Core Manager by turning off both of the MSP breakers. The MSP breakers, located at the front of the MSP, supply power to the CS 2000 Core Manager.

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

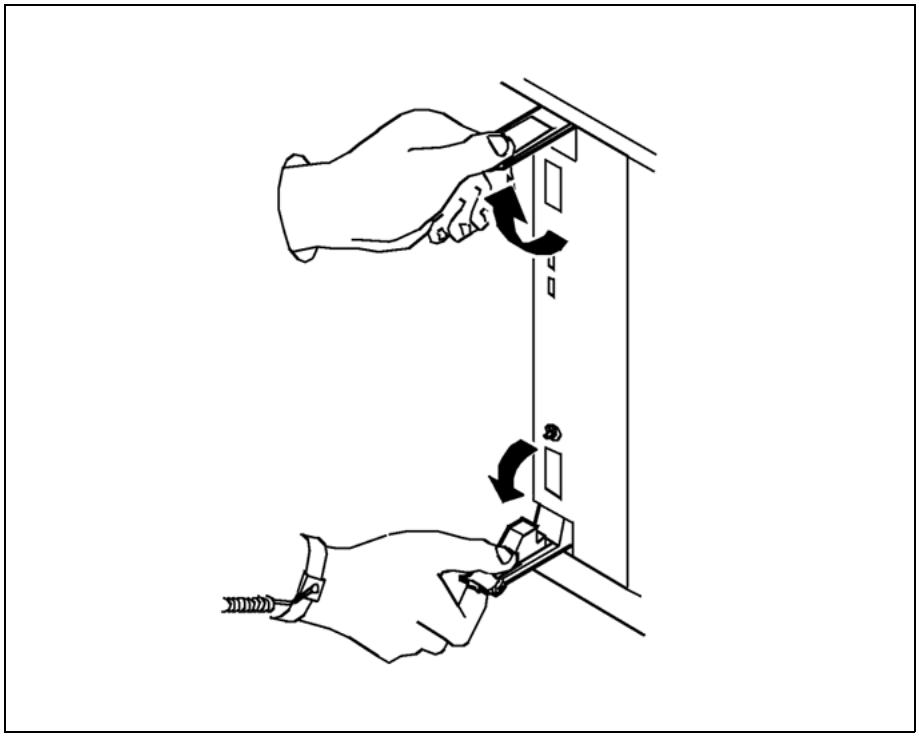
At the front of the CS 2000 Core Manager

23 Unscrew the thumbscrews located on the top and bottom of the CPU module noted in step 16. The thumbscrews are the captive type, and you cannot remove them from the module.

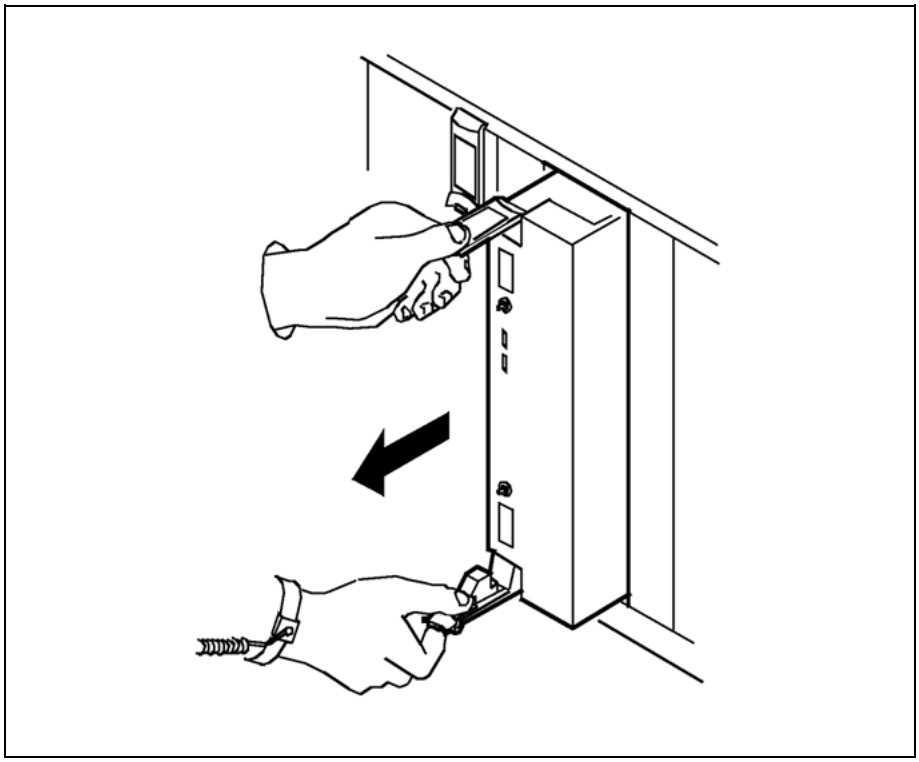
24 Depress the tips of the locking levers on the face of the CPU module.



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



26 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



At the MSP

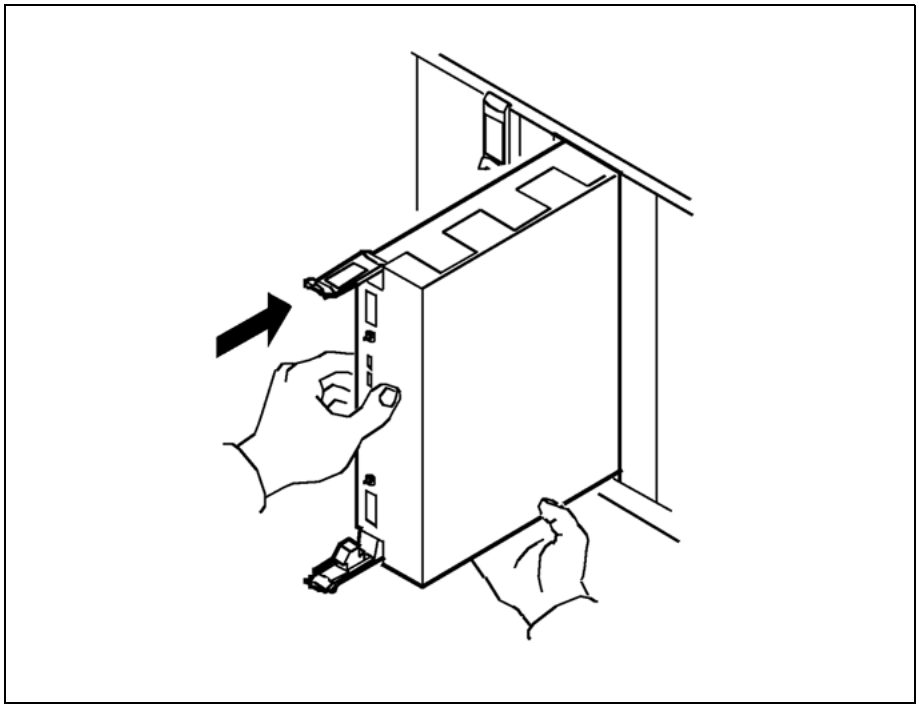
27 Restore the power to the CS 2000 Core Manager by turning on the MSP breakers, according to the chassis structure of your system.

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

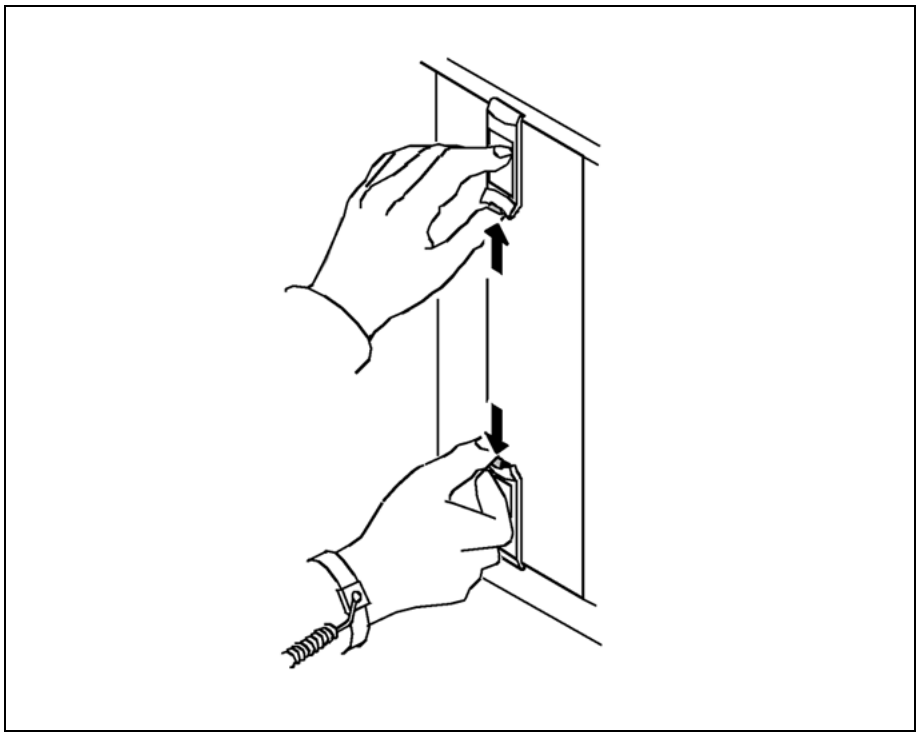
Note: Wait at least 15 seconds before re-inserting the pulled CPU.

At the front of the CS 2000 Core Manager

28 After 15 seconds, gently push the CPU module that you pulled out in step 26 back into the slot.



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



30 Tighten the thumbscrews on the module.

When you put the CPU controller module back into the slot, both LEDs on the module turn on briefly and then off. This action indicates that

- you have seated the module correctly
- the module is receiving power
- the module has passed all self-tests

At the local VT100 console

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

The firmware on the other CPU is upgraded automatically when you log into the CS 2000 Core Manager, dependent on the successful completion of step 7, *followed by steps* 16 *through* 30.

32 Once the system indicates that the CPU modules have fully integrated with the CS 2000 Core Manager, and that they have the correct firmware, press the Enter key to continue the procedure.

33 Return the CS 2000 Core Manager to service:

```
rts
```

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

—End—

Installing an X.25 controller module and personality module

Purpose

Use this procedure if you have an MFIO hardware module and want to upgrade the CS 2000 Core Manager to incorporate an X.25 controller module (NTRX50FY) and an X.25 personality module (NTRX50FZ).

Prerequisites

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

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

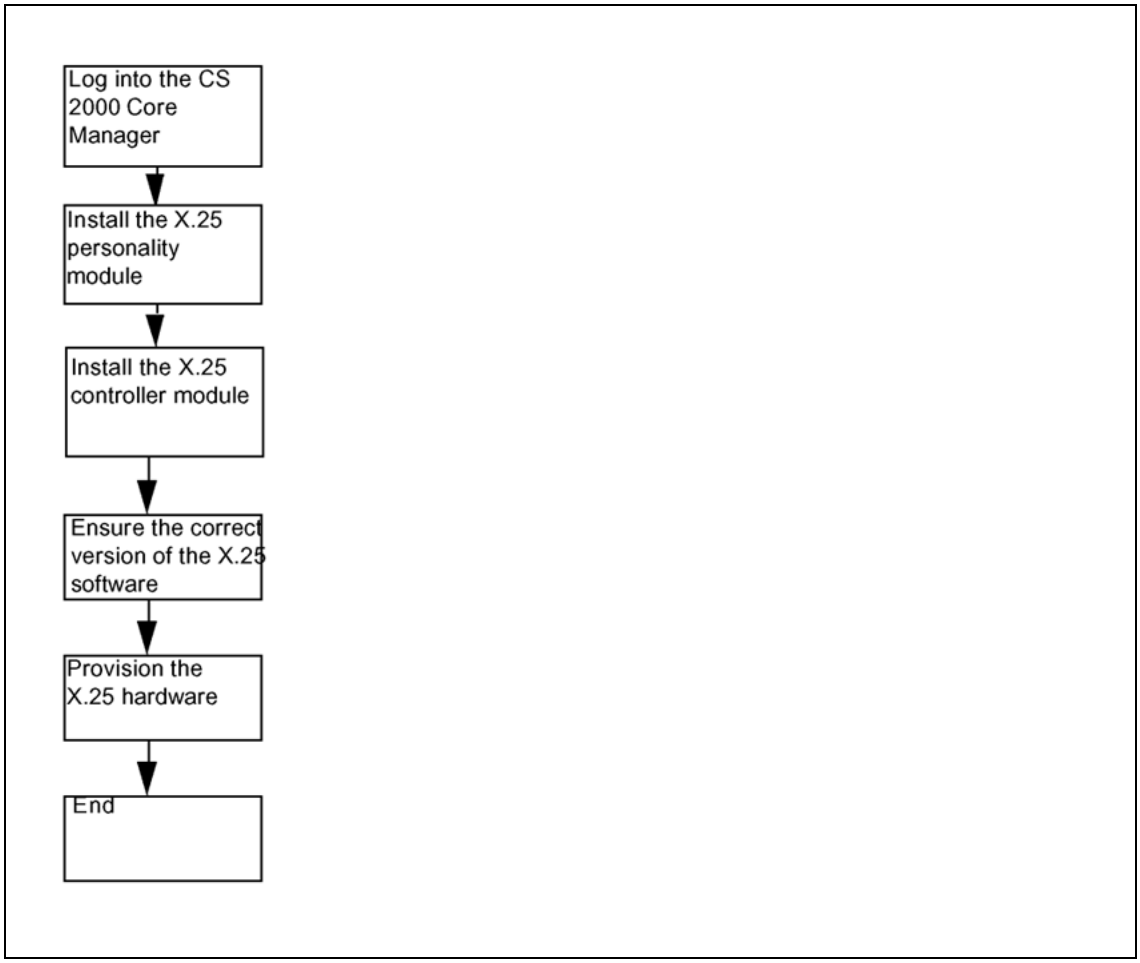
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Task flow diagram

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedures that follow the flowchart to perform the tasks.

Task flow for Installing an X.25 controller module and personality module



Procedures

ATTENTION

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

Installing an X.25 controller module and personality module

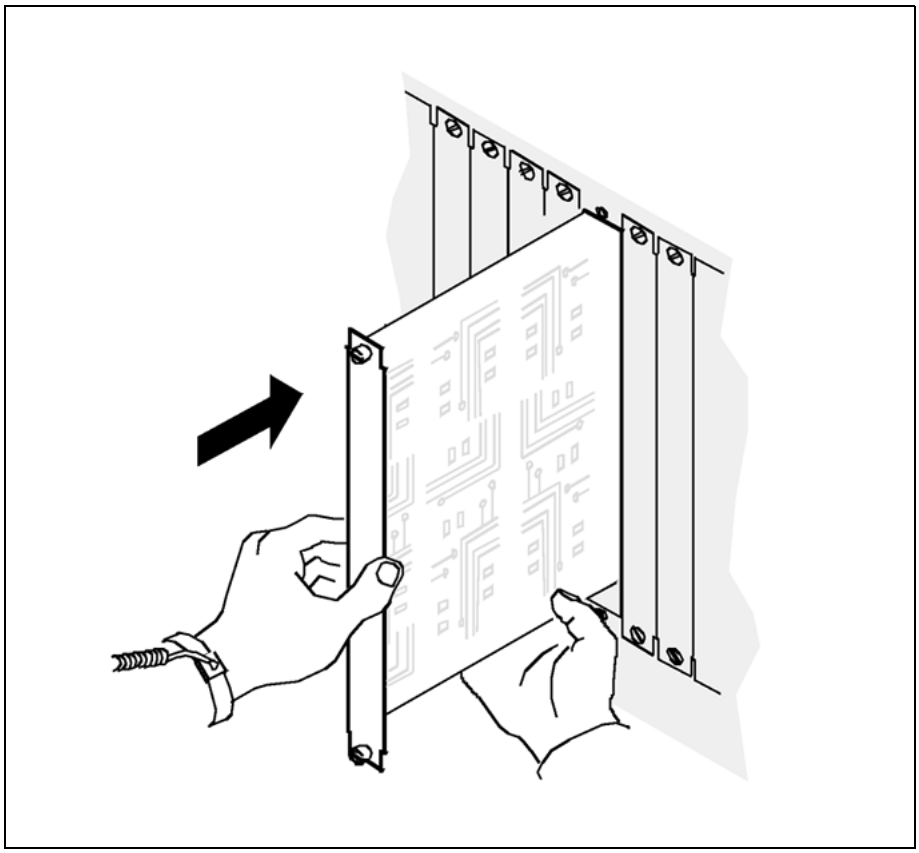
Step	Action

At the back of the CS 2000 Core Manager

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.

1 Insert the new X.25 personality module into the CS 2000 Core Manager shelf.

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



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

At the front of the CS 2000 Core Manager

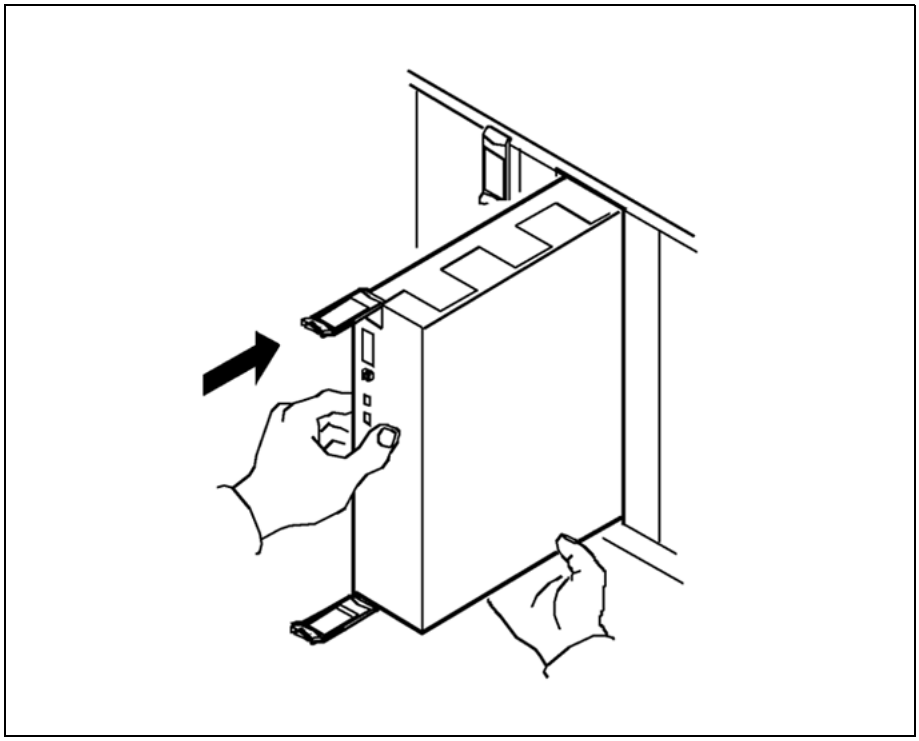
4 Put on an electrostatic discharge grounding wrist strap.

5 Remove the filler plates covering the slots where you will install the new modules.

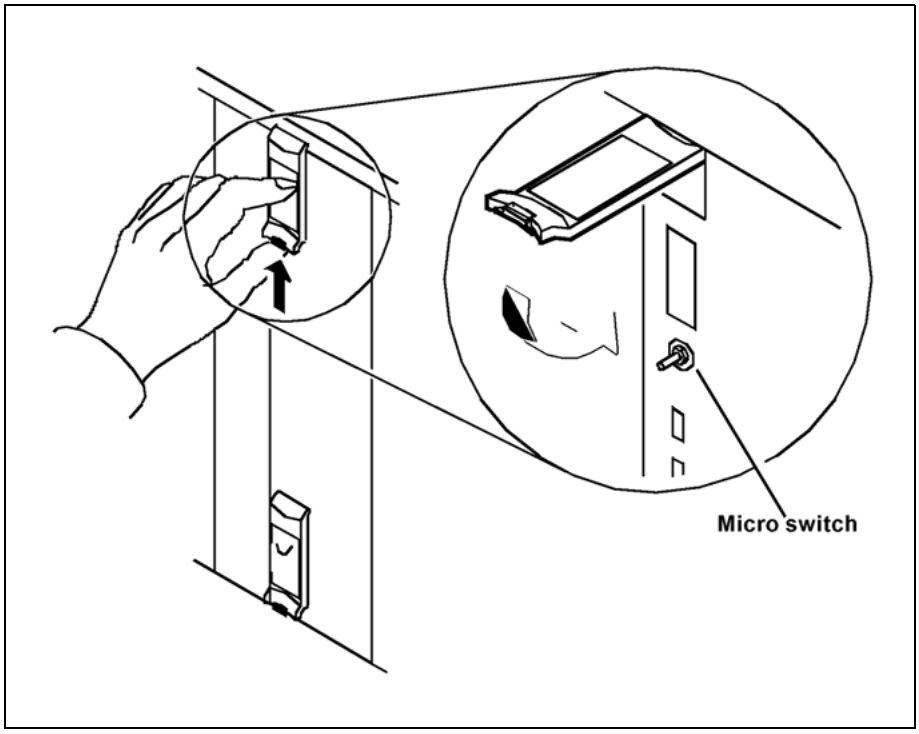
6 Determine whether you are installing a single X.25 module or two X.25 controller modules as a logical pair in either the main or expansion chassis.

- If you are installing a single X.25 module, you must install it on domain 0.
- If you are installing an X.25 pair, the two slots used must be exactly 8 slot positions apart (for example, slots 1 and 9, or 2 and 10) and both modules in a logical pair must have the same PEC.

7 Insert the X.25 controller module(s) into the CS 2000 Core Manager shelf. Gently slide the module into the shelf until it is fully inserted.



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



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

—End—

ATTENTION

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

Provisioning the X.25 hardware

Step	Action
	At the local or remote VT100 console
1	Log in to the CS 2000 Core Manager as a user authorized to perform config-admin actions.
2	Ensure that the latest version of the X.25 software is available on the system. Insert the tape labeled: for the new software load, into slot 2 and wait until the tape drive stabilizes (yellow LED is off) before you proceed.
3	Access the maintenance interface: `sdmmtc`

4 Display the contents of the tape:

```
apply 0
```

5 Install the X.25 software:

```
apply bundle x25
```

6 Confirm the command:

```
y
```

Example response:

```
Command completed with no errors
```

7 Access the hardware level of the Maintenance Interface:

```
hw
```

8 Add the X.25 hardware:

```
add <chassis> <slot> <PEC> [SIMPLEX]
```

where

<chassis> is sdmm for the main chassis, and sdme for the expansion chassis
<slot> is the slot number of the X.25 card in domain 0
<PEC> is the PEC code of the X.25 controller module (NTRX50FY)
[SIMPLEX] is an optional parameter. Enter this parameter if you are installing only one X.25 module on the system.

Example response:

```
Add sdme 5 ntrx50fy - Command complete.
```

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

—End—

Removing a standalone X.25 interface

Purpose

Use this procedure to remove the following X.25 hardware modules from the CS 2000 Core Manager:

- NTRX50FY - X.25 controller module
- NTRX50FZ - X.25 personality module

CAUTION
If you delete only one X.25 controller module, it must be the X.25 controller module in domain 1.

Prerequisites

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

To perform this procedure, you must obtain the following information:

- the chassis (SDMM for main chassis; SDME for expansion chassis) for the installed X.25 module(s)
- the slot number of the X.25 controller module(s)

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

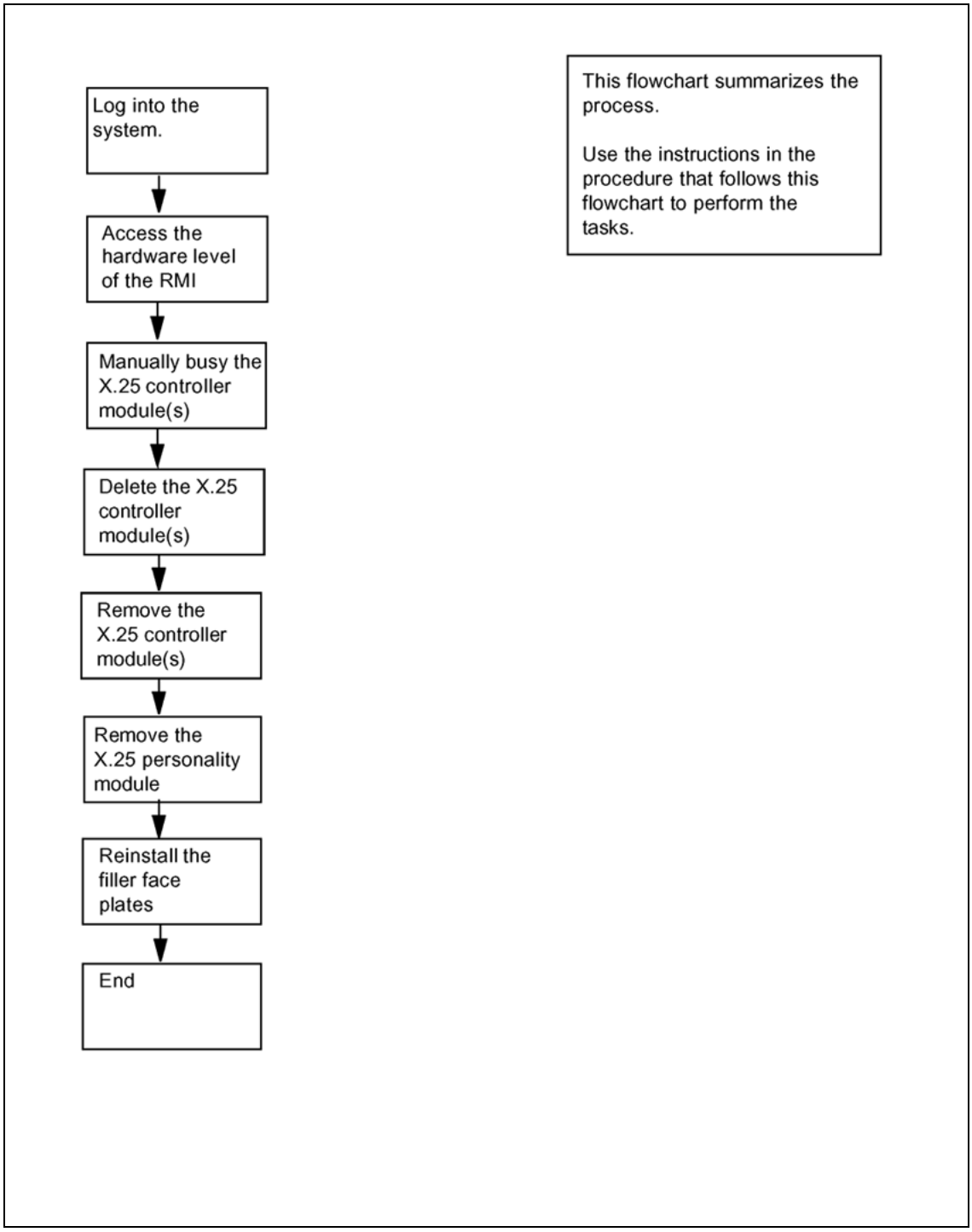
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Task flow diagram

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

Task flow for Removing the standalone X.25 interface



Procedure

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

Removing a standalone X.25 interface

Step	Action

At the local or remote VT100 console

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

2 Access the top menu level of the remote maintenance interface (RMI):

```
sdmmtc
```

3 Access the hardware (Hw) menu level:

```
hw
```

CAUTION
Deleting an X.25 controller module requires you to put the module into a ManB state. These modules will not be in service. If you are deleting only one X.25 module, put only the module in domain 1 in the ManB state.

4 Manually busy the module in each domain:

bsy <domain> X25

where

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

Example: bsy 1 X25

Example response:

```
Hardware Bsy - Domain 1 Device X25
This action will bring service down for all X.25 Ports
in I/O domain 1.
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

5 Confirm the Bsy command:

```
y
```

Example response:

```
Hardware Bsy :  Command submitted.  Hardware Bsy :
Domain 1 Device X25.
```

6 When the Bsy command is finished, observe that the message: `Please wait`, along the command confirmation disappear. The status of the domain transitions from initiated to submitted and finally to complete.

Example response:

```
Hardware Bsy :  Domain 1 Device X25 - Command complete.
```

7 Use the following table to determine your next step.

If	Do
you have not yet manually busied the module(s) you wish to delete	step 4
you have manually busied the module(s) you wish to delete	step 8

Note: After you see the response to the Bsy command, the X.25 controller module state changes to M at the hardware menu level of the RMI.

8 Use the Locate command to determine the chassis and slot number of the module to delete. Use the Enter key to scroll through the display:

`locate`

Example response:

```
Site Flr RPos Bay_id Shf   Description Slot Eq PEC
HOST 00  00   CSDM          SDME X25(0)  05 NTRX50FY
FRNT HOST 00  00  CSDM          SDME X25    05
NTRX50FZ BACK HOST 00  00  CSDM          SDME X25(1)
13 NTRX50FY FRNT HOST 00  00  CSDM          SDME
X25    13 NTRX50FZ BACK
```

Note: The example shown only displays part of the information generated from the Locate command.

9 Delete the module:

`delete <chassis> <slot> [SIMPLEX]`

where

`<chassis>` is the chassis where the module is located (SDMM for the main chassis or SDME for the I/O expansion chassis)
`<slot>` is the slot number (from 1 to 16) where the module is located

[SIMPLEX] is an optional parameter. Enter this parameter if you are deleting only one X.25 module from the system.

ATTENTION

If you do not specify SIMPLEX, the module in the corresponding slot of the other domain is also deleted.

Example 1: Deleting only one module

delete sdme 13 SIMPLEX

Example 1 response:

```
Module in slot 13 of SDME will be deleted.
X.25(1) will be deleted.
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

Example 2: Deleting both modules

delete sdme 5

Example 2 response:

```
Module in slot 5 of SDME will be deleted.  X.25(0) will
be deleted.  Module in slot 13 of SDME will also be
deleted.  X.25(1) will be deleted.
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

10 Confirm that this is the module you want to delete:

y

The delete command can take several minutes to complete. When the command is finished, the following message is displayed:

Example 1 response

If you are deleting both modules, after a few seconds the module disappears from the listing shown at the hardware menu level of the RMI. If you are deleting one module, domain 1 will show a dash at the hardware menu level of the RMI.

```
Delete sdme 13 SIMPLEX - Command complete.
```

Example 2 response

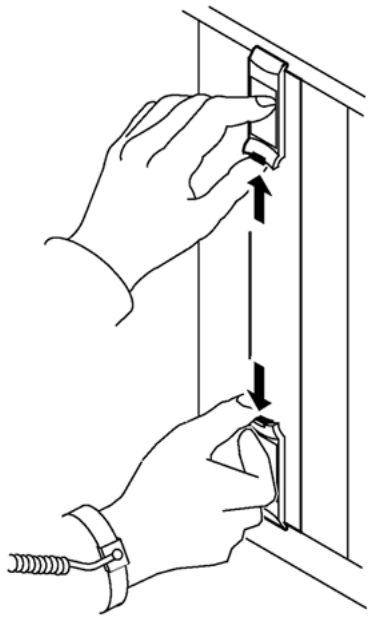
```
Delete sdme 5 - Command complete.
```

At the front of the CS 2000 Core Manager

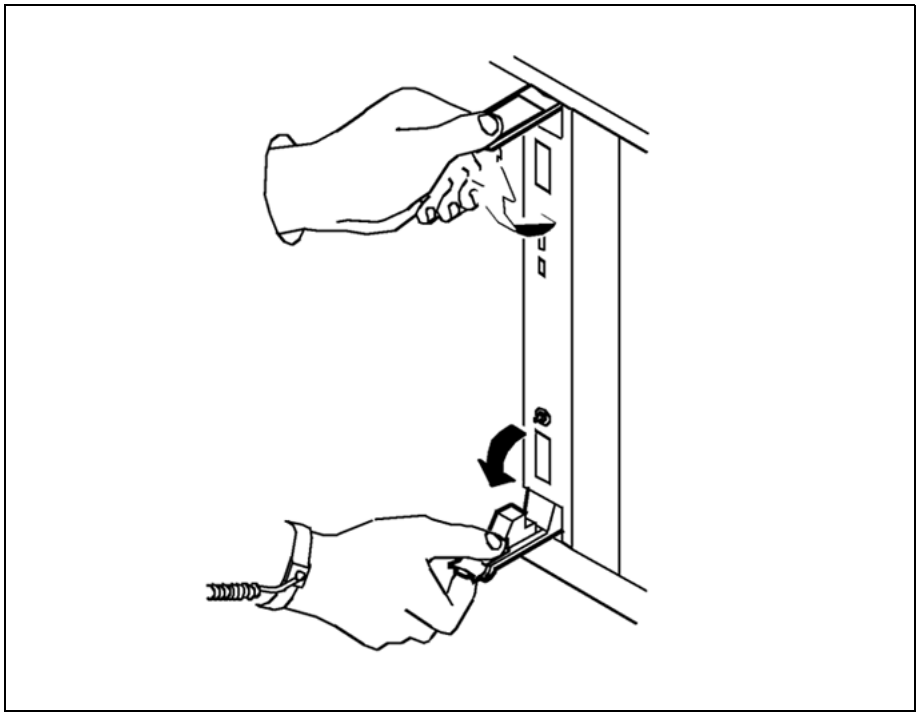
11 Wear an electrostatic discharge grounding wrist strap and connect the clip to the chassis ground.

CAUTION
Damage from Static Electricity
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.

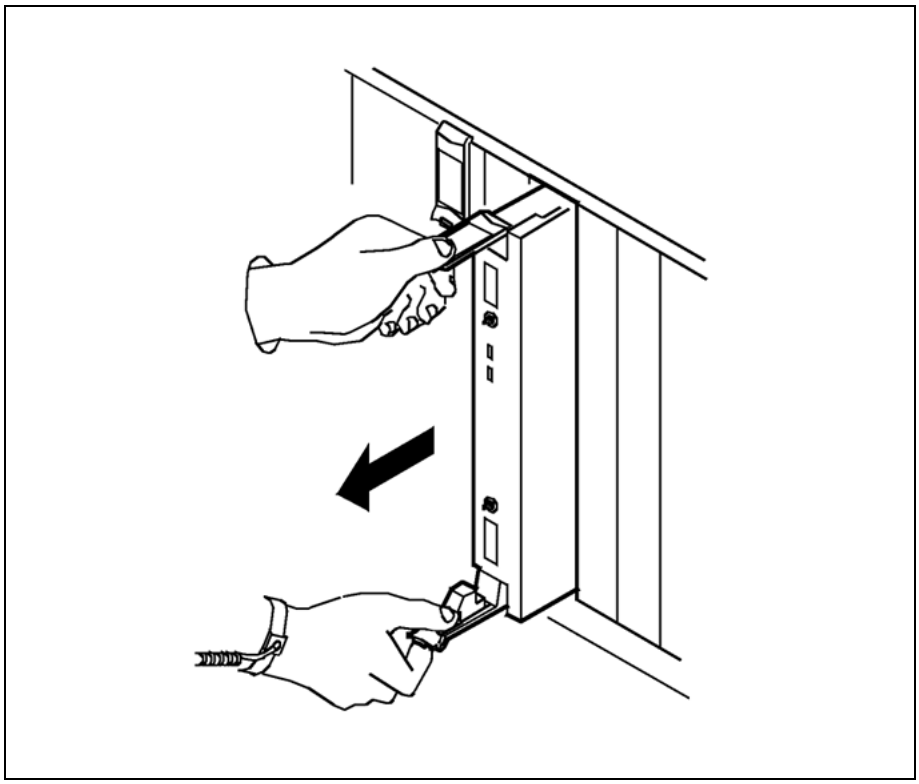
12 Depress the tips of the locking levers on the face of the X.25 controller module.



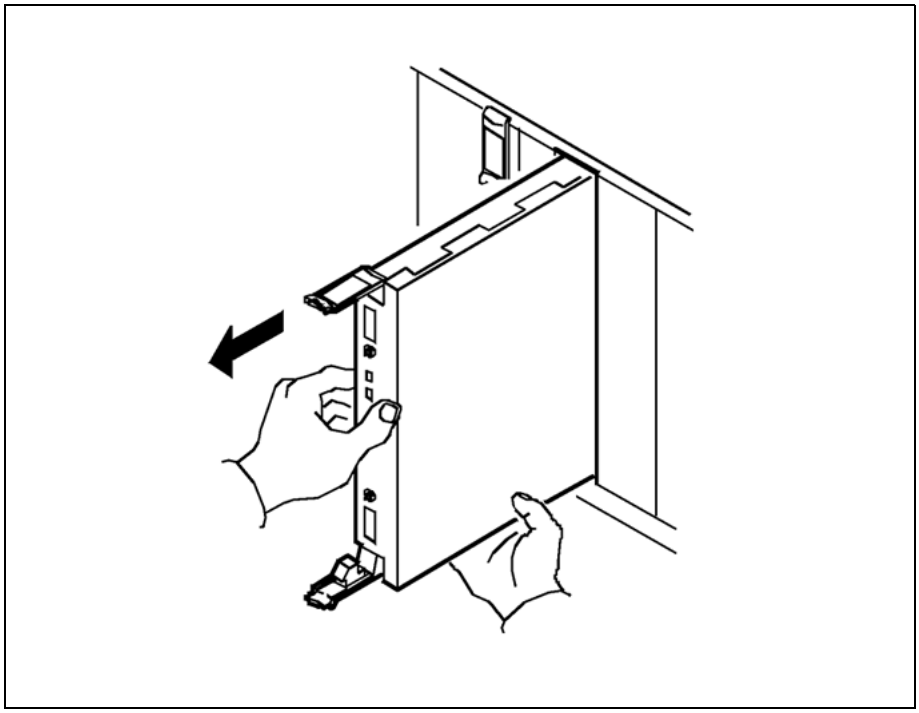
13 Open the locking levers on the face of the module by moving the levers outwards.



14 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the 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.

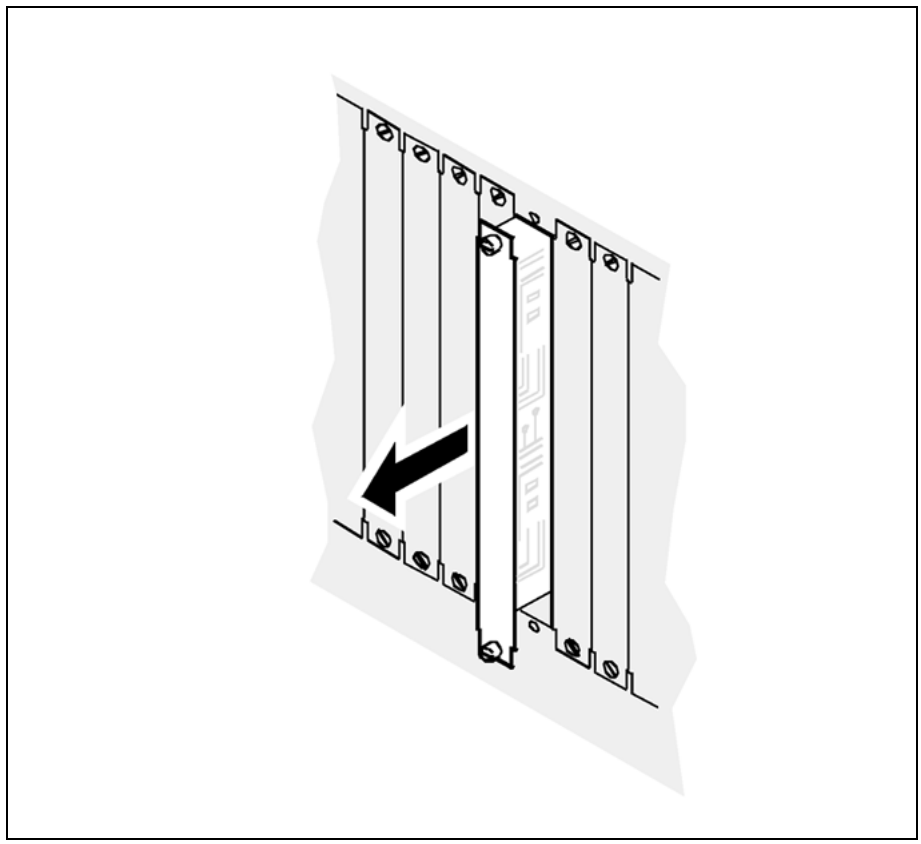
At the rear of the CS 2000 Core Manager

17 Disconnect one or both X.25 modem connection cables from the X.25 personality module, depending on whether the X.25 module is commissioned to use one or both of its X.25 ports.

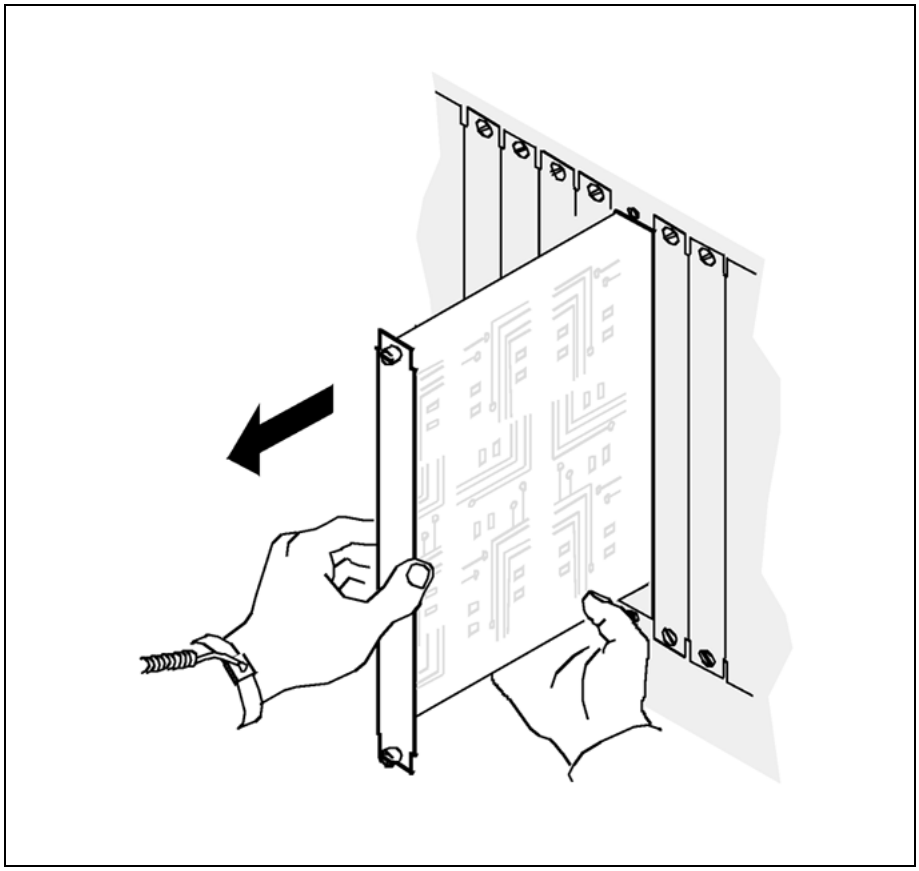
18 Loosen the two captive type thumbscrews located at the top and the bottom of the X.25 personality module.

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

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



20 Hold the X.25 personality 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 X.25 personality module you have removed in an ESD protective container.

22 Reinstall the filler plates covering the slots from which you removed the modules.

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

—End—

Removing X.25 from your system

Purpose

This procedure only applies to SYNC X25 modules (standalone), and does not apply to X25 as part of the UMFIOs. The process of removing X.25 from the system has three phases:

- Removing the X.25 modules from the system (this procedure)
- Deleting the X.25 software (this procedure
- Removing the X.25 hardware modules from the SDM CS 2000 Core Manager(refer to the procedure "Removing a standalone X.25 interface" (page 271))

Procedures

Removing X.25 modules from the system

Step	Action
	At the SDMCS 2000 Core Manager
1	Log in to the SDMCS 2000 Core Manager as the root user.
2	Stop the X.25 daemon: `# /etc/rc.psx25 stop`
3	Take the X.25 controller module offline: `# modchange -ol SYNC- <domain_num> -y` where `<domain_num>` is the domain number (0 or 1) of the X.25 controller module that you are taking offline • 0 if the module is located in one of the slots from in one of the slots from — 1 to 6 on the main chassis, or — 1 to 8 on the expansion chassis • 1 if the module is located in one of the slots from in one of the slots from — 10 to 16 on the main chassis, or — 9 to 16 on the expansion chassis Example of command:

 # modchange -ol SYNC-0 -y

The system responds with warnings about the items that are about to go offline:

```
Warning:  This request will not allow SYNC-0 to stay
online.
Warning:  This request will not allow pgen-0 to stay
online.
Warning:  This request will not allow SYNC-PM to stay
online.
```

4 Take the X.25 personality module offline:

 # modchange -ol SYNCPM- <domain_num>

where

<domain_num> is the domain number (0 or 1) of the X.25 personality module that you are taking offline.

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

Example of command:

modchange -ol SYNCPM-0

5 Take the logical device offline:

 # modchange -ol pgen <domain_num>

where

<domain_num> is the domain number (0 or 1) of the logical device that you are taking offline

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

— 10 to 16 on the main chassis, or

— 9 to 16 on the expansion chassis

Example of command:

modchange -ol pgen0

6 Delete the logical device:

 # rmdev -dRl pgen <domain_num>

where

<domain_num> is the domain number (0 or 1) of the logical device that you are deleting:

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

Example of command:

rmdev -dRl pgen0

Example response:

```
pgen0 deleted
```

7 Delete the X.25 controller module:

 # rmdev -dRl SYNC- <domain_num>

where

<domain_num> is the domain number (0 or 1) of the controller module that you are deleting:

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

— 10 to 16 on the main chassis, or

— 9 to 16 on the expansion chassis

Example of command:

rmdev -dRl SYNC-0

Example system response:

```
SYNCPM-0 deleted
SYNC-0 deleted
```

8 Repeat steps 3 through 7 for each X.25 module installed in the system.

CAUTION
Loss of service
Do not delete the X.25 software until you have removed all X.25 modules from the system using steps 3 through 7.

9 Delete the X.25 software:

```
# /usr/lpp/psx25/tmp/psx25_remove
```

The system can take several minutes to remove X.25 software. During this time the screen can display messages indicating that filesets are being removed from the system. The command prompt appears when all X.25 software is removed.

10 Remove all X.25 hardware installed on the system using procedure "Removing a standalone X.25 interface" (page 271).

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

—End—

Adding I/O controller modules

Purpose

Use this procedure to add one of the following hardware modules to the CS 2000 Core Manager:

- NTRX50FU - I/O controller module with two 2-Gbyte disk drives and Ethernet
- NTRX50GP - I/O controller module with two 4-Gbyte disk drives and Ethernet
- NTRX50NL - I/O controller module with two 36-Gbyte disk drives and Ethernet
- NTRX50NY - X.25 controller module

Application

I/O controller modules do not require LAN personality modules (NTRX50FS) installed at the back of the CS 2000 Core Manager except for the mandatory NTRX50GN I/O controller modules located in slots 2 and 3, and 13 and 14.

Slot positions

I/O controller modules can be added to slots 4 and 5, and 15 and 16, of the CS 2000 Core Manager main chassis, and added to unoccupied slots in the I/O expansion chassis.

All available slots can be used in the I/O expansion chassis to install two I/O controller modules as a logical pair. However, the left slot position of the left I/O controller module must be 8 slot positions apart from the left slot position of the right I/O controller module of the pair.

For example, if the left I/O controller module of the pair occupies slots 1 and 2, the right I/O controller module must occupy slots 9 and 10. Both modules in a logical pair must have the same PEC.

LAN personality module

The rear LAN personality module I/O controller module must occupy the lower number of the two rear slots that are associated with the front module. For example, if the new I/O controller module occupies front slots 4 and 5, its associated LAN personality module must be installed in rear slot 4. The unused rear slots remain covered by filler plates.

Prerequisites

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

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

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

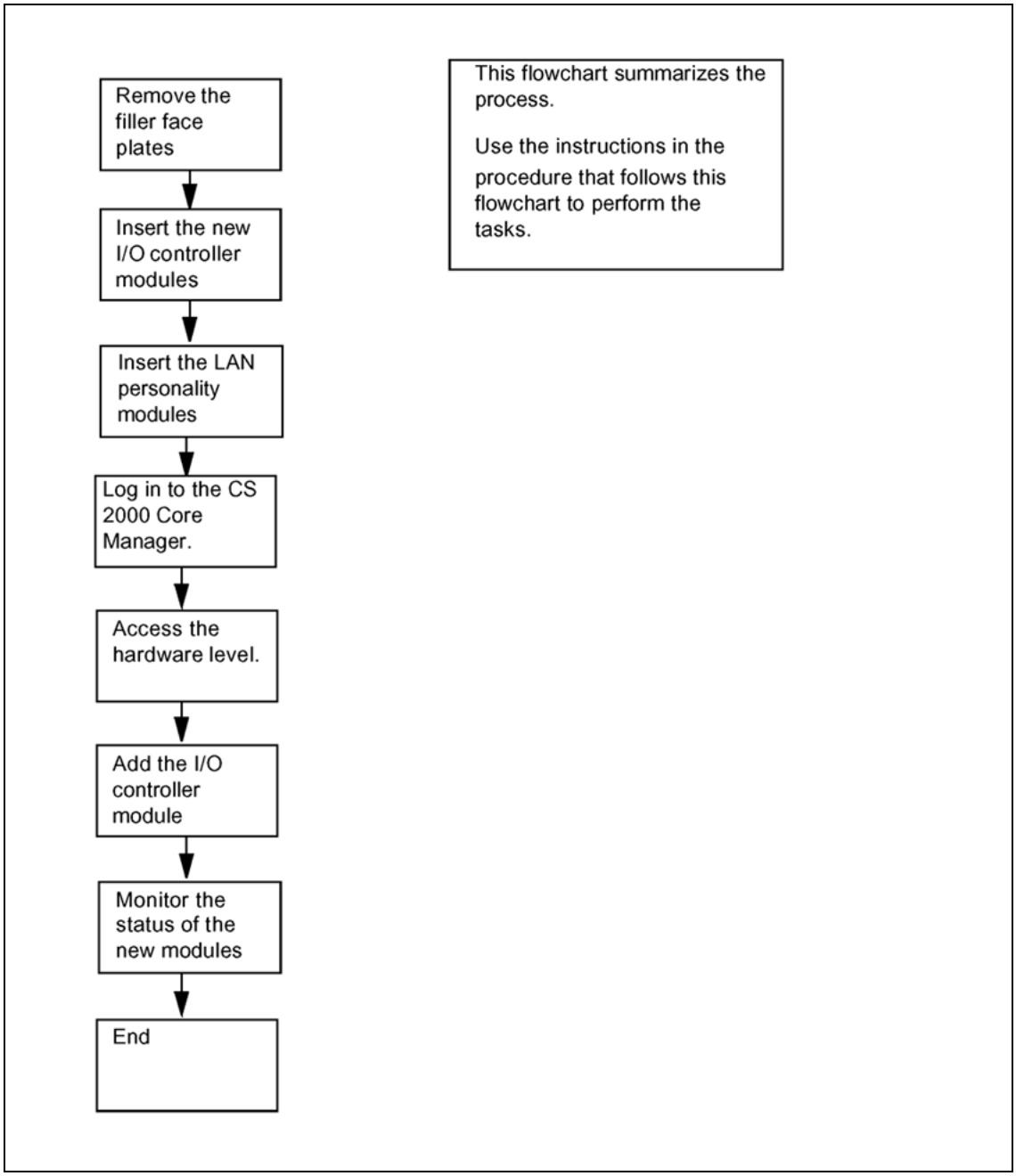
To perform this procedure, you must have the following information:

- the chassis type (SDMM for a main chassis; SDME for an I/O expansion chassis) used for housing the modules
- the I/O controller module's slot number (from 1 to 16)
- the I/O controller module's product engineering code (PEC)

Procedure

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

Task flow for Adding I/O controller modules



Procedure

ATTENTION

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

Adding I/O controller modules

Step	Action

At the front of the CS 2000 Core Manager

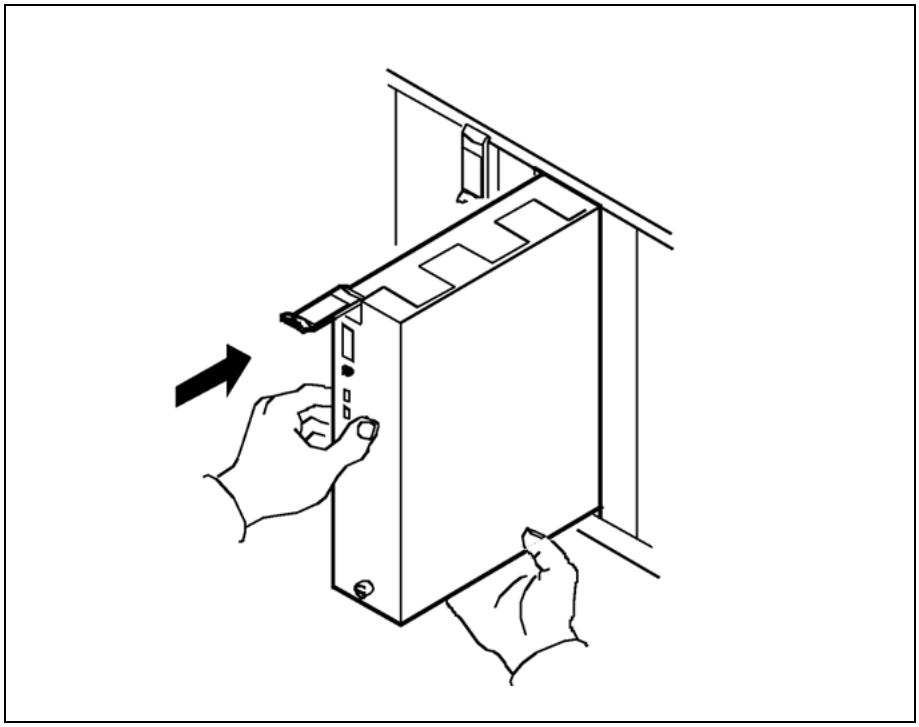
1 Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module.

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.

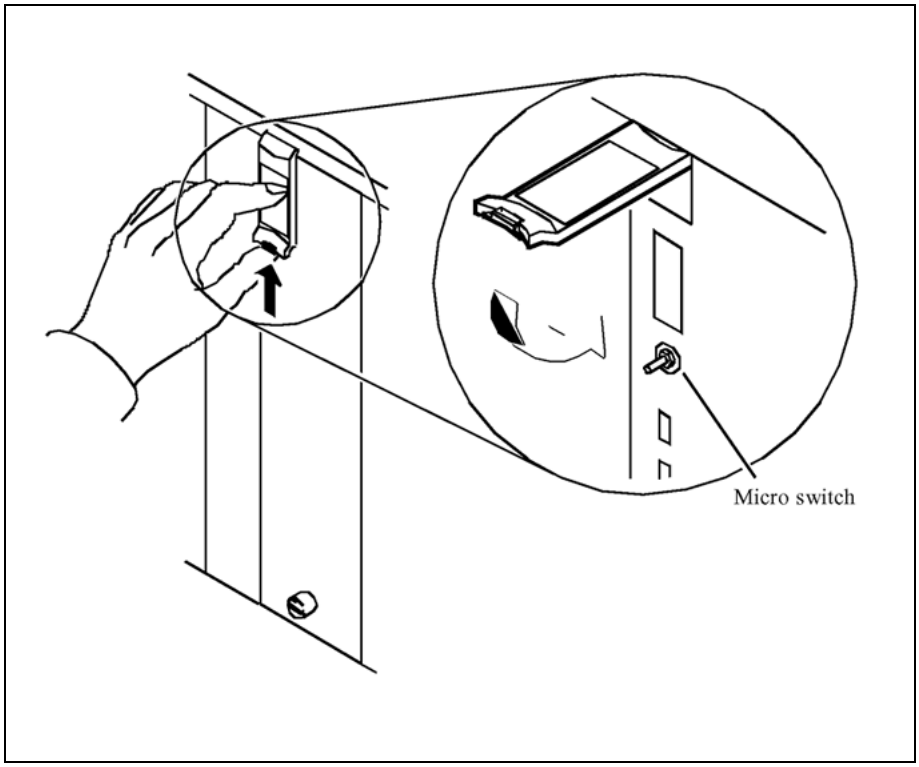
2 Remove the filler plates covering the slots in which you will install the new modules.

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

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



5 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.



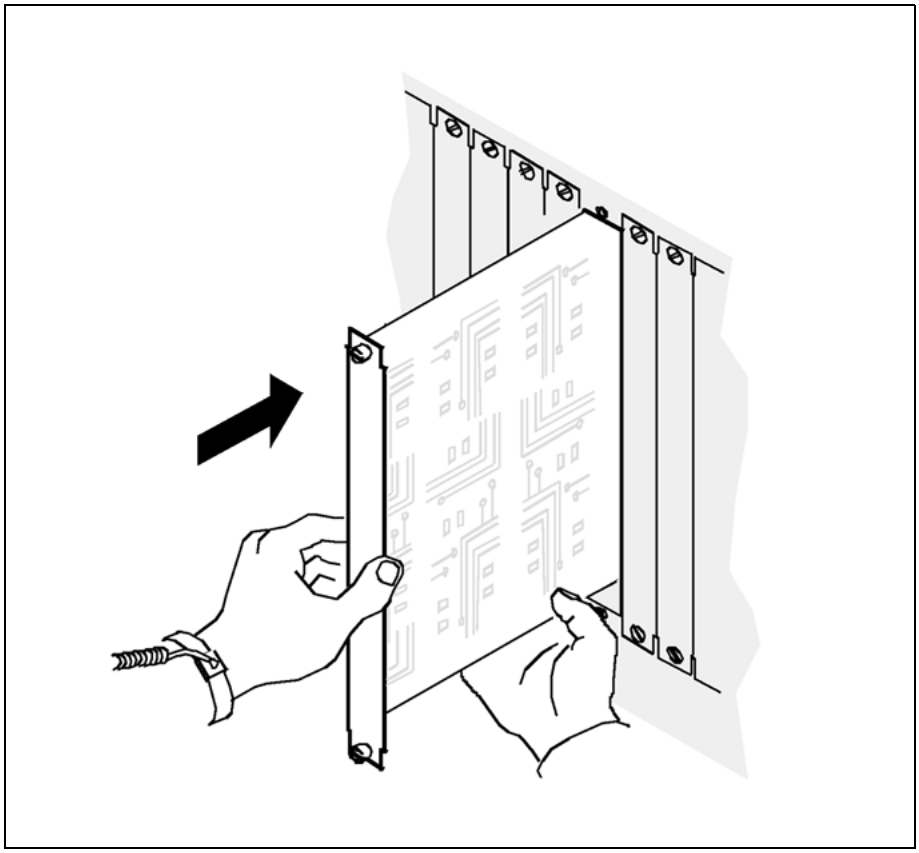
6 Tighten the thumbscrews on the module.

If you	Do
need to install a LAN personality module	step 7
do not need to install a LAN personality module	step 10

At the back of the CS 2000 Core Manager

7 Insert the new LAN personality module into the CS 2000 Core Manager shelf.

8 Gently slide the LAN personality module into the shelf until it is fully inserted.



9 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

At the local or remote VT100 console

10 Log in to the CS 2000 Core Manager as a user authorized to perform config-admin actions.

11 Access the maintenance interface:

```
sdmmtc
```

12 Access the hardware (Hw) level:

```
hw
```

13 Add the logical pair of I/O controller modules simultaneously:

```
add <chassis> <slot> <pec>
```

where

<chassis> is the chassis where the module will be located (SDMM for a main chassis or SDME for an I/O expansion chassis)
<slot> is the lower of the two physical slot numbers the module occupies

<pec> is the product engineering code (PEC) of the I/O controller module you want to add

Note: To add a single I/O controller module to domain 0, use the command: **add <chassis> simplex <slot> <pec>**

14 The add command can take several minutes to complete. When the command is finished, the following message is displayed:

Example response:

```
Hardware Add Module - Command complete.
```

15 Monitor the status of the new hardware at the hardware (Hw) level.

The system does not initially show the new hardware that has been added.

```
          I F C E D 5 D X
           C A P T S 1 A 2
           M N U H K 2 T 5
Domain 0  . . . . . . . .
Domain 1  . . . . . . . .
```

The system takes a few seconds to display the new hardware elements (DSKn for hard disks). Previously installed disks on the system are automatically renumbered as necessary to reflect the new hardware configuration. The status of the new hardware elements can initially appear as F (failed).

Example response:

```
         I F C E D D D D 5
          C A P T S S S A 1
          M N U H K K K T 2
                  1 2 3
Domain 0 . . . . . F F . .
Domain 1 . . . . . F F . .
```

The modules are automatically put into service and their status changes to in-service (indicated by the in-service dot).

Example response:

```
         I F C E D D D D 5
          C A P T S S S A 1
          M N U H K K K T 2
                  1 2 3
Domain 0 . . . . . . . . .
Domain 1 . . . . . . . . .
```

16 If necessary, use the Locate command to verify slot numbers since devices have been renumbered.

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

—End—

Removing I/O controller modules

Purpose

Use this procedure to delete the following hardware modules from the CS 2000 Core Manager:

- NTRX50FU - I/O controller module with two 2-GByte disk drives and Ethernet
- NTRX50GP - I/O controller module with two 4-GByte disk drives and Ethernet

ATTENTION

Contact Nortel personnel before you remove any I/O controller modules. You cannot remove I/O controller modules until Nortel deletes the data volume group (datavg) to which the module belongs. Nortel also recommends that you remove I/O controller modules in pairs.

If necessary to change or correct the physical location of the modules, this procedure can be followed by the procedure "Removing I/O controller modules" (page 293)

Note: The I/O controller modules (NTRX50GN) in slots 2 and 3, and 13 and 14, of the main chassis are mandatory for system operation and cannot be removed.

CAUTION
Removing a module
Do not delete modules that are part of a volume group. If the module is not part of a volume group, continue with this procedure.

CAUTION
Re-using an I/O controller module
An I/O controller module must be manually busied and deleted before it can be re-used in a different slot.

Prerequisites

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

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

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

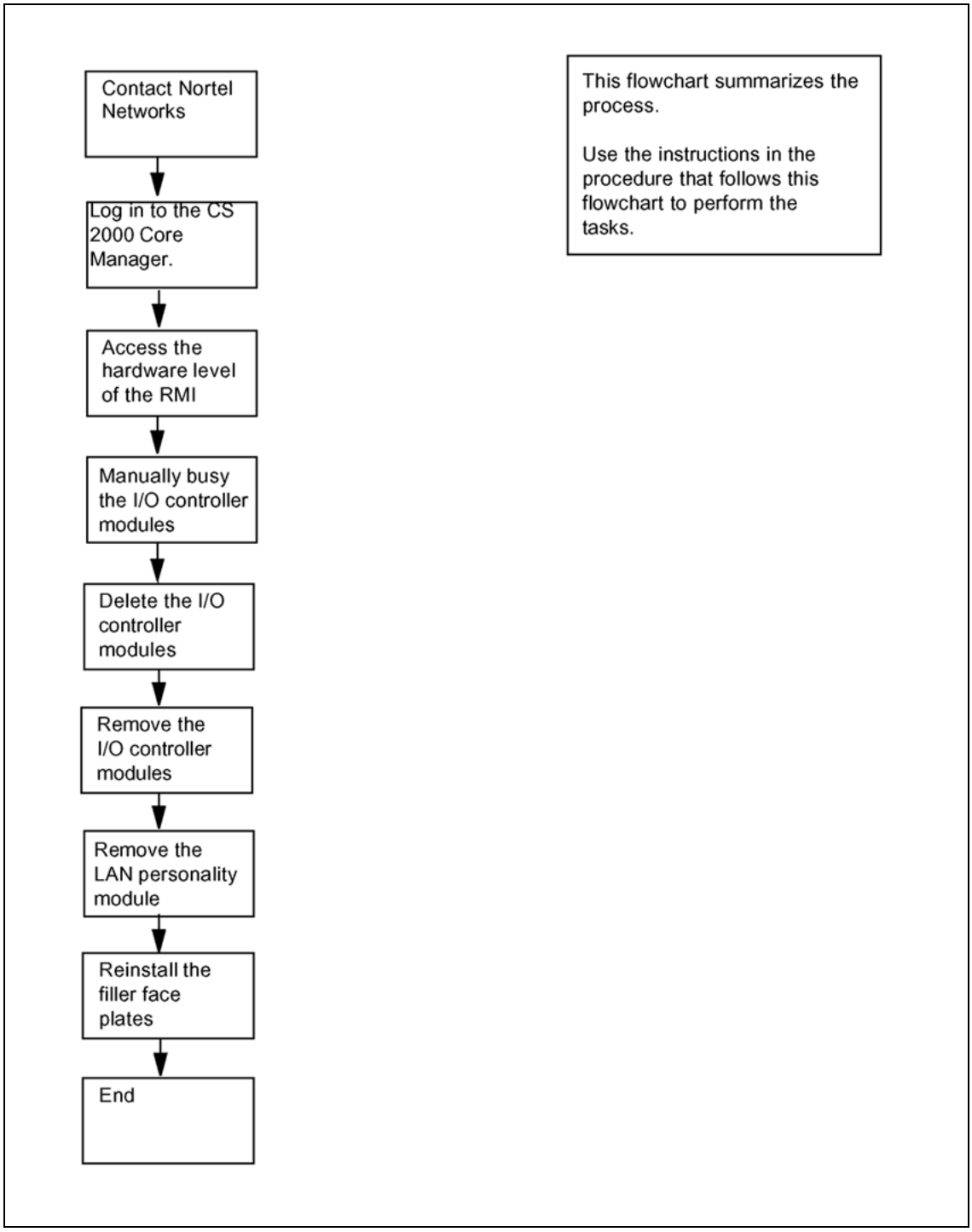
To perform this procedure, you must know the following information:

- the chassis (SDMM for main chassis; SDME for I/O expansion chassis) where the modules will be removed from
- the I/O controller module's slot number (from 1 to 16)

Task flow diagram

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

Task flow for Removing I/O controller modules



Procedure

ATTENTION

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

Removing I/O controller modules

Step	Action

At the local or remote VT100 console

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

2 Access the top menu level of the remote maintenance interface (RMI):

```
sdmmtc
```

3 Access the hardware (Hw) menu level:

```
hw
```

4 Determine the devices on the I/O controller module:

```
locate
```

CAUTION

Deleting an I/O controller module

Deleting an I/O controller module requires you to put the module in both domains in a ManB state. These modules are out of service.

5 Manually busy the module in each domain:

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

where

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

- 0 if the module is located in slots
  - — 4 and 5 of the main chassis
  - — any two slots from 1 to 8 in the I/O expansion chassis
- 1 if the module is located in slots
  - — 15 and 16 of the main chassis

— in any two slots from 9 to 16 of the I/O expansion chassis

<n>
is the disk number that you are replacing (Use the Locate command to determine the disk number of the module.)

Example response:

```
Hardware Bsy - Domain 1 Device DSK2
Busying DSK2(1) will also busy DSK3(1).
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

6 Confirm the Bsy command:

y

Example response:

```
Hardware Bsy:  Domain 1 Device DSK2 - Command
initiated.
Please wait...
```

When the Bsy command is finished, observe that the message: `Please wait` along the command confirmation disappear. The status of the domain transitions from initiated to submitted and finally to complete.

Example response:

```
Hardware Bsy:  Domain 1 Device DSK2 - Command complete.
```

7 Repeat steps 5 through 7 for the other domain. Once you have manually busied the module in both domains, go to step 8.

Note: After you see the response to the Bsy command, the I/O controller module's state changes to M at the hardware level.

8 Use the Locate command to determine the chassis and slot number of the module you wish to delete. Press the Enter key to scroll through the display to see all the information:

locate

Example response:

```
Site Flr RPos Bay_id Shf   Description    Slot EQPEC
HOST 00  00   CSDM   SDME   DSK2(0),DSK3(0)
02  NTRX50FU   FRNT
```

9 Delete the module:

delete <chassis> <slot>

where

<chassis> is the chassis where the module is located (SDMM for the main chassis or SDME for the I/O expansion chassis)
<slot> is the slot number (from 1 to 16) where the module is located

Note: The module in the corresponding slot of the other domain will also be deleted.

Example response:

```
Module in slot 4 of SDMM will be deleted.
DSK2(0), DSK3(0) will be deleted.
Module in slot 15 of SDMM will also be deleted.
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

10 Confirm that you want to delete the module:

Y

The delete command can take several minutes to complete. When the command is finished, the following message is displayed:

```
Hardware Del Module - Command complete.
```

Within a few seconds, the module disappears from the listing shown at the hardware level, and the device numbers change on the screen display.

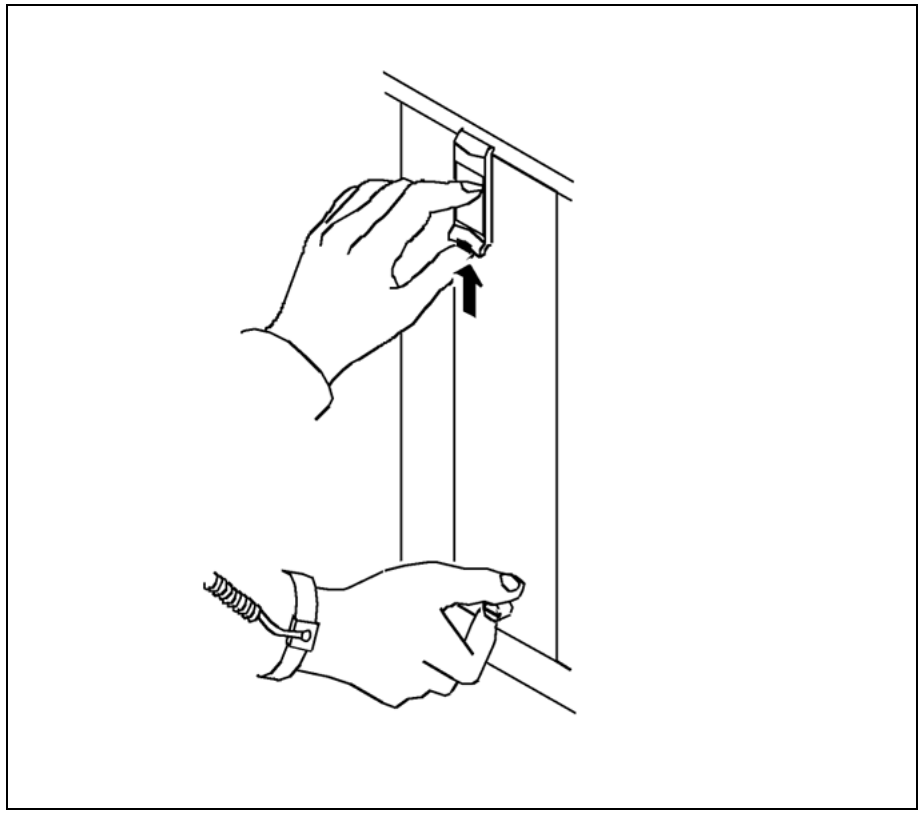
At the front of the CS 2000 Core Manager

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.

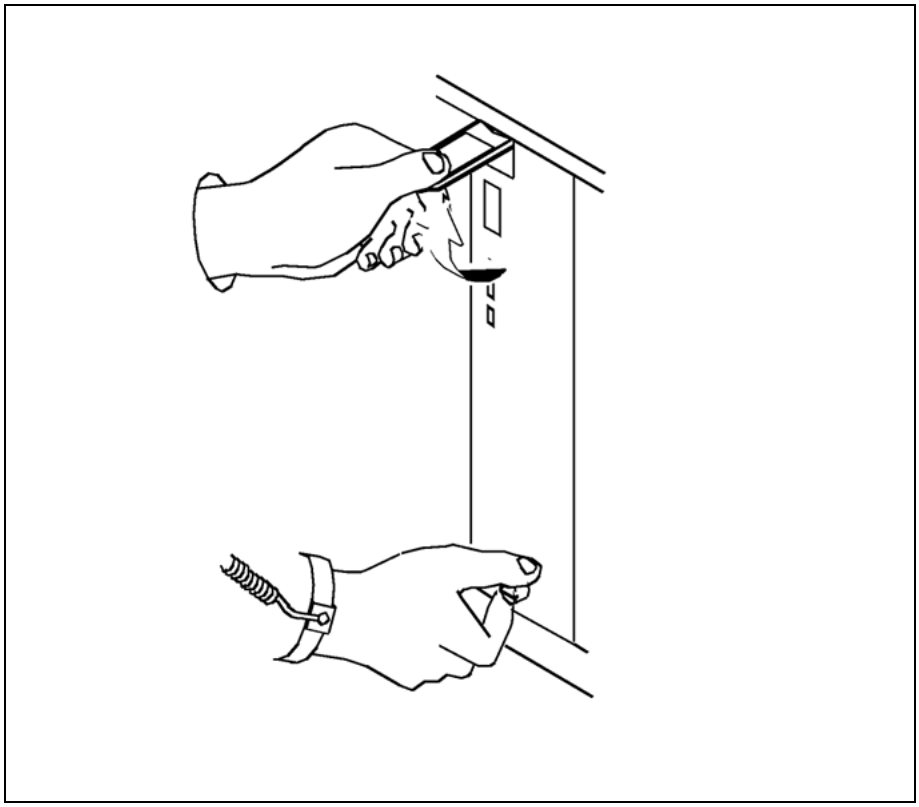
11 Wear an electrostatic discharge (ESD) grounding wrist strap.

12 Undo the thumbscrews located on the top and the bottom of the I/O controller module. The thumbscrews are the captive type, and cannot be removed from the module.

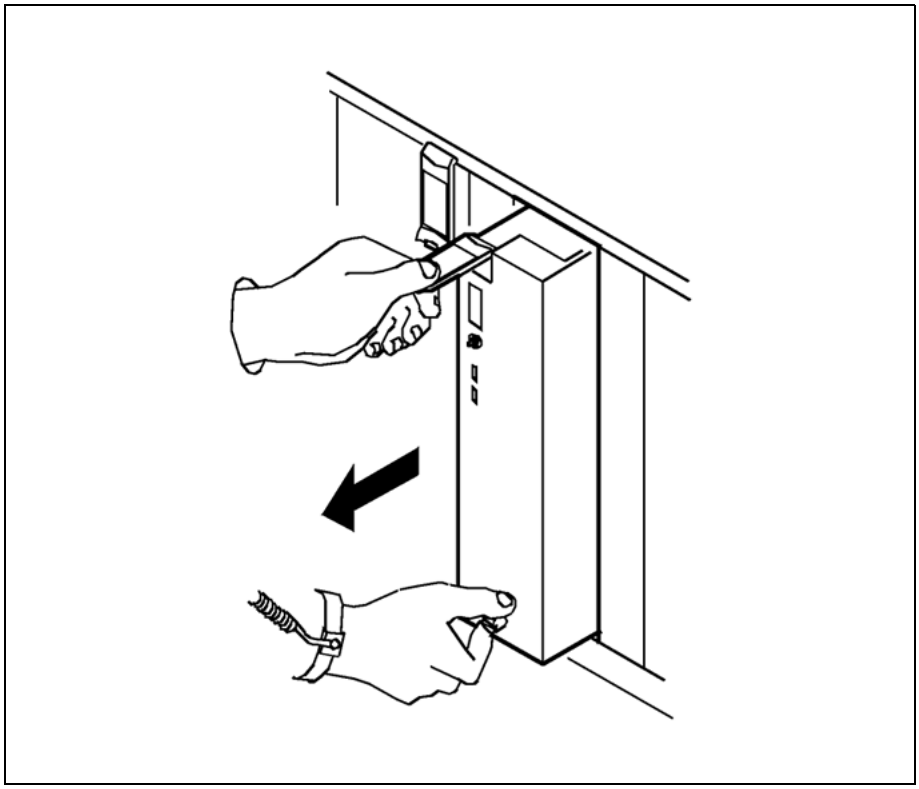
13 Depress the tip of the locking lever on the face of the I/O controller module.



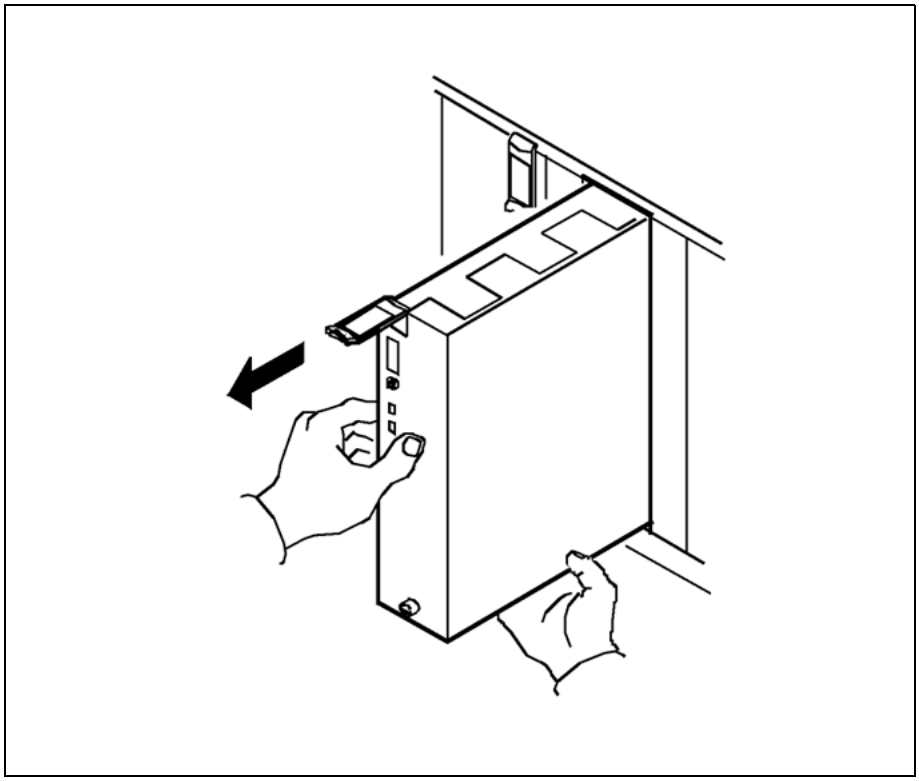
14 Open the locking lever on the face of the module by moving the lever outwards.



15 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 inches (5 cm) from the CS 2000 Core Manager shelf.



16 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.



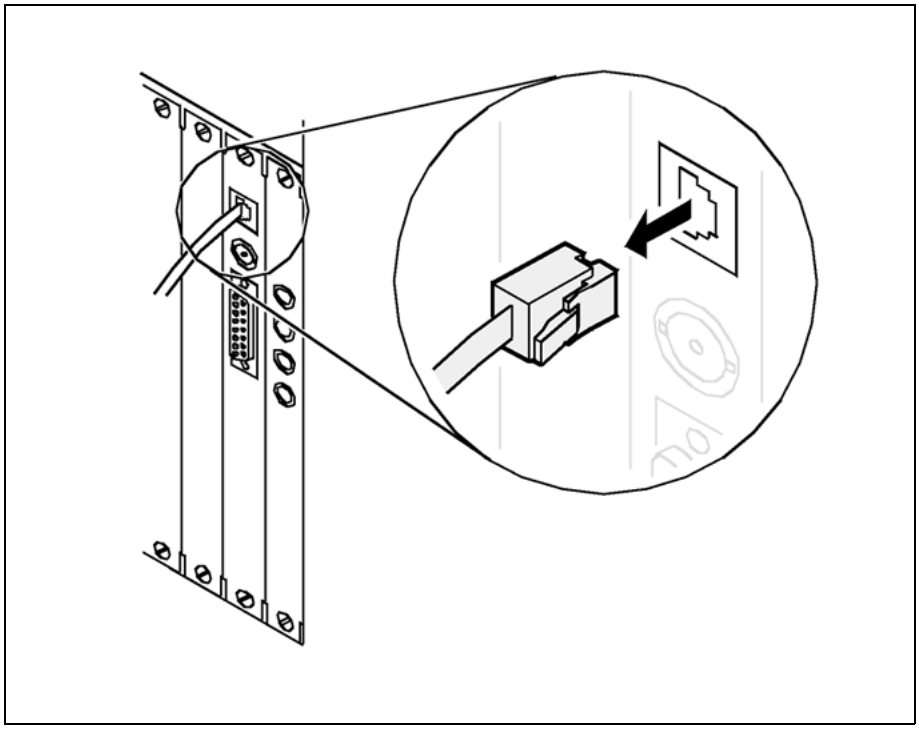
17 Place the module you have removed in an ESD protective container.

At the back of the CS 2000 Core Manager

18 Determine what kind of hardware module your CS 2000 Core Manager has.

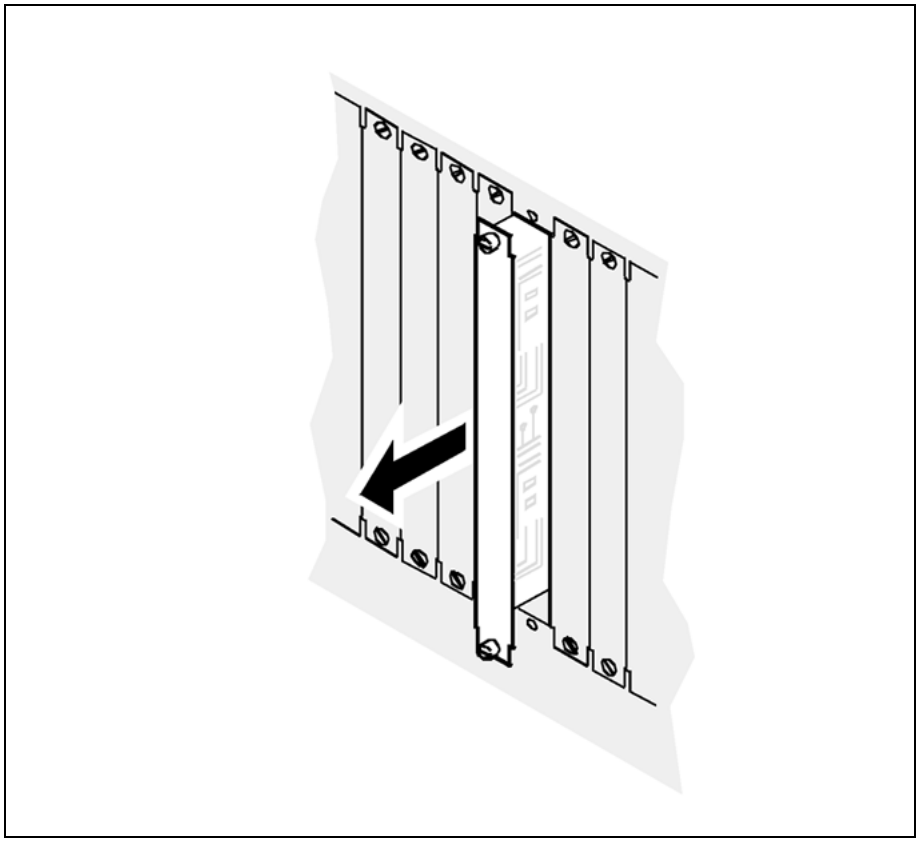
If you have	Do
NTRX50GN	step 19
NTRX50FU and NTRX50GP	step 20

19 Disconnect the 10BASE-T cable from the corresponding LAN personality module, as shown in the following diagram.

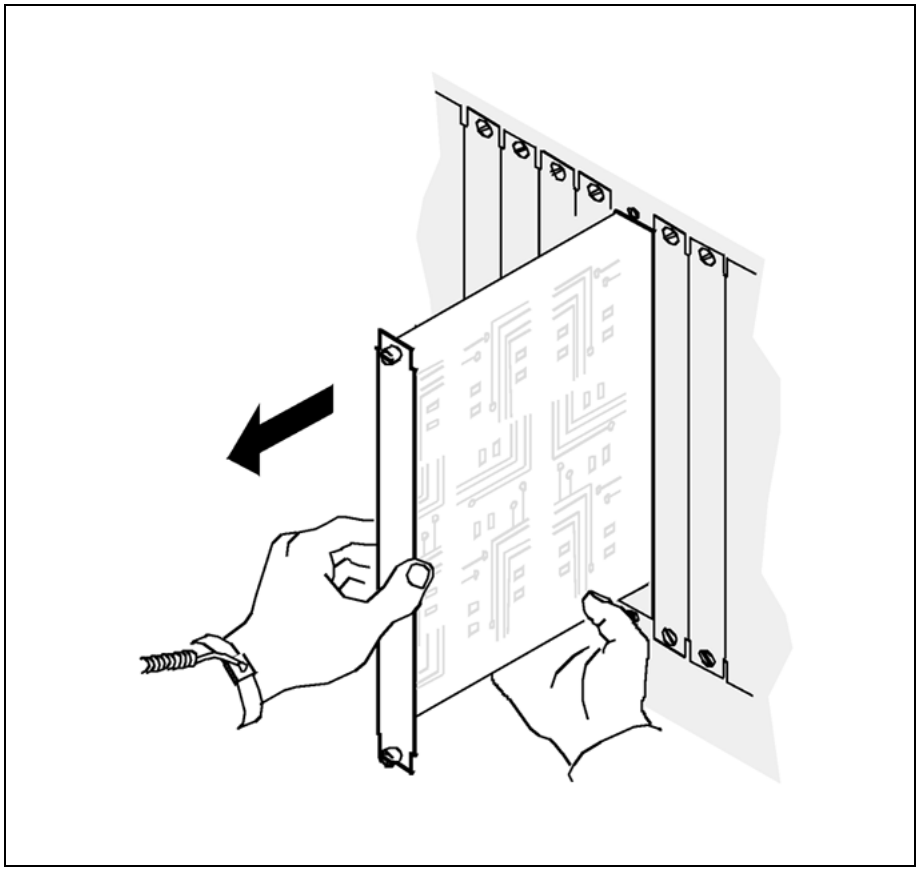


20 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module. The thumbscrews are the captive type, and cannot be removed from the module.

21 While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 inches (5 cm) from the CS 2000 Core Manager shelf.



22 Hold the LAN personality 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 LAN personality module you have removed in an ESD protective container.

24 Reinstall the filler plates covering the slots from which you removed the modules.

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

If necessary to change or correct the physical location of the modules, this procedure can be followed by the procedure "Removing I/O controller modules" (page 293)

—End—

Removing an I/O expansion chassis (NTRX50EC)

Purpose

ATTENTION
Do not perform this procedure if there are any hardware faults on the CS 2000 Core Manager.

Use this procedure to remove an I/O expansion chassis (NTRX50EC) from an existing system.

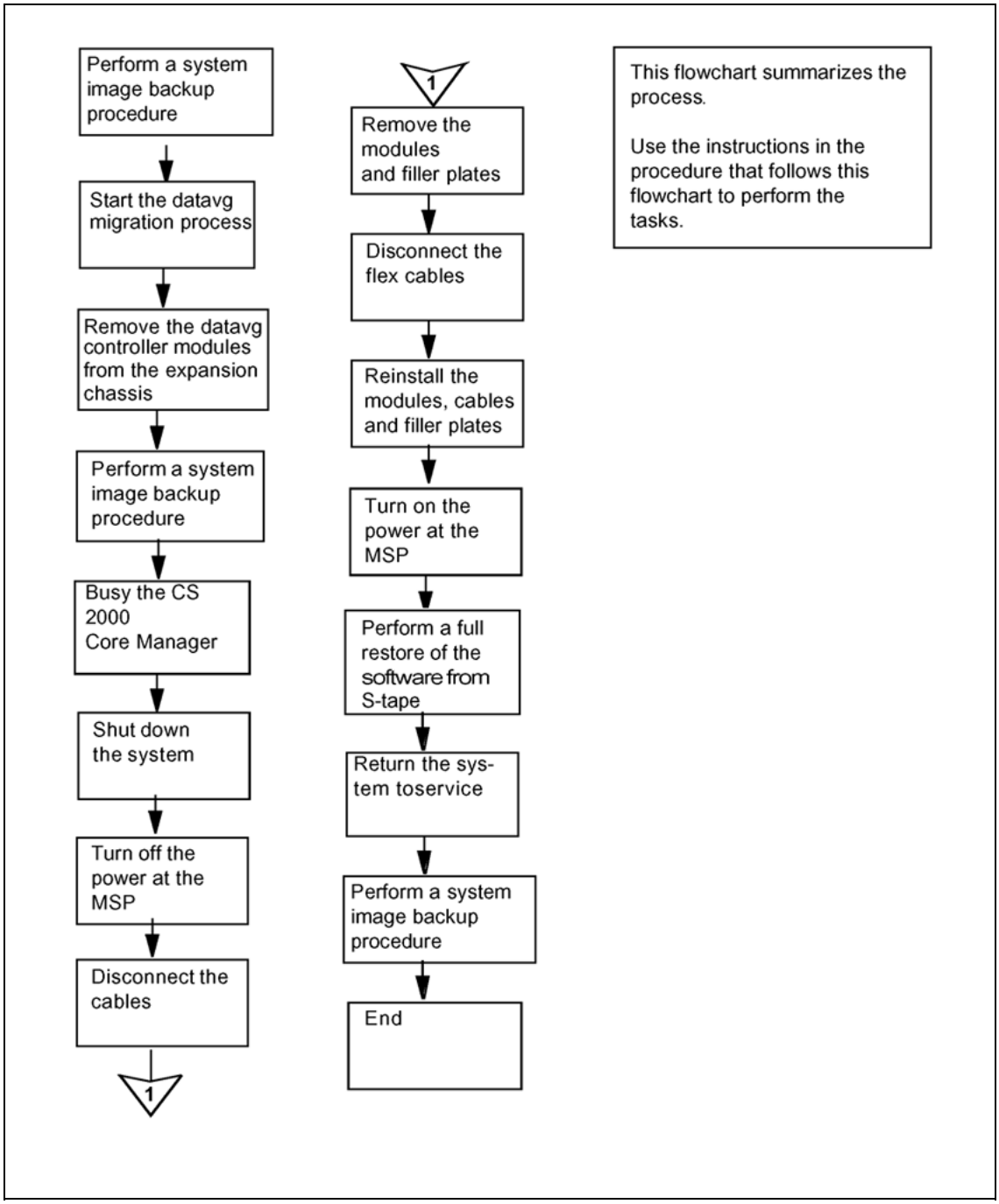
Prerequisites

Make sure that your main chassis has been upgraded to the 36-Gbyte + 36-Gbyte Ultra-Multifunction Input/Output (UMFIO), before you start this procedure. Use the procedure "Upgrading a datavg MFIO to MFIO or UMFIO" (page 350), if required.

Task flow diagram

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

Task flow for removing an I/O expansion chassis (NTR50EC)



Procedure

ATTENTION

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

Removing an I/O expansion chassis (NTRX50EC)

Step	Action

At the local or remote VT100 console

1 Perform a system image backup. Use the procedure "Creating system image backup tapes (S-tapes)" in the Security and Administration document.

2 Exit the maintenance interface and return to the AIX command line:

```
quit all
```

3 Check that no faults exist on the CS 2000 Core Manager:

```
querysdm flt
```

If	Do
faults are present	correct the faults using the procedures in the *CS 2000 Core Manager Fault Management*, NN10082-911, and return to this procedure
no faults are present	step 4

4 Start the process of migrating datavg from the expansion chassis to the main chassis:

```
ftmigratepv
```

The system performs several checks, listing them on the screen.

5 Use the following table to determine your next step.

If	Do
If no error is displayed	step 6
the error message indicates you don’t have physical volumes for datavg in expansion chassis	go to step 18
the error message indicates you there is insufficient free disk space on main chassis for migration	contact your next level of support

6 When prompted, confirm that you want to continue the data migration:

```
y
```

7 Confirm again that you want to continue the data migration:

```
y
```

The system continues the data migration process, listing all completed sub-processes, and then prompts you to remove the datavg modules on the expansion chassis. The migration process takes approximately 30 minutes.

Example response:

```
Please take out the datavg module in slot 1 on the
expansion chassis from the SDM. Please take out the
datavg module in slot 9 on the expansion chassis from
the SDM.
```

At the front panel

8 Remove the datavg controller modules from the expansion chassis slots indicated by the system.

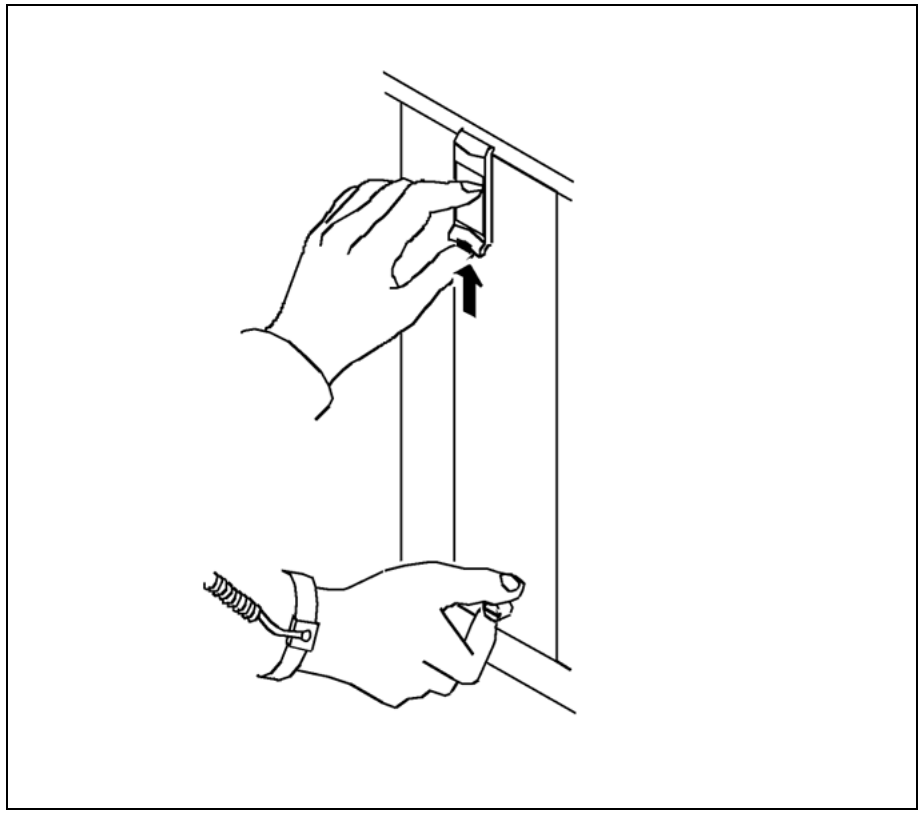
WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

9 Put on an electrostatic discharge (ESD) grounding wrist strap connected to the C28B.

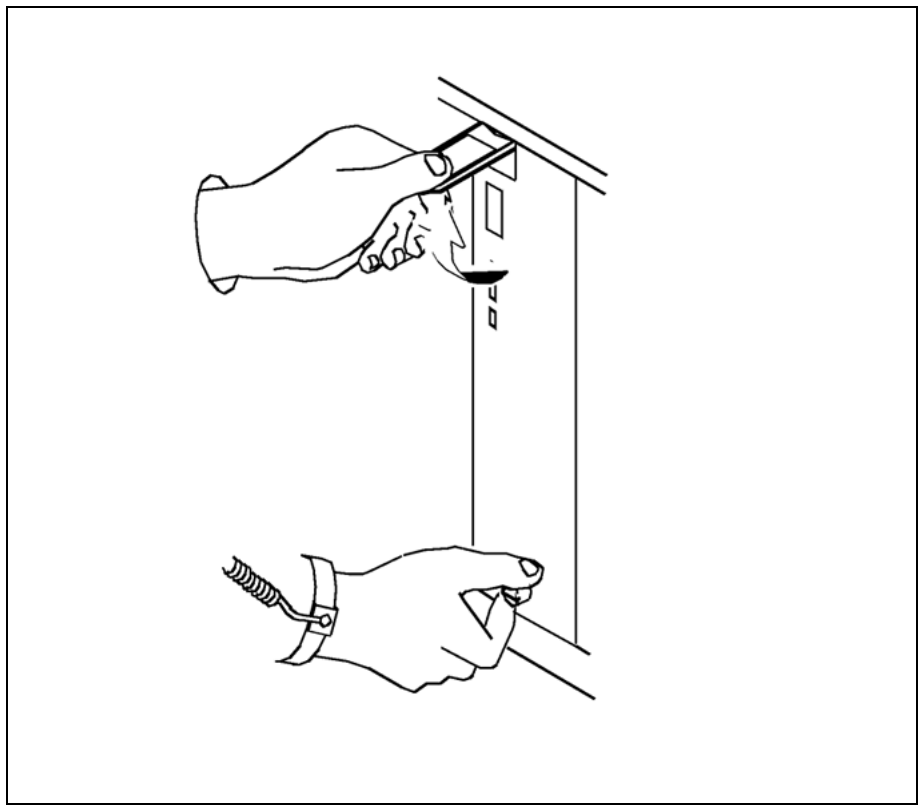
10 Undo the captive type thumbscrews located on the top and the bottom of the datavg controller module in domain 0.

Note: The thumbscrews cannot be removed from the module.

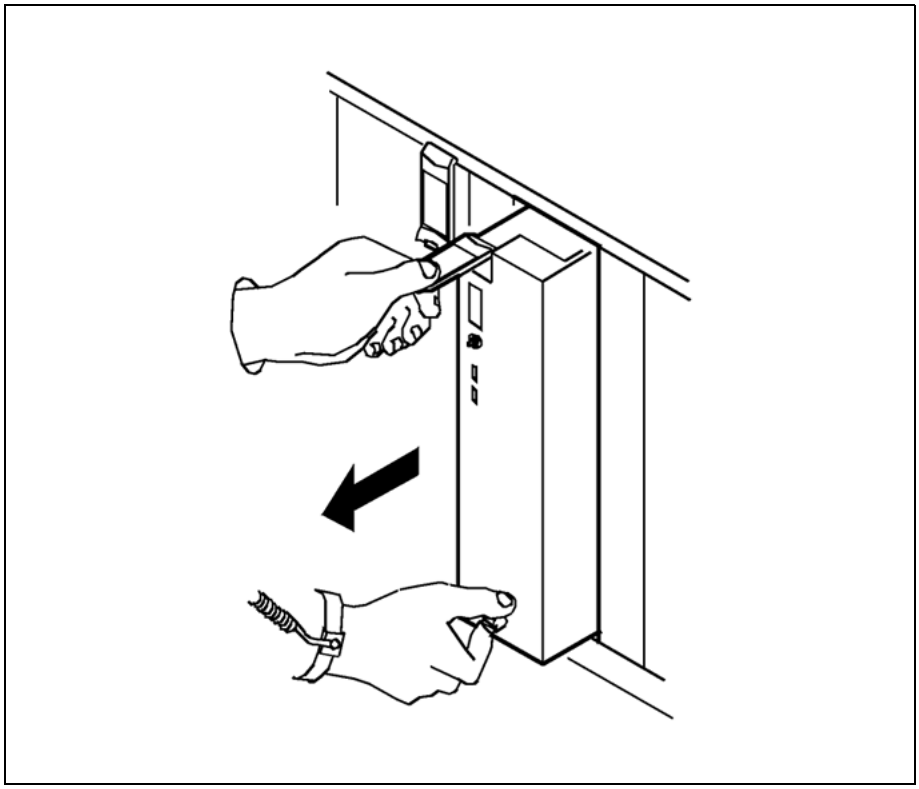
11 Depress the tip of the locking lever on the face of the I/O controller module.



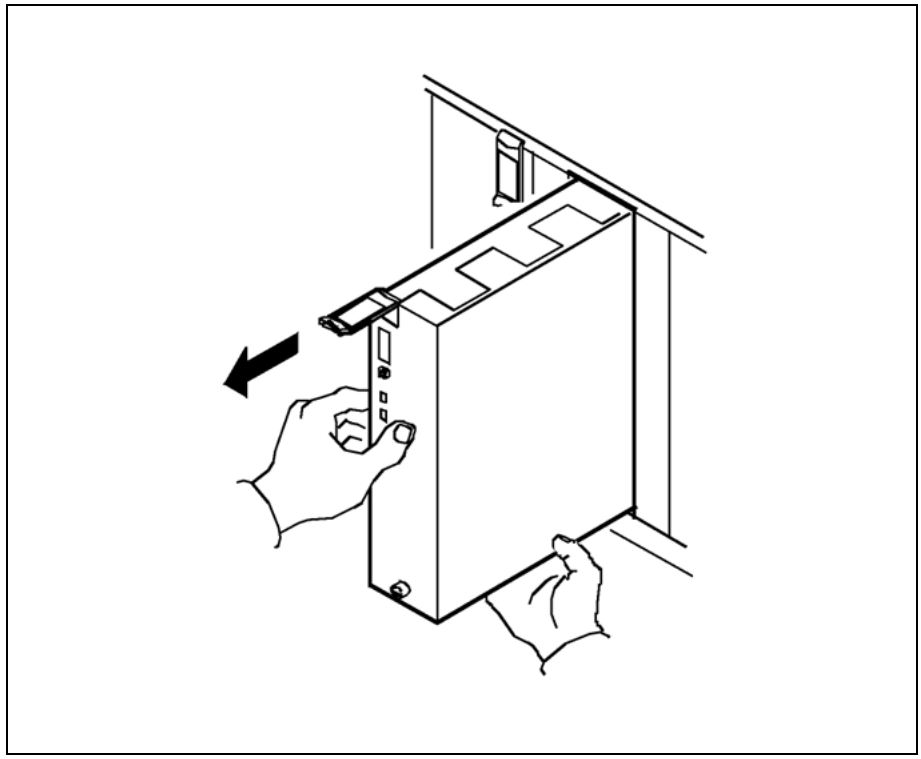
12 Open the locking lever on the face of the module by moving the lever outwards.



13 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in (5 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 module toward you until it clears the shelf.



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

16 Repeat steps 10 through 15 for the datavg controller module in domain 1.

At the VT100 console

17 Wait until data migration is completed.

The system responds:

```
Data on expansion chassis has been migrated to main
chassis with no error.
```

18 Perform a system image backup. Use the procedure "Creating system image backup tapes (S-tapes)" in *CS 2000 Core Manager Security and Administration*, NN10170-611.

While executing the backup procedure, you are asked if you want to eject the S-tape from the drive. Enter n (no). Then, go back to the previous menu by typing y, and return to the admin level by typing 0 (zero). Exit the maintenance interface by typing quit all and pressing the Enter key.

At the MAP terminal

19 Access the SDM level of the MAP display:

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

20 Busy the CS 2000 Core Manager:

```
bsy
```

21 Confirm the busy request:

```
y
```

22 Verify that each billing stream has entered the active backup mode by posting and querying each of your billing streams.

```
sdmbil;post<stream>;query
```

At the VT100 console

23 Disable the autoboot attribute for CPU 0:

```
autoboot -c 0 -o vb=n
```

24 Disable the autoboot attribute for CPU 1:

```
autoboot -c 2 -o vb=n
```

25 Shut down the CS 2000 Core Manager:

```
shutdown now
```

At the modular supervisory panel (MSP)

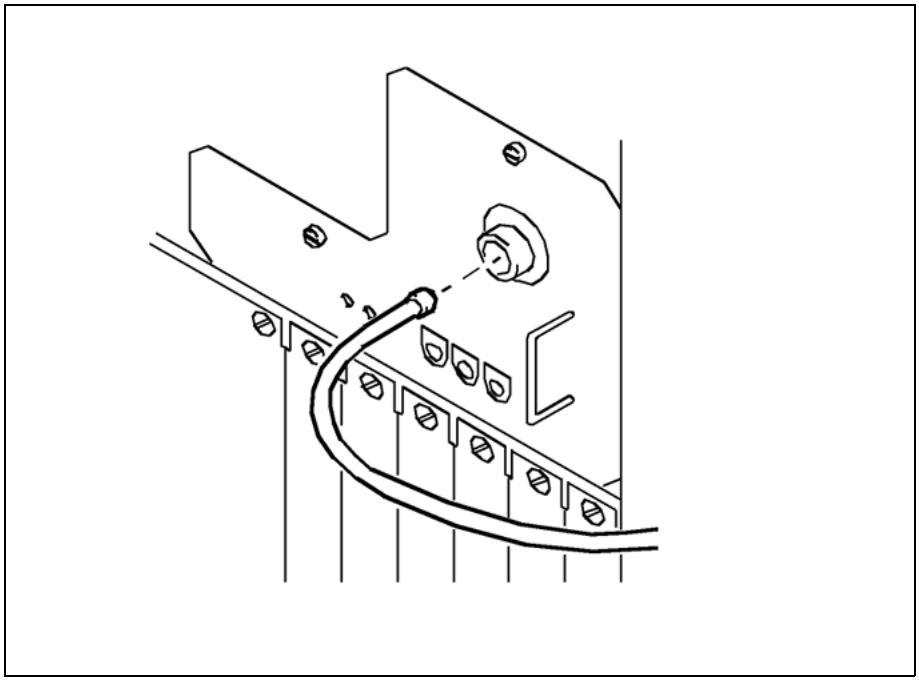
26 Interrupt power to the CS 2000 Core Manager by turning off all four MSP breakers located at the front of the MSP.

At the back of the CS 2000 Core Manager

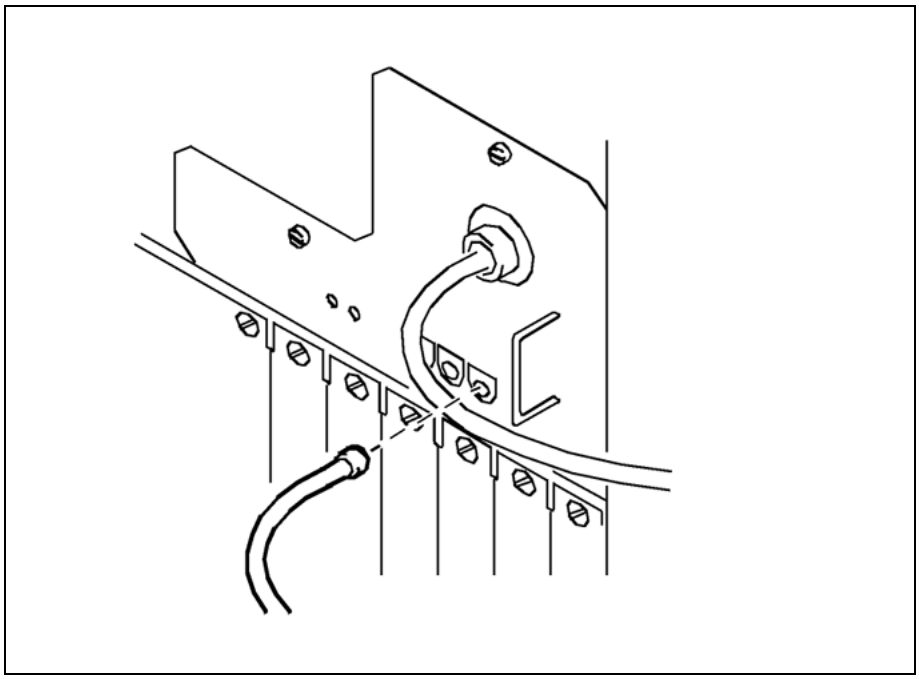
WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

27 Put on an electrostatic discharge (ESD) grounding wrist strap connected to the C28B.

28 Disconnect the power cables from the interconnect module ICM 0 and ICM 1 on both chassis, then remove and store them.



29 If there are any alarm cables connected to the I/O expansion chassis, disconnect them.

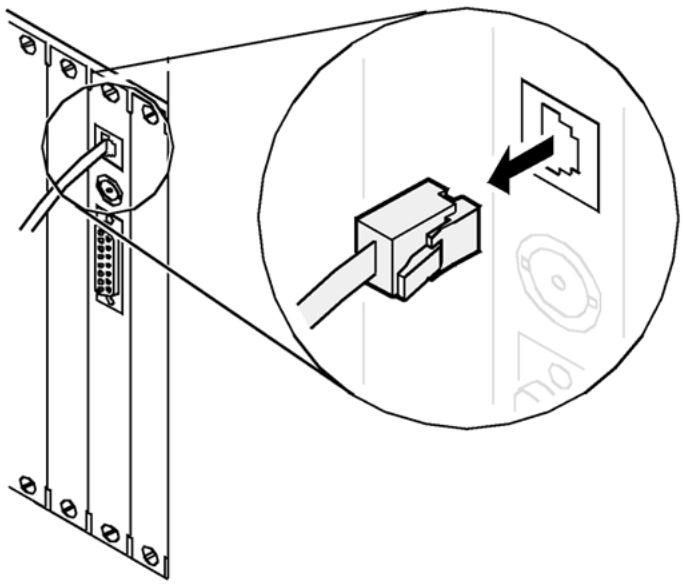


30 Label the cables.

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.

31 Disconnect the four DS512 fiber cables from both DS512 personality modules (on the main shelf) by pressing the fiber cable in, and turning it a quarter-turn to the left.

32 Disconnect the 10BASE-T cables from both LAN personality modules on the main shelf.



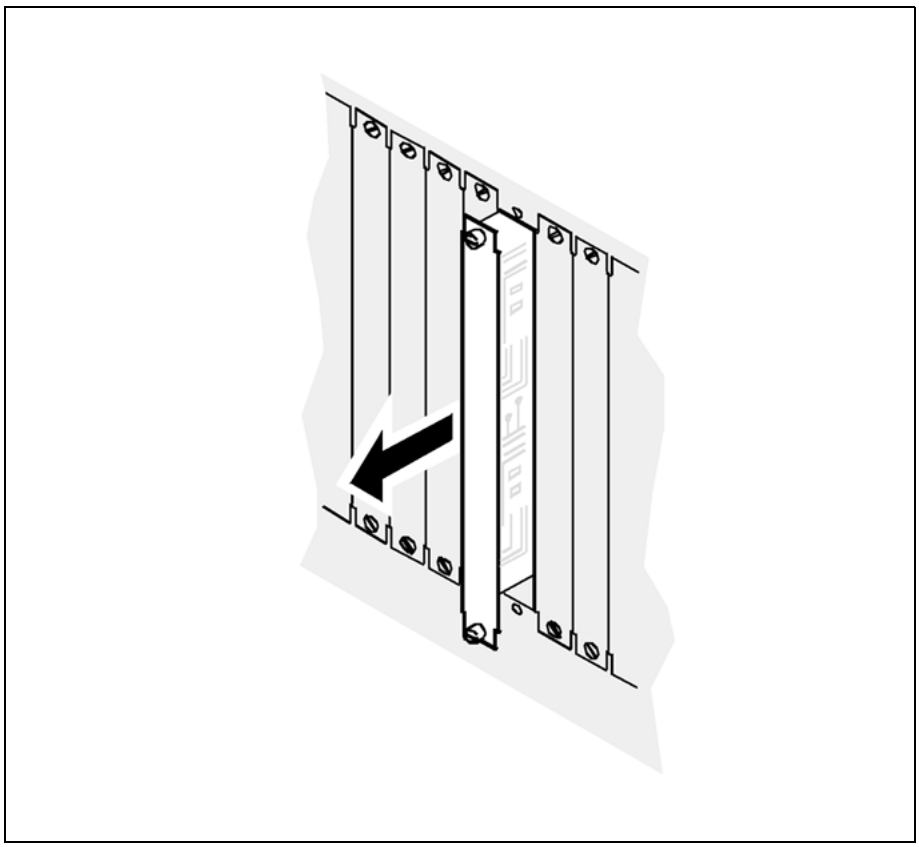
33 To gain access to the flex cable, remove all personality modules and filler plates located in slots 1, 2, 3, 14, 15, and 16 on both chassis.

34 Record the slot number of each personality module and each filler plate that you are removing from the main shelf.

35 Loosen the thumbscrews located at the top and bottom of the personality module.

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

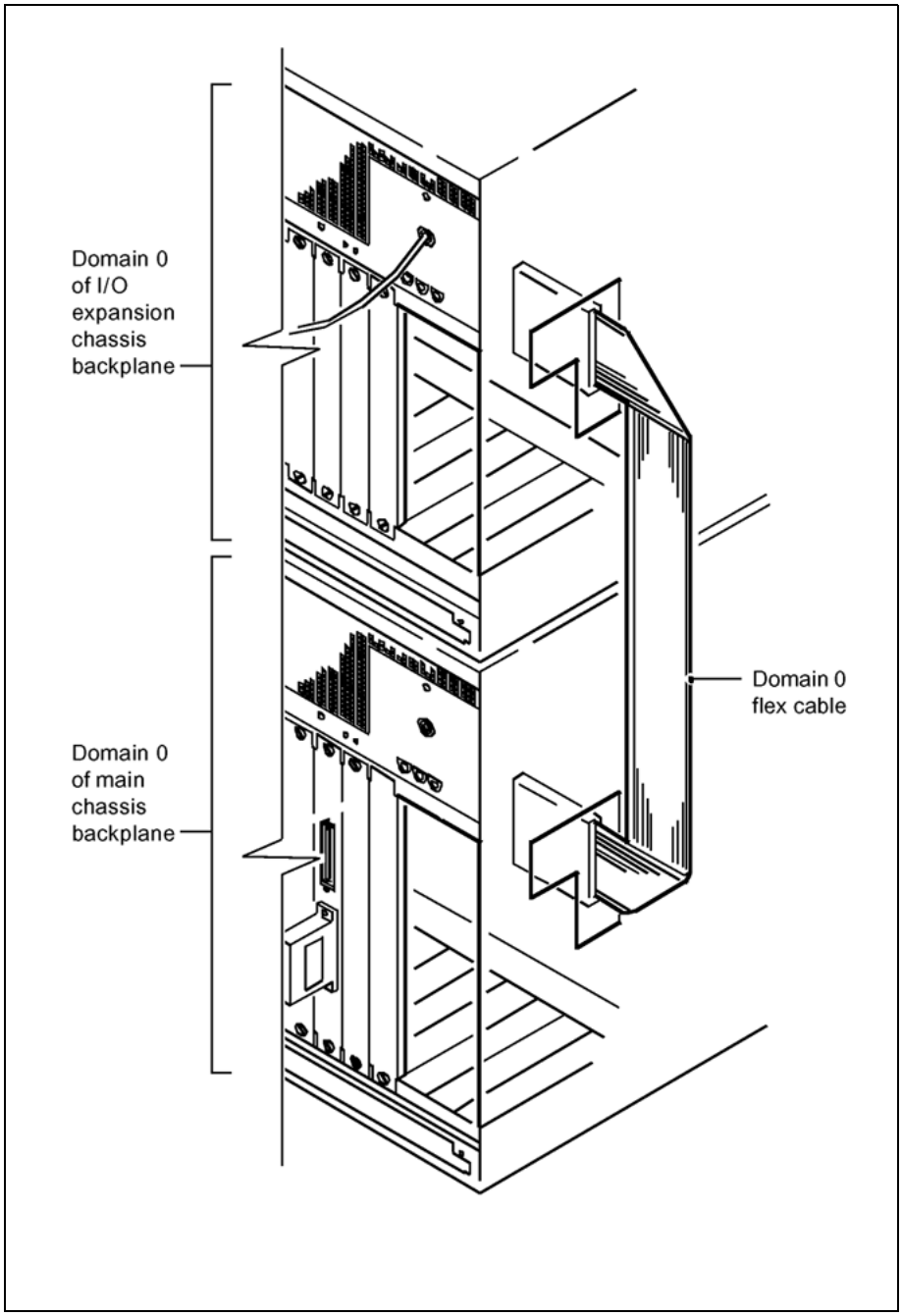
36 While grasping the thumbscrews, carefully pull the personality module out of the SDMCS 2000 Core Manager shelf.



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

38 Remove the domain 0 and domain 1 flex covers that run from the outside of the main and I/O expansion chassis.

39 Disconnect and remove the domain 0 flex cable (NTRX5088) from the I/O expansion chassis backplane side 0 and from the main chassis backplane side 0. Through the empty slots, reach the ends of the flex cable and pull them towards you. Once disconnected from both chassis, remove the cable through the side opening.



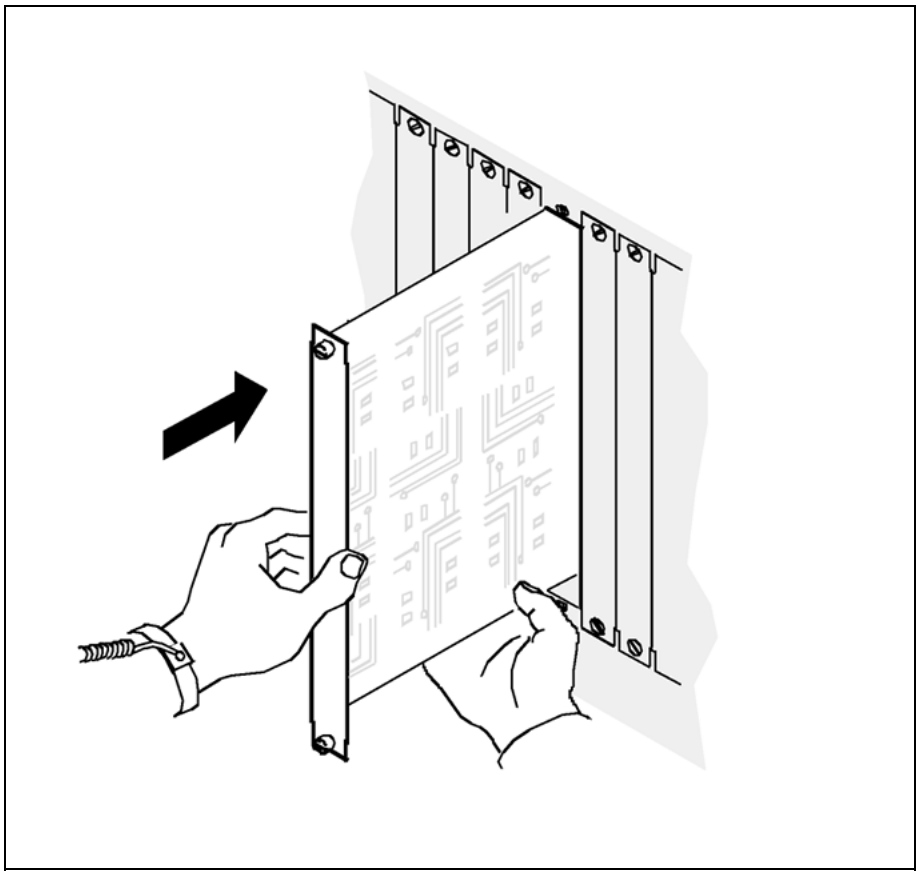
40 Return to step 33 and repeat the same operation on domain 1.

41 Reinstall all personality modules and filler plates (on the main chassis only) that you removed in step 33.

Use your records from step 33 to make sure that you are placing each module in the same slot from which it was removed.

42 Reinstall all modules and filler plates in domain 0 first. Start from slot 2, and continue to the right. Repeat the same process on domain 1, starting from slot 16, and continuing to the left.

43 Carefully slide the personality module into the appropriate slot until it is fully inserted.



44 Tighten the thumbscrews at the top and bottom of the personality module.

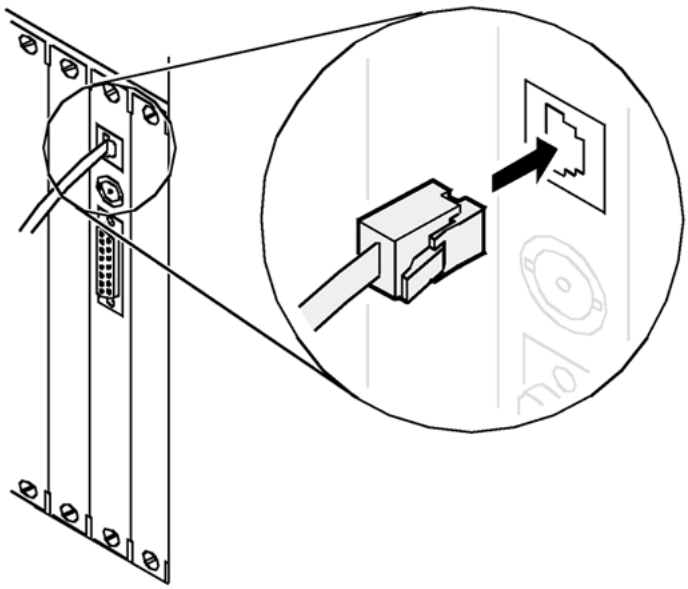
45 Repeat steps 43 and 44 for each personality module that you need to reinstall, then continue.

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.

46 Reconnect the four DS512 fiber cables on the DS512 personality module (on both domains) by pressing the fiber cable in, and turning it a quarter-turn to the right.

- Link 0 transmit and link 0 receive connect to MS0
- Link 1 transmit and link 1 receive connect to MS1

47 Reconnect the 10BASE-T cable to the LAN personality module (on both domains).



48 Reconnect the power cables to ICM 0 and ICM 1 in the main chassis.

At the modular supervisory panel (MSP)

49 Restore power to the CS 2000 Core Manager by turning on the top two MSP breakers.

At the VT100 console

50 Perform a full restore of the CS 2000 Core Manager software load from the system image backup tape (S-tape) that you created

in step 18. Use the procedure "Performing a full restore of the software from S-tape" in *CS 2000 Core Manager Fault Management*, NN10082-911, starting with step 13.

At the MAP terminal

51 Access the SDM level of the MAP display:

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

52 Return the CS 2000 Core Manager to service:

```
rts
```

Note: It will take at least 5 minutes for the CS 2000 Core Manager to return to service on the core side.

53 Verify that the CS 2000 Core Manager status is InSv (in-service) or ISTb (in-service trouble).

54 Verify that all billing streams are either in-service or in recovery by posting and querying each of your billing streams:

```
sdmbil;post<stream>;query
```

At the VT100 terminal

55 Enable the autoboot attribute for CPU 0:

```
autoboot -c 0 -o vb=y
```

56 Enable the autoboot attribute for CPU 1:

```
autoboot -c 2 -o vb=y
```

57 Perform a system image backup. Use the procedure "Creating system image backup tapes (S-tapes)" in *CS 2000 Core Manager Security and Administration*, NN10170-611.

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

—End—

Migrating from a rootvg system to a rootvg/datavg system

Purpose

Use this procedure to move from a rootvg system to a system with both rootvg and datavg.

This procedure creates datavg, and moves logical volumes from rootvg to datavg.

Logical volume data can be stored in the root volume group (rootvg) or the data volume group (datavg). Create datavg for logical volumes with large amounts of data. If you do not create datavg, the system stores logical volume data in rootvg.

ATTENTION
This procedure must be performed by a trained AIX system administrator who is authorized to perform config-admin actions to access the CS 2000 Core Manager.

ATTENTION
Perform this procedure after you have installed the required I/O controller modules (in pairs) in the appropriate slots in the main or I/O expansion chassis. If you have not installed the required modules, refer to the procedure "Adding I/O controller modules" in *Upgrading the CS 2000 Core Manager*, NN10060-461.

ATTENTION
This procedure requires that your system is MANB. Nortel recommends that you add a datavg when you upgrade the CS 2000 Core Manager.

ATTENTION
A maximum of 16-Gbyte storage capacity is supported for datavg.

Prerequisites

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

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

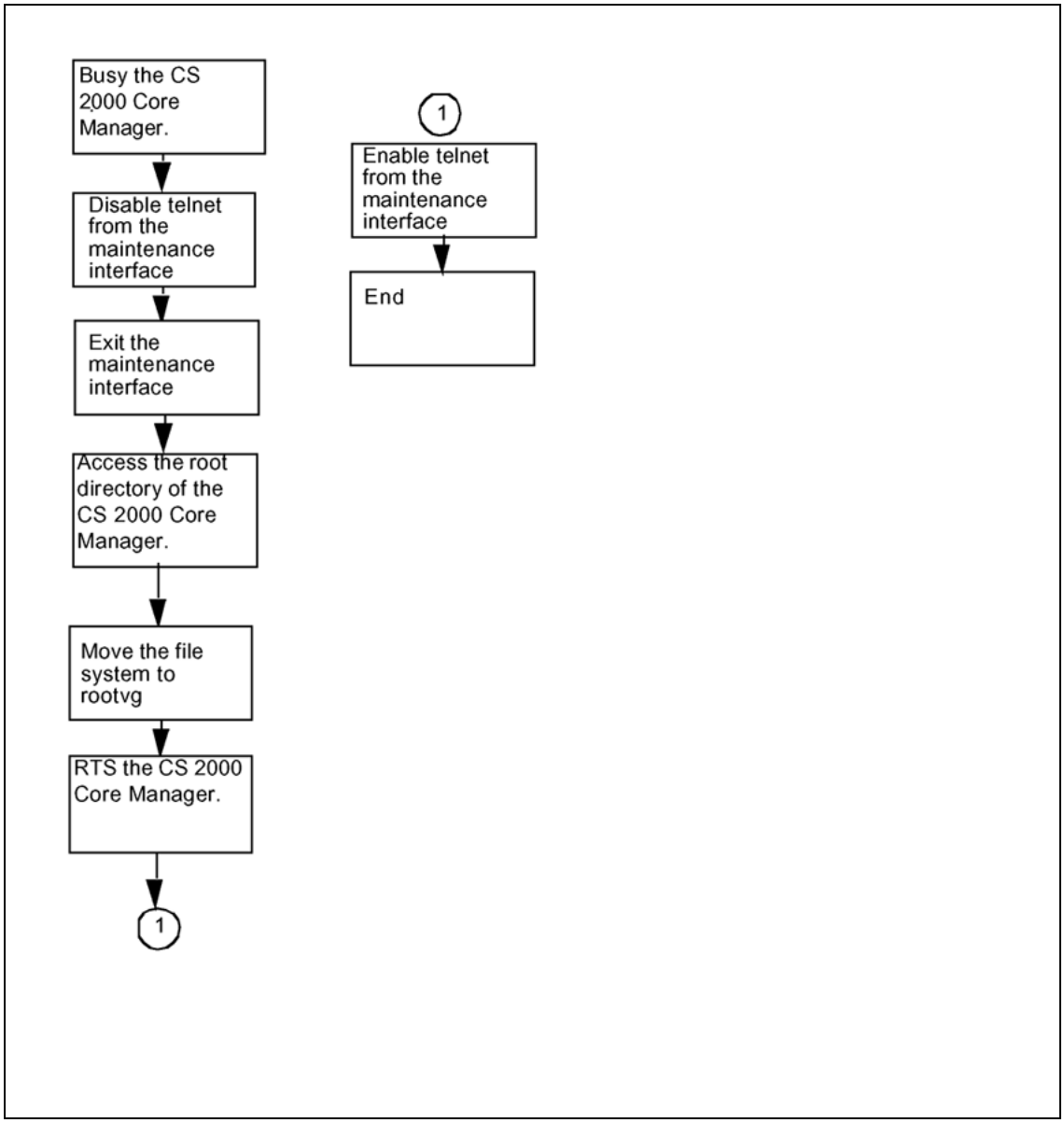
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Task flow diagram

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

Task flow for migrating from a rootvg system to a rootvg/datavg system



Procedure

ATTENTION

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

Creating a data volume group

Step	Action

At the SDM level of the MAP display

1 Busy the CS 2000 Core Manager:

```
bsy
```

At the local or remote VT100 console

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

3 Access the administration (Admin) level:

```
admin
```

4 Access the Access level:

```
access
```

The CS 2000 Core Manager displays the state of the telnet service. Use the following table to determine your next step.

If telnet is	Do
disabled	step 8
enabled	step 5

5 Disable telnet to ensure that no other user has access to CS 2000 Core Manager during the volume group migration:

```
change
```

6 Confirm the command:

```
y
```

7 Exit the maintenance interface:

```
quit all
```

8 Access the root directory:

```
cd /
```

9 Move the file system from rootvg to datavg:

```
movevg
```

The movevg process takes some time to complete. When the process is complete, the system returns to the # prompt. It can be several minutes after the movevg command is completed before datavg is displayed as Mirrored under the storage level.

At the SDM level of the MAP display

10 Return the CS 2000 Core Manager to service:

```
rts
```

At the local or remote VT100 console

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

12 Access the administration (Admin) level:

```
admin
```

13 Access the Access level:

```
access
```

14 Enable telnet:

```
change
```

15 Confirm the command:

```
y
```

16 Exit the maintenance interface:

```
quit all
```

17 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure, or refer to procedure "Adding disks and creating a logical volume in datavg" in *CS 2000 Core Manager Security and Administration*, NN10170-611.

—End—

Upgrading from an X.25 SYNC card to a UMFIO X.25 card

Purpose

Use this procedure to upgrade a system from a rootvg-only system with SYNC X25 to a rootvg/datavg system with UMFIO/X25PM.

Prerequisites

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

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

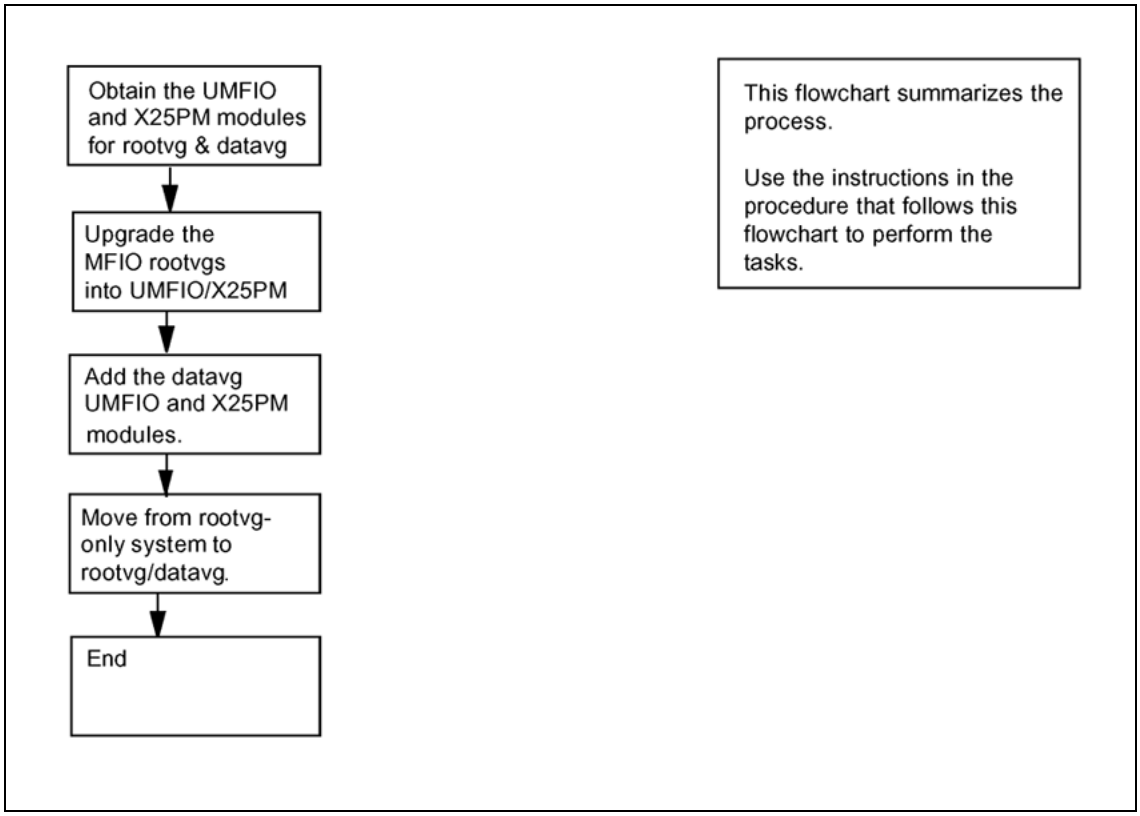
Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

Procedure

The following task flow diagram provides a summary of the process. To move from a rootvg-only system to a rootvg/datavg with X.25, use the instructions in the procedure that follows the flowchart.

Task flow for upgrading from an X.25 SYNC card to a UMFIO X.25 card



Upgrading from an X.25 SYNC card to a UMFIO X.25 card

Step	Action
	At the CS 2000 Core Manager
1	Obtain the UMFIO controller modules for rootvg and the X25PM modules. Ensure that the upgraded modules have the correct product engineering code (NTRX50NM for rootvg UMFIO and NTRX50NN for X25PM). The PEC is printed on the top locking lever.
2	Perform the procedure "Upgrading the rootvg MFIO to MFIO or UMFIO" (page 330), to upgrade from rootvg MFIO with SYNC X25 into rootvg UMFIO/X25PM for both domains.
3	Obtain the UMFIO controller modules for datavg and the X25PM modules. Ensure that the upgraded modules have the correct product engineering code (NTRX50NL for datavg UMFIO and NTRX50NN for X25PM). The PEC is printed on the top locking lever.
4	Perform the procedure "Removing I/O controller modules" (page 293), to add the datavg UMFIO and X25PM modules for both domains to the system.

5 Perform the procedure "Migrating from a rootvg system to a rootvg/datavg system" (page 322), to migrate from a rootvg-only system to a rootvg datavg system.

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

—End—

Upgrading the rootvg MFIO to MFIO or UMFIO

Purpose

Use this procedure to upgrade from a 4GB + DAT Multifunction Input/Output (MFIO) module to a 9GB + DAT MFIO module.

You can also use this procedure to perform the following tasks:

- upgrade from a 4GB + DAT MFIO module or a 9GB + DAT MFIO module to a 36GB + DAT Ultra-Multifunction Input/Output (UMFIO) module
- upgrade to any other supported combinations. For the list of supported combinations, refer to the table "Supported MFIO and UMFIO, datavg and rootvg configurations" in *Upgrading the CS 2000 Core Manager*, NN10060-461.
- revert a rootvg I/O module to the original hardware configuration, if the rootvg I/O module in a single domain was upgraded. Before reverting back, confirm that the storage system has regained full mirroring.

ATTENTION

Do not use this procedure to revert to the original rootvg I/O module if you have successfully upgraded the rootvg I/O module in both domains, or if you have upgraded from an MFIO with SYNC X.25 to a UMFIO with X.25 PMs

Prerequisites

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

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

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

UMFIO pre-upgrade requirements

If you are upgrading to a UMFIO, you must check your system for UMFIO readiness prior to the upgrade. To check for UMFIO readiness, type the following:

```
# umfiocheck
```

The following example shows the output for a system that is UMFIO ready.

```
1+0 records in.
1+0 records out.
1+0 records in.
1+0 records out.
This system is UMFIO ready.
```

If the UFMIO is not ready, you must perform a backup and restore procedure. Perform the backup using the procedure "Creating system image backup tapes (S-tapes) manually" in the *CS 2000 Core Manager Security and Administration*, NN10170-611, Perform the restore using the procedure "Performing a full restore of the software from S-tape" in the *CS 2000 Core Manager Fault Management*, NN10082-911.

Once you have completed the backup and restore, rerun the ufmiocheck command. If your system is still not UMFIO ready, contact your next level of support.

ATTENTION

Have the correct UMFIO LAN personality module available. In order to upgrade to the UMFIO, you must have either the UMFIO LAN personality module (NTRX50NK) or the X25 personality module (NTRX50NN) available.

CAUTION

Back up the system before you begin this procedure. If SBA is installed, make sure you back up the billing data. Also, make sure there is no tape in the MFIO DAT drive.

The following table lists the product engineering codes (PEC) for various modules used in this procedure.

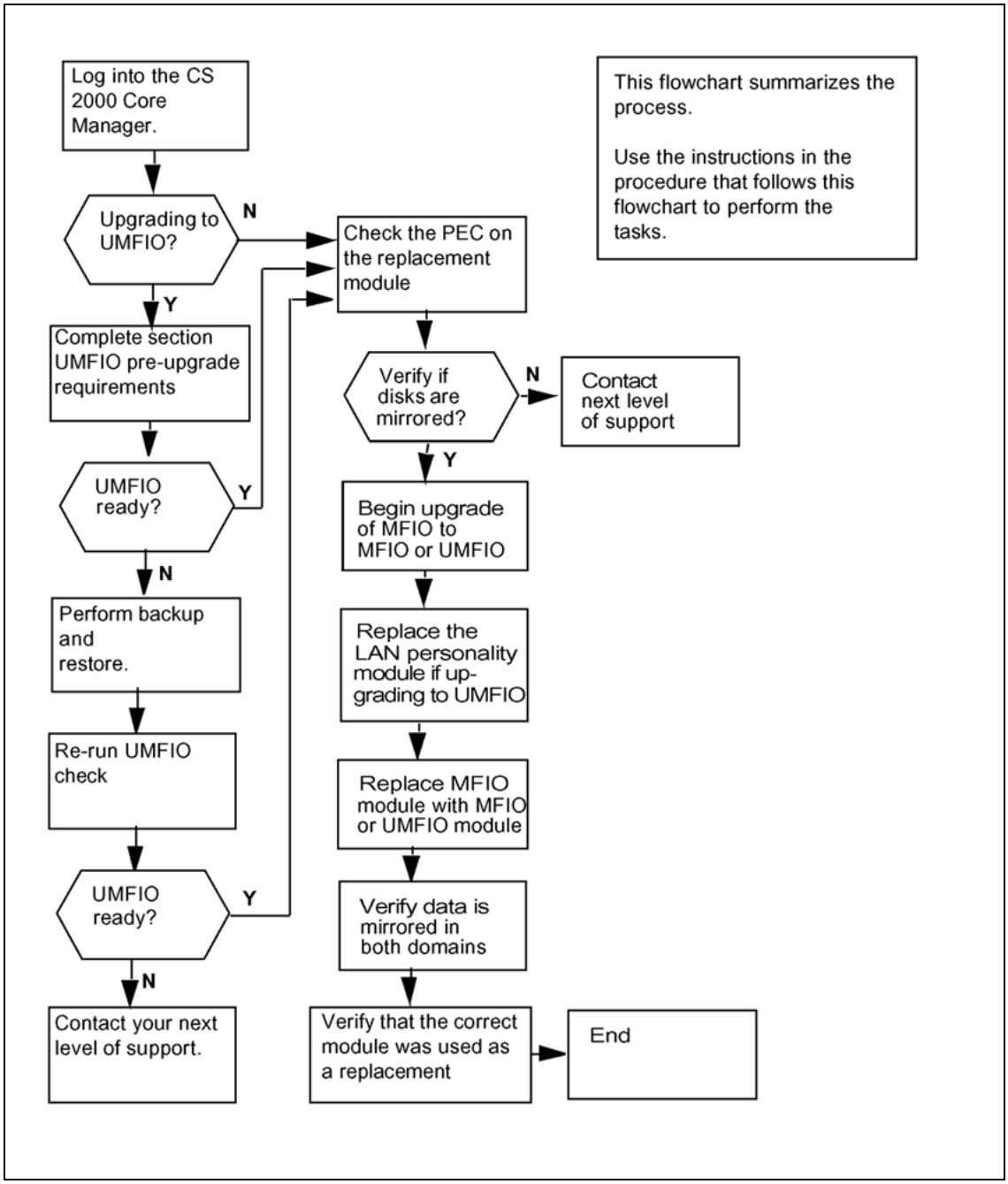
Nortel PEC	Name
NTRX50FS	LAN personality module for MFIO
NTRX50GN	4GB + DAT rootvg MFI

Nortel PEC	Name
NTRX50ND ***Note:*** Replacements for the NTRX50ND are filled on a best-effort basis before and after the manufacturers discontinue (MD) date of 31 December 2004. After 31 December 2004, the NTRX50NM is the replacement for the NTRX50ND	9GB + DAT rootvg MFIO
NTRX50NK	LAN personality module for UMFIO
NTRX50NN	X25 personality module for UMFIO
NTRX50NM	36GB + DAT rootvg UMFIO

Task flow diagram

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

Task flow for Upgrading the rootvg MFIO to MFIO or UMFIO



Procedure

ATTENTION

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

Upgrading the rootvg MFIO to MFIO or UMFIO

Step	Action

At the VT100 console

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

2 Check the label on the module that you want to use as a replacement. Make sure that label shows the product engineering code (PEC) that you want to use for your upgrade.

3 Access the storage level:

```
sdmmtc storage
```

If the State of both volumes is	Do
Mirrored	step 4
not Mirrored	contact your next level of support

4 Access the hardware level under the maintenance interface:

```
hw
```

5 Upgrade the MFIO:

```
upgrade <chassis> <slot> <pec>
```

where

<chassis> is sdmm since both rootvg MFIOs are located in the main chassis
<slot> is slot 2 if you are upgrading domain 0 or slot 13 if you are upgrading domain 1
<pec> is the product engineering code of the MFIO or UMFIO controller module you want to add

The following example command shows an upgrade to the 36GB + DAT UMFIO in slot 2 of the main chassis:

upgrade sdmm 2 NTRX50NM

6 Use the following table to determine your next step.

If you are	Do
prompted to delete the X25 sync module configuration	step 7
not prompted to delete the X25 sync module configuration	step 8

7 Confirm the deletion of the X25 SYNC module configuration:

```
y
```

The system responds:

```
Transitioning forward from START to INFO_RETRIEVED

Volume group = rootvg on hdisk0
Physical partition size 16 with max partitions 3048

Transitioning forward from INFO_RETRIEVED to OFFLINED
Transitioning forward from OFFLINED to DEPENDENCIES_REMOVED
Transitioning forward from DEPENDENCIES_REMOVED to REPLACED

Replace ORIGINAL MFIO I/O-2 (c1-f2) with UPGRADED MFIO

Enter 1 to continue, 99 to exit:
```

8 Use the following table to determine your next step.

If	Do
you want to replace the MFIO	Do not type 1 at the console until the MFIO is replaced. Go to step 9 to replace the MFIO.
you want to gracefully exit this procedure and back out of the upgrade without replacing any hardware	type 99, press Enter and go to step 47

9 Begin the MFIO replacement.

ATTENTION
Do not press 1 (1 to continue) at the console until you have replaced the MFIO module.

10 If applicable, the following warning may be displayed as the MFIO upgrade progresses.

```
0516-1193 chvg:  WARNING, once this operation is
completed, volume group rootvg cannot be imported into
AIX 430 or lower versions.  Continue (y/n)?
```

If this response is	Do
displayed	step 11
not displayed	step 12

11 Confirm the operation:

```
y
```

Response

```
0516-1164 chvg:  Volume group rootvg changed.  With
given characteristics rootvg can include up to 10
physical volumes with 3048 physical partitions each.
```

At the front of the CS 2000 Core Manager

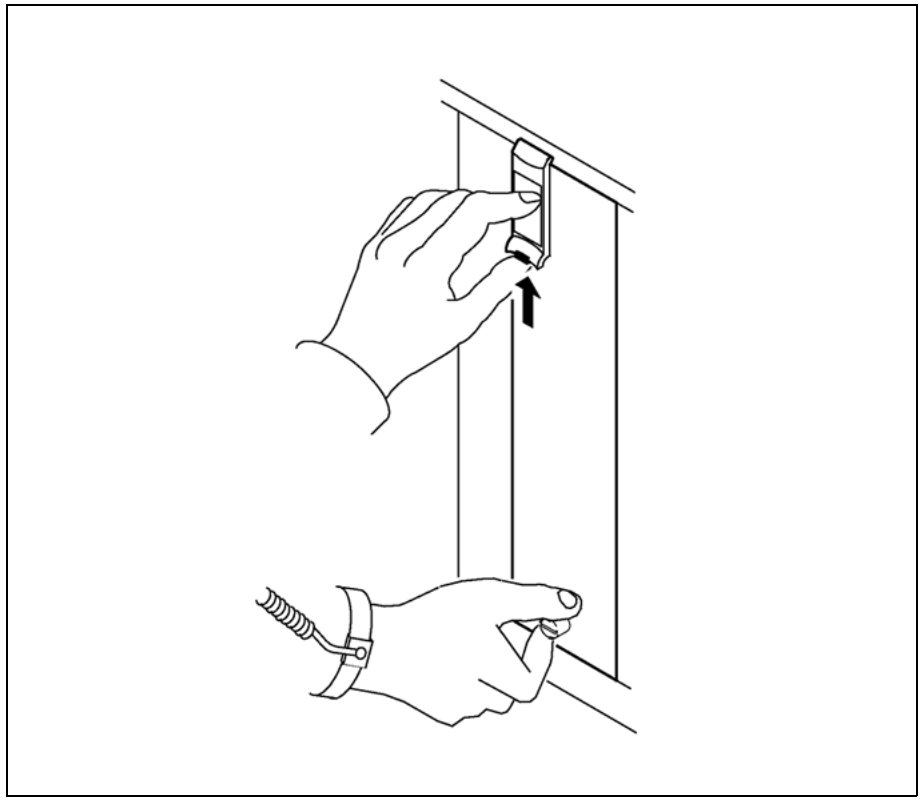
12 Wear an electrostatic discharge grounding wrist strap.

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.

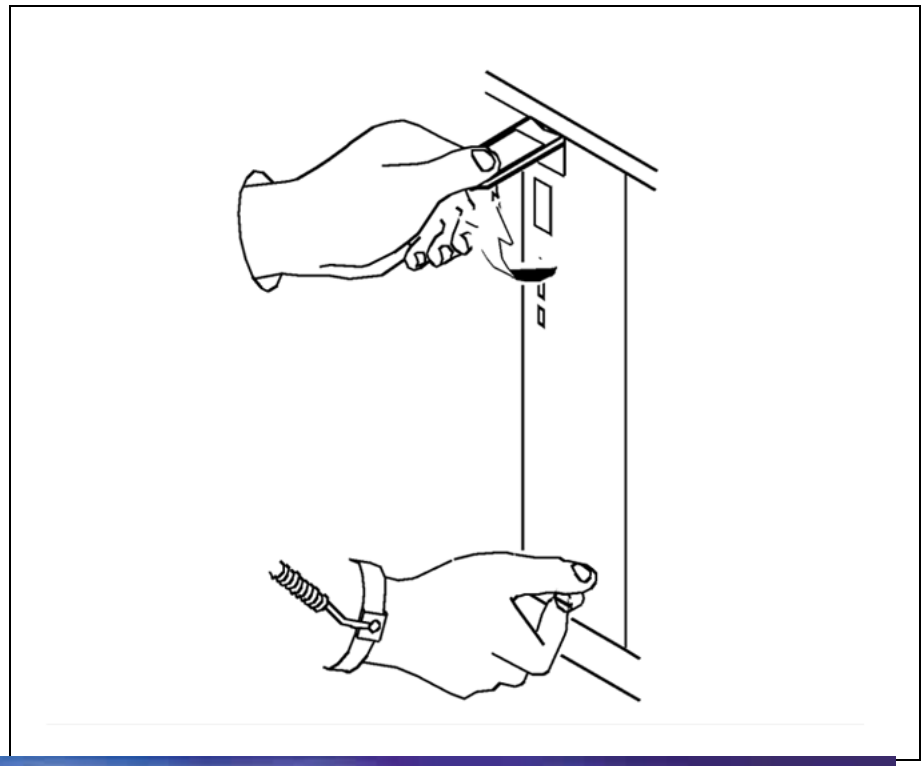
13 Make sure the LED of the module you want to upgrade is either red or off before you remove it.

14 Undo the thumbscrews located on the top and the bottom of the MFIO controller module to be upgraded. The thumbscrews are the captive type, and cannot be removed from the module.

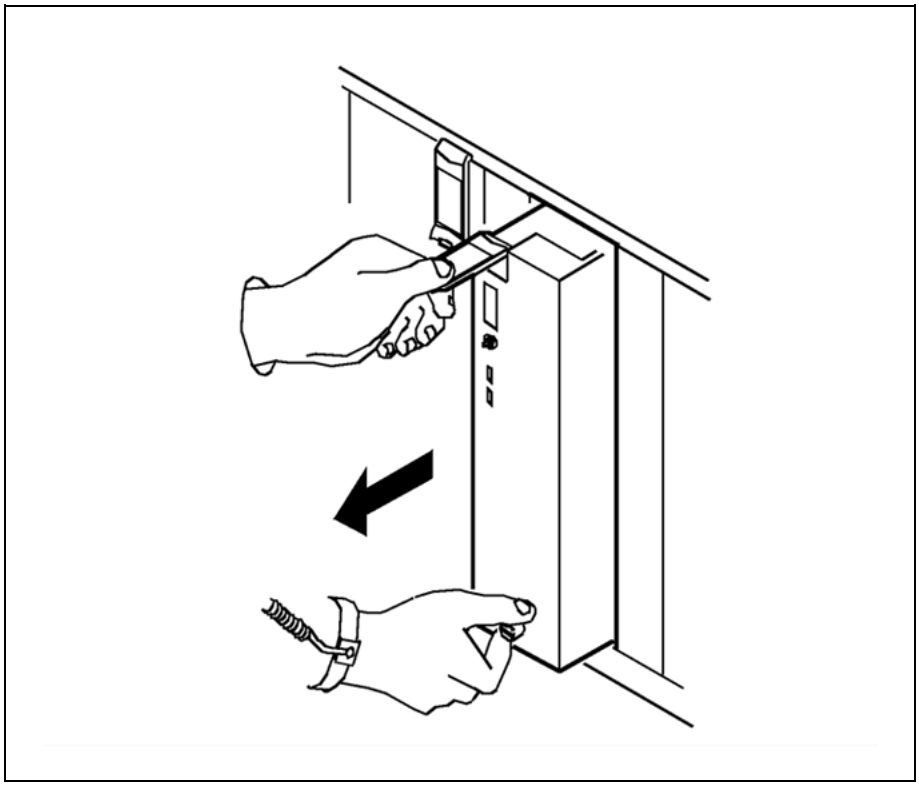
15 Depress the tip of the locking lever on the face of the MFIO controller module.



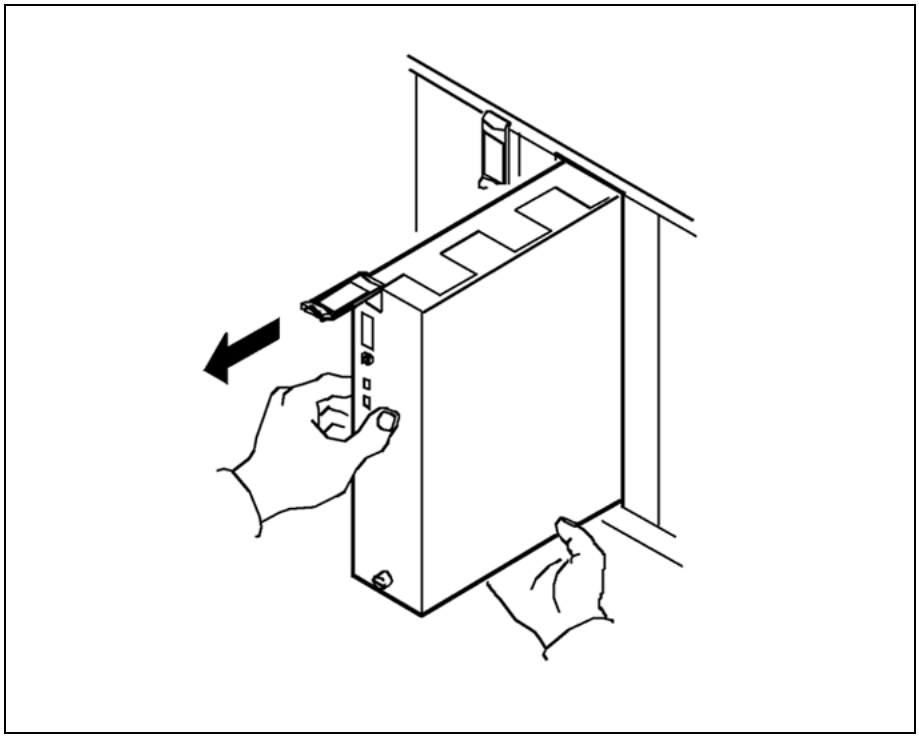
16 Open the locking lever on the face of the module by moving the lever outwards.



17 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



18 Hold the card 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.



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

At the back of the CS 2000 Core Manager

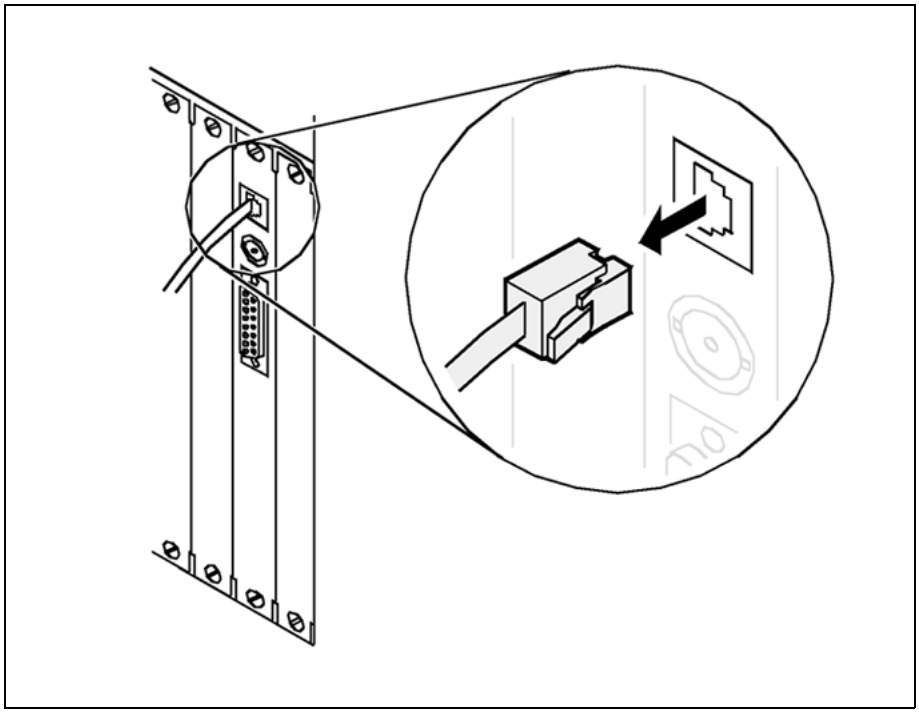
20 Determine if you are upgrading to the UMFIO.

If you are	Do
upgrading to the UMFIO	step 21
not upgrading to the UMFIO	step 32

21 Remove the existing LAN personality module and replace it with the new personality module (NTRX50NK or NTRX50NN) that came with the new UMFIO module. This must be done before inserting the new UMFIO module. It is located at the rear of the I/O controller module to be upgraded.

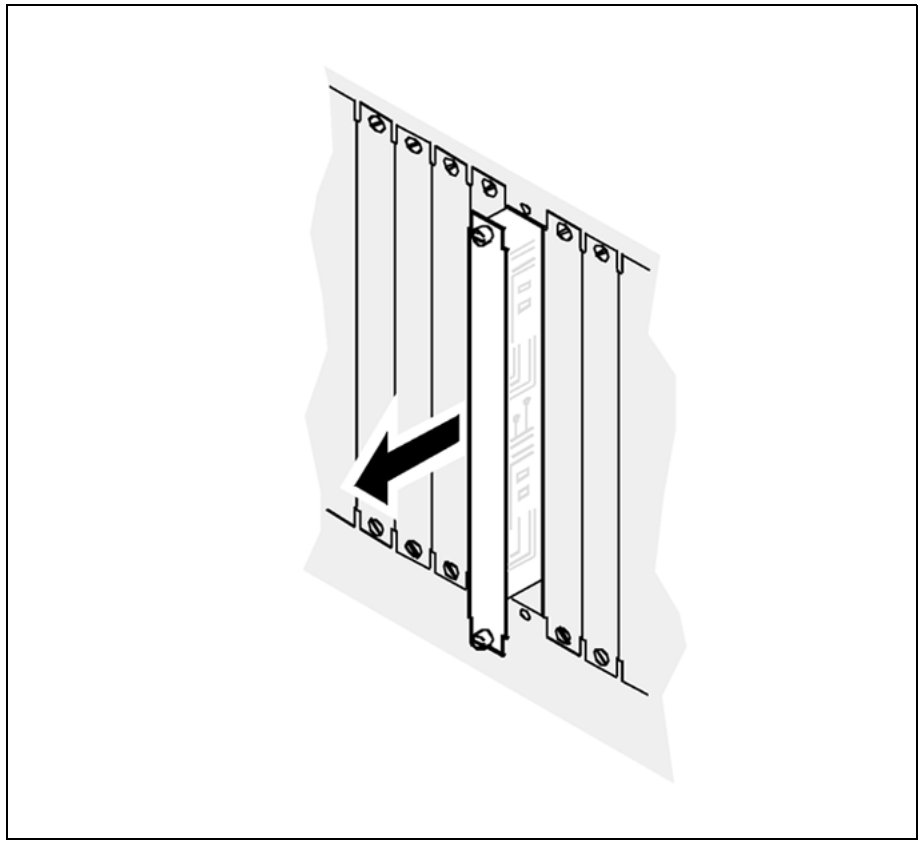
22 Label the Ethernet cable connected to the LAN personality module you wish to replace.

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

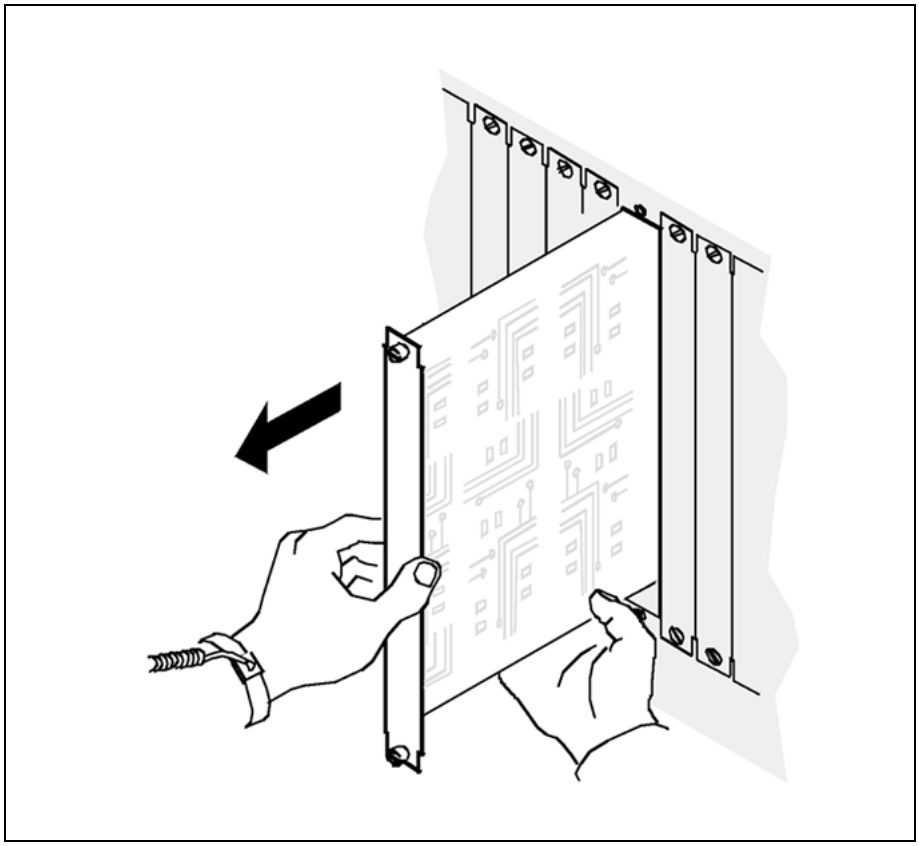


24 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module. The thumbscrews are the captive type, and cannot be removed from the module.

25 While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



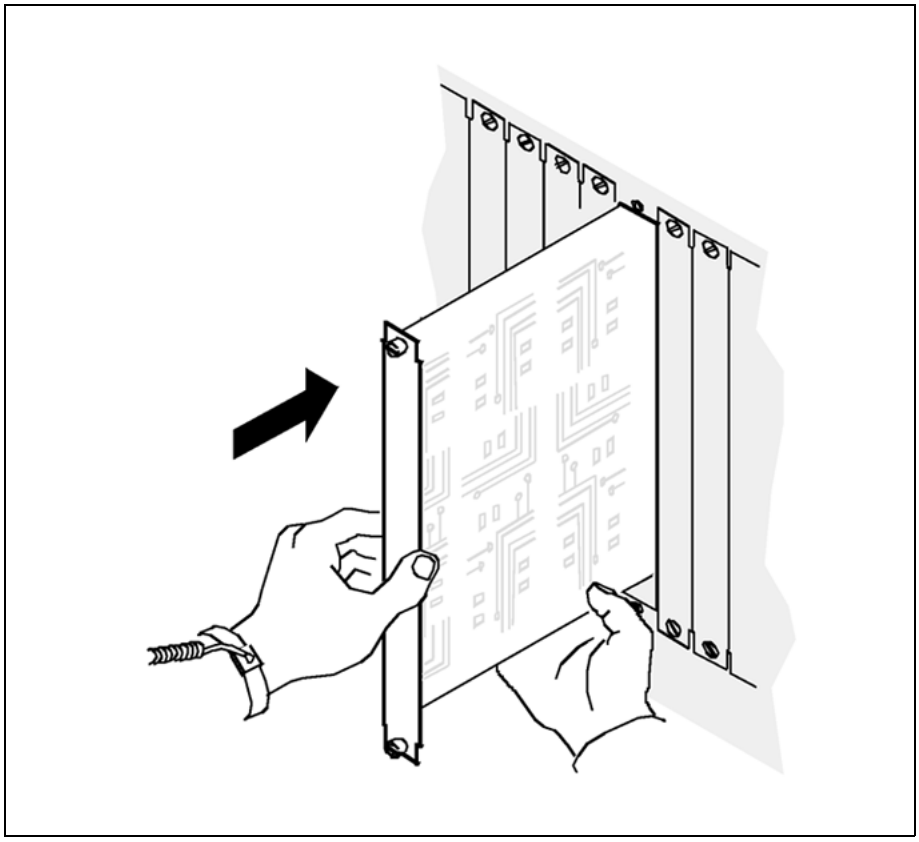
26 Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



27 Place the LAN personality module you have removed in an ESD protective container.

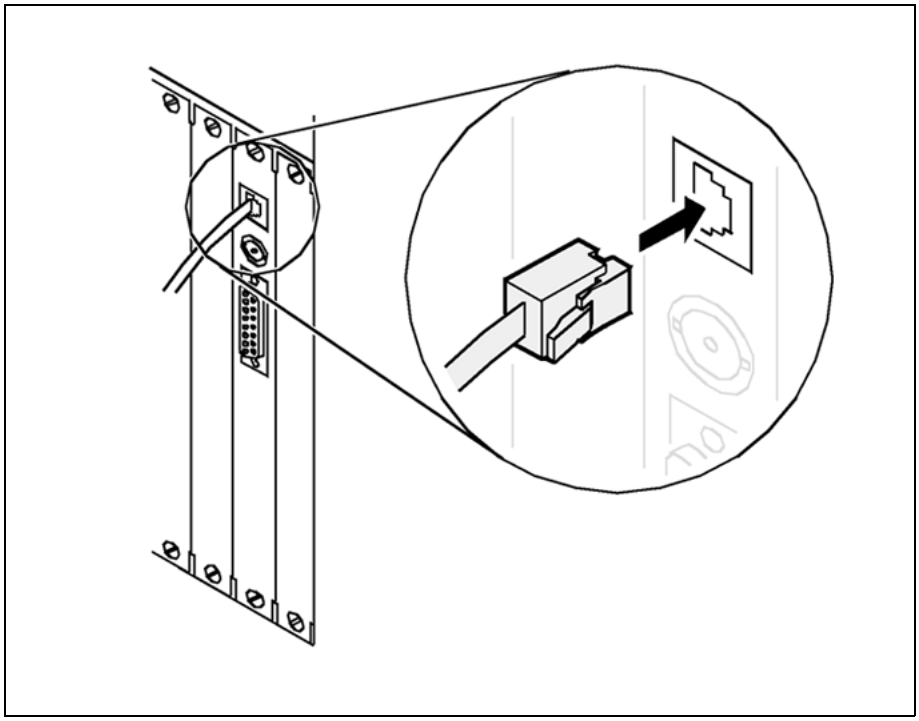
28 Insert the new personality module (either NTRX50NK or NTRX50NN) into the CS 2000 Core Manager shelf.

29 Gently slide the LAN personality module into the shelf until it is fully inserted.



30 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

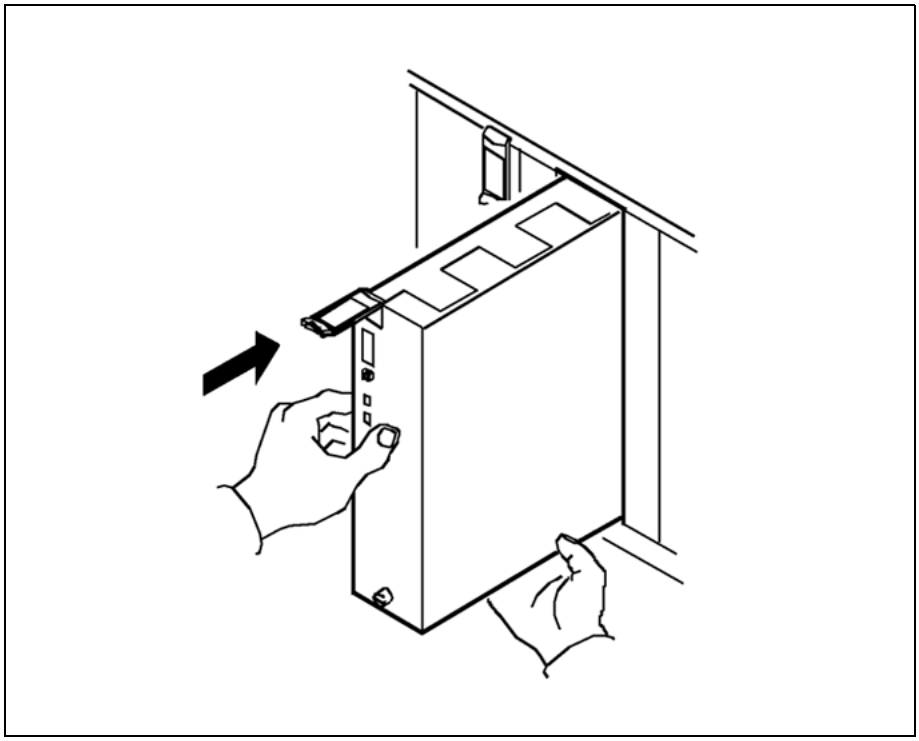
31 Reconnect the Ethernet cable to the LAN personality module. You can remove the label that you put on the cable in step 22.



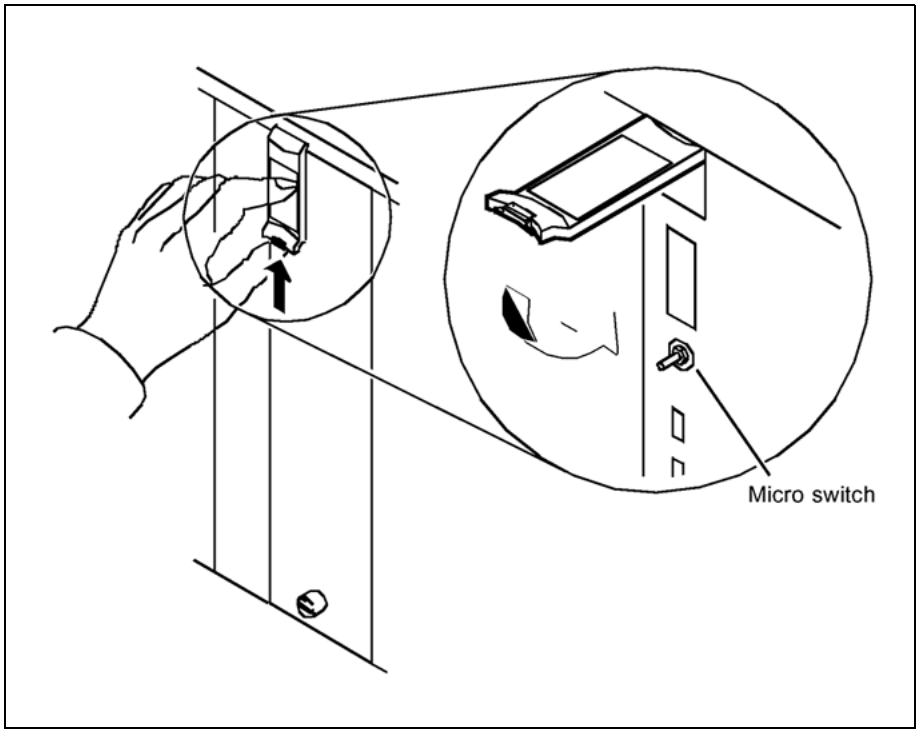
At the front of the CS 2000 Core Manager

32 Insert the PEC MFIO or PEC UMFIO module into the CS 2000 Core Manager shelf.

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



34 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.



35 Tighten the thumbscrews on the module.

At the VT100 console

36 Return to the console.

```
Replace ORIGINAL MFIO I/O-2 (c1-f2) with UPGRADED MFIO
Enter 1 to continue, 99 to exit:
```

37 Continue the upgrade. Type **1** and press Enter.

If only one MFIO controller module is replaced, the system responds as follows:

```
Transitioning forward from REPLACED to ONLINED
Transitioning forward from ONLINED to DEPENDENCIES_
ADDED
Transitioning forward from DEPENDENCIES_ADDED to
OFFLINED_AFTER_UPGRADE
Transitioning forward from OFFLINED_AFTER_UPGRADE to
ONLINED2
Transitioning forward from ONLINED2 to COMPLETE
>
```

If both the MFIO controller modules are replaced, the system responds as follows and the command 'ftrecfgpent' is executed to confirm if there is any Ethernet reconfiguration required once the upgrade for MFIO/UMFIO is completed for both the domains.

```
Transitioning forward from REPLACED to ONLINED
Transitioning forward from ONLINED to DEPENDENCIES_
ADDED
Transitioning forward from DEPENDENCIES_ADDED to
OFFLINED_AFTER_UPGRADE
Transitioning forward from OFFLINED_AFTER_UPGRADE to
ONLINED2
Transitioning forward from ONLINED2 to COMPLETE

Running the command 'ftrecfgpent'
```

38 Use the following table to determine your next step.

If the system	Do
prompts you to remove the X25 SYNC module from slot <n>	step 39
does not prompt you to remove the X25 SYNC module	step 41

39 Remove the X25 SYNC module from the slot indicated in the display.

Example response:

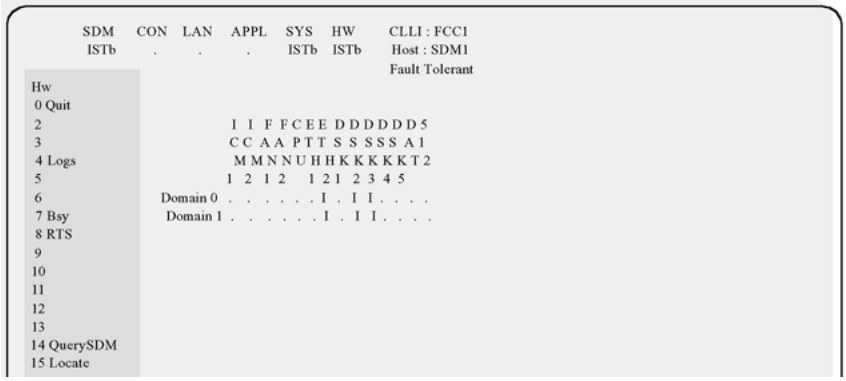
```
Please remove the X.25 SYNC module from the main chassis
slot 4.

Enter 1 to continue when ready:("1"):
```

40 Once you have removed the X25 SYNC module, continue the upgrade. Type:

1

The system begins reintegration and are automatically returned to the sdmmtc hardware level as shown in the following figure.

Hardware menu level

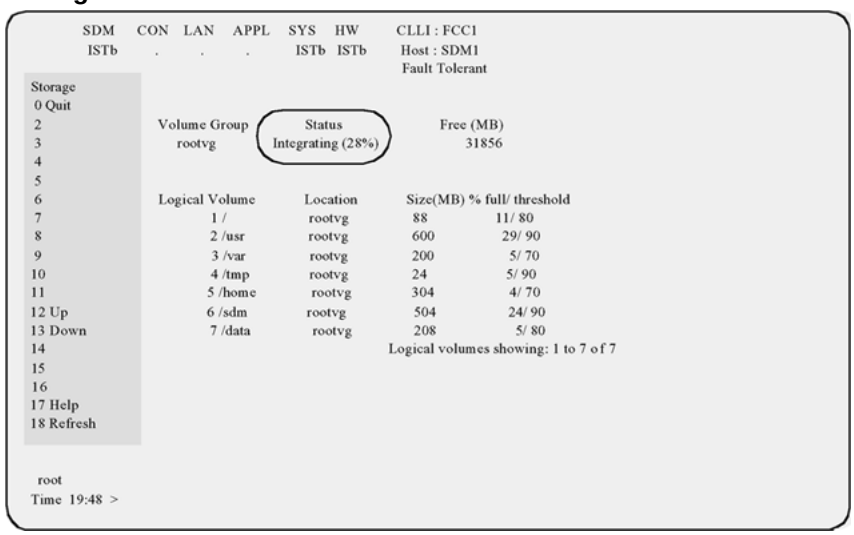


41 Use the following table to determine your next step.

If your system	Do
uses X.25 and you are upgrading to a UMFIO with X25PM, you must reconfigure the X.25 ports as part of the UMFIO upgrade. Reconfiguring the X.25 ports can be done during system reintegration.	Complete procedure Commissioning X.25 connectivity on page 172, then return to this procedure and continue with the next step.
does not use X.25	step 42

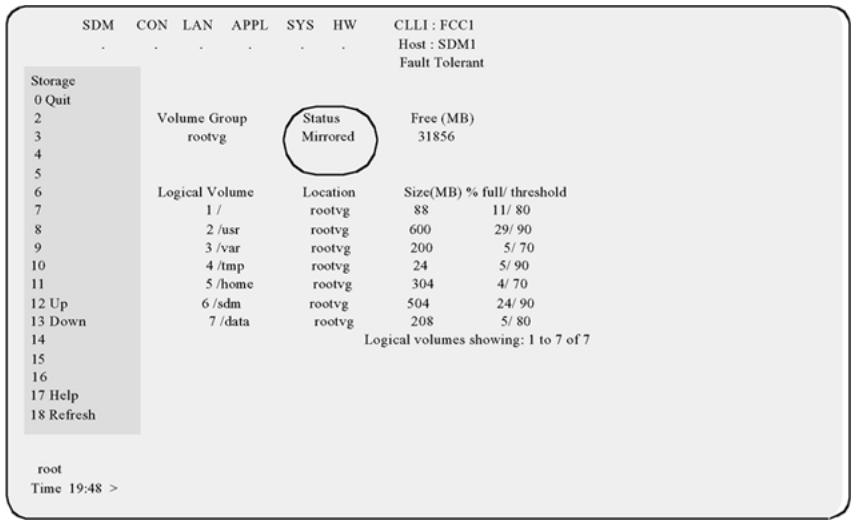
42 Monitor the system reintegration at the storage level, shown in the following figure.

Storage menu level



43 Once reintegration is complete the status of the volume group changes to Mirrored as shown in the following figure.

Storage menu level



44 Verify that the correct module was used as a replacement:

```
locate
```

The system displays a list of hardware.

45 Confirm that the correct PEC is listed for the newly upgraded module.

46 Upgrade the MFIO /UMFIO module in the other domain by repeating steps 4 through 45, then continue to the next step.

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

—End—

Upgrading a datavg MFIO to MFIO or UMFIO

Purpose

Use this procedure to perform the following Multifunction Input/Output (MFIO) to MFIO or Ultra-Multifunction Input/Output (UMFIO) upgrades:

- 4GB + 4GB MFIO to 9GB + 9GB MFIO
- 4GB + 4GB MFIO to 36GB + 36GB UMFIO
- 9GB + 9GB MFIO to 36GB + 36GB UMFIO

Application

You can also use this procedure to upgrade to other supported combinations. For the list of supported combinations, refer to the table "Supported MFIO and UMFIO, datavg and rootvg configurations" in *Upgrading the CS 2000 Core Manager*, NN10060-461.

> ***Note:*** As of the 15.2 release, the system allows you to gracefully back out of an MFIO upgrade.

You can use this procedure to revert to the original MFIO in a single domain, but only when the procedure is complete and you have confirmed that the storage system has regained full disk mirroring. Do not use this procedure to revert to the original MFIO if you have successfully upgraded the MFIO in both domains.

CAUTION
Possible loss of intercept service
If the MFIO to be upgraded supports lawful intercept through an X.25 interface, this procedure removes lawful intercept from service for a short period of time. After you complete the upgrade procedure, you must restart the lawful intercept application.

Refer to the following table for the product engineering codes.

Nortel PEC	Name
NTRX50FS (back)	LAN personality module for MFIO
NTRX50GP (front)	4GB + 4GB datavg MFIO

Nortel PEC	Name
NTRX50NC (front) ***Note:*** Replacements for the NTRX50NC are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004 the NTRX50NL is the replacement for the NTRX50NC.	9GB + 9GB datavg MFIO
NTRX50NK (back)	LAN personality module for UMFIO The NTRX50NK is required if you want to use the datavg UMFIO (NTRX50NL) for LAN access. If you intend to use the datavg UMFIO for storage only, or if you do not currently have LAN cards, you do not need to install the NTRX50NK.
NTRX50NN (back)	X25 personality module for UMFIO
NTRX50NL (front)	36GB + 36GB datavg UMFIO

Prerequisites and guidelines

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

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

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

ATTENTION

Perform a backup of your billing files before starting this procedure. Also, ensure that an S-tape (System Image Tape) of your CS 2000 Core Manager is made prior to starting the upgrade procedures.

ATTENTION

Upgrading a mirrored pair of MFIOs can require a full maintenance window to complete. If an expansion chassis is provisioned, the upgrade of additional mirrored pairs of MFIOs can require multiple maintenance windows.

ATTENTION

You must be a user authorized to perform config-admin actions to perform this procedure.

ATTENTION

A UMFIO upgrade requires the UMFIO LAN personality module (NTRX50NK) or the X25 personality module (NTRX50NN).

No CS 2000 Core Manager should be populated with more than 2 MFIOs per I/O domain (for any combination) as part of datavg.

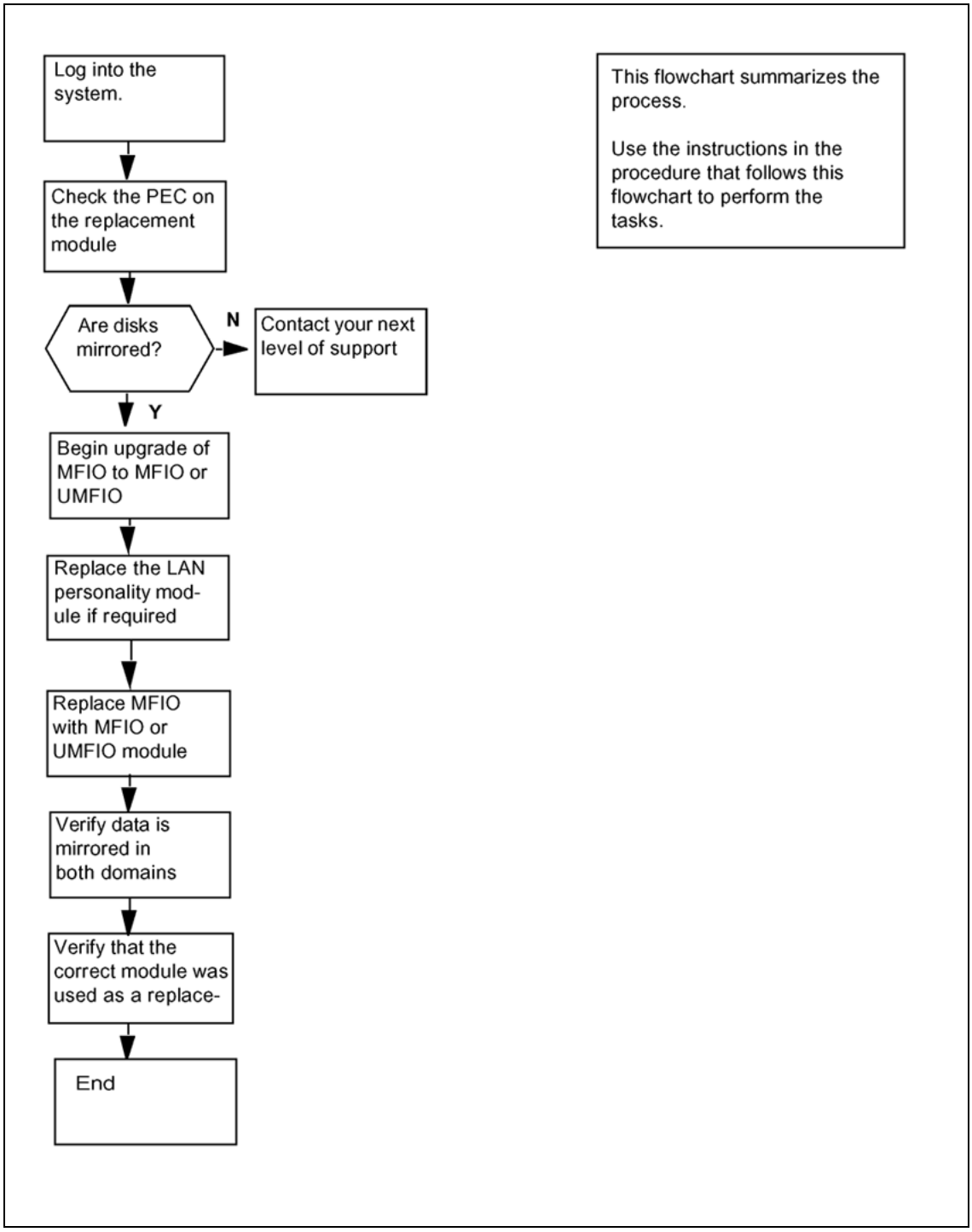
Nortel recommends that the MFIOs in the main chassis be upgraded first, starting with domain 1 and ending with domain 0. After upgrading the main chassis, proceed to upgrade the expansion chassis, if there is one. Datavg modules must be upgraded in pairs. For example, if you upgrade the MFIO in slot 4 of the main chassis, you must also upgrade the MFIO module in slot 15 of the main chassis. Refer to the following table for more information about upgrading MFIO pairs.

Upgrade Sequence	Domain 0	Domain 1	MFIO davavg pairing location
1	slot 4	slot 15	main chassis
2	slot 1	slot 9	expansion chassis
3	slot 3	slot 11	expansion chassis
4	slot 5	slot 13	expansion chassis
5	slot 7	slot 15	expansion chassis

Procedure

The task flow diagram that follows provides a summary of this process. Use the instructions in the procedure that follows the flowchart to perform the tasks.

Task flow for Upgrading a datavg MFIO to MFIO or UMFIO (datavg)



Procedure

ATTENTION

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

Upgrading a datavg MFIO to MFIO or UMFIO

Step	Action

At the VT100 console

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

2 Check the label on the module that you want to use as a replacement. Make sure that label shows the product engineering code (PEC) that you want to use for your upgrade.

3 Determine the physical location of the hard disk drives:

```
locate
```

Example response:

Site	Flr	RPos	Bay_id	Shf	Description	Slot	EqPEC
HOST	01	A02	CSDM	SDMM	512(0)	01	NTRX50GA FRNT
HOST	01	A02	CSDM	SDMM		01	NTRX50FS BACK
HOST	01	A02	CSDM	SDMM	ETH(0),DSK1(0),DAT(0)	02	NTRX50GN FRNT
HOST	01	A02	CSDM	SDMM		02	NTRX50FS BACK
HOST	01	A02	CSDM	SDMM	DSK2(0),DSK3(0)	04	NTRX50GP FRNT
HOST	01	A02	CSDM	SDMM	CPU(0)	06	NTRX50FK FRNT
HOST	01	A02	CSDM	SDMM		06	NTRX50FD BACK
HOST	01	A02	CSDM	SDMM	CPU(1)	10	NTRX50FK FRNT
HOST	01	A02	CSDM	SDMM	512(1)	12	NTRX50GA FRNT
HOST	01	A02	CSDM	SDMM		12	NTRX50GH BACK
HOST	01	A02	CSDM	SDMM	ETH(1),DSK1(1),DAT(1)	13	NTRX50GN FRNT
HOST	01	A02	CSDM	SDMM		13	NTRX50FS BACK
HOST	01	A02	CSDM	SDMM	DSK2(1),DSK3(1)	15	NTRX50GP FRNT
HOST	01	A02	CSDM	SDMM	FAN1(0)	--	NTRX50FE FRNT
HOST	00	A02	CSDM	SDMM	FAN1(1)	--	NTRX50FF FRNT
HOST	01	A02	CSDM	SDME	ICM1(0)	--	NTRX50FG BACK
HOST	01	A02	CSDM	SDME	ICM1(1)	--	NTRX50FH BACK
HOST	01	A02	CSDM	SDME	DSK4(0), DSK5(0)	01	NTRX50FU FRNT

4 Using the information displayed, record the physical location of all hard disk drives in order to avoid removing the wrong drive. It is necessary to also record the chassis, slot, and PEC of the IO module you want to upgrade:

chassis (Shf)
is the chassis where the IO module you want to upgrade is located. The main chassis is identified as sdmm. The expansion chassis is identified as sdme. The chassis identifier is displayed under the Shf heading.

Slot
is the slot number (1-16) in the chassis where the IO module to be upgraded is located. The slot number is displayed under the Slot heading.

pec (EqPEC)
is the product engineering code for the IO controller module you want to add (either NTRX50NC or NTRX50NL).

ATTENTION
Replacements for the NTRX50NC are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NL is the replacement for the NTRX50NC.

5 Ensure that the datavg logical volumes are in sync:

```
lsvg -l datavg
```

From the output, confirm that all logical volumes have a status of open/syncd under column LV State, and that each logical volume has 2 physical volumes under column PVs.

If	Do
all logical volumes show LV State as open/syncd and PVs as 2	step 6
not all logical volumes show LV State as open/syncd or PVs as 2	contact your next level of support

6 Access the storage level:

```
sdmmtc storage
```

If the status of the datavg disks is	Do
mirrored	step 7
not mirrored	contact your next level of support

7 Access the hardware level:

```
hw
```

8 Upgrade the MFIO:

```
upgrade <chassis> <slot> <PEC>
```

where

<chassis>

is the chassis where the MFIO module to be upgraded is located. The main chassis is identified as 'sdmm'. The expansion chassis is identified as 'sdme'.

<slot>
is the slot number (1-16) in the chassis where the MFIO module to be upgraded is located

Note: For slots 1-9 you are not required to enter a 0 (zero) before the slot number. For instance, to specify slot 5, enter 5 not 05.

<PEC>
is the product engineering code for the MFIO or the UMFIO controller module you want to add (either NTRX50NC or NTRX50NL)

Note: Replacements for the NTRX50NC are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NL is the replacement for the NTRX50NC.

Example
upgrade sdmm 4 NTRX50NL

This example indicates an upgrade to the 36GB + 36GB UMFIO in slot 4 of the main chassis.

If you are	Do
prompted to delete an X.25 interface	step 9
not prompted to deleted an X.25 interface	step 14

9 Confirm the deletion of the X.25 interface:

Y

The system responds:

```
Transitioning forward from START to INFO_RETRIEVED

Volume group = datavg on hdisk4
Physical partition size 16 with max partitions 3048

Volume group = datavg on hdisk5
Physical partition size 16 with max partitions 3048

Transitioning forward from INFO_RETRIEVED to OFFLINED
Transitioning forward from OFFLINED to DEPENDENCIES_REMOVED
Transitioning forward from DEPENDENCIES_REMOVED to REPLACED

Replace ORIGINAL MFIO I/O-1 (c1-f15) with UPGRADED MFIO

Enter 1 to continue, 99 to exit:
```

10 Use the following table to determine your next step.

If	Do
you want to replace the MFIO	Do not type 1 at the console until the MFIO is replaced. Go to step 11 to replace the MFIO.
you want to gracefully exit this procedure and back out of the upgrade without replacing any hardware	Type 99, press Enter and go to step 46

11 Begin the replacement of the MFIO.

ATTENTION
Do not press 1 (1 to continue) at the console until you have replaced the MFIO module.

12 If applicable, the following warning may be displayed as the MFIO upgrade progresses.

```
0516-1193 chvg:  WARNING, once this operation is
completed, volume group rootvg cannot be imported into
AIX 430 or lower versions.  Continue (y/n)?
```

If this response is	Do
displayed	step 13
not displayed	step 14

13 Confirm the operation:

```
y
```

Response

```
0516-1164 chvg:  Volume group rootvg changed.  With
given characteristics rootvg can include up to 10
physical volumes with 3048 physical partitions each.
```

At the front of the CS 2000 Core Manager

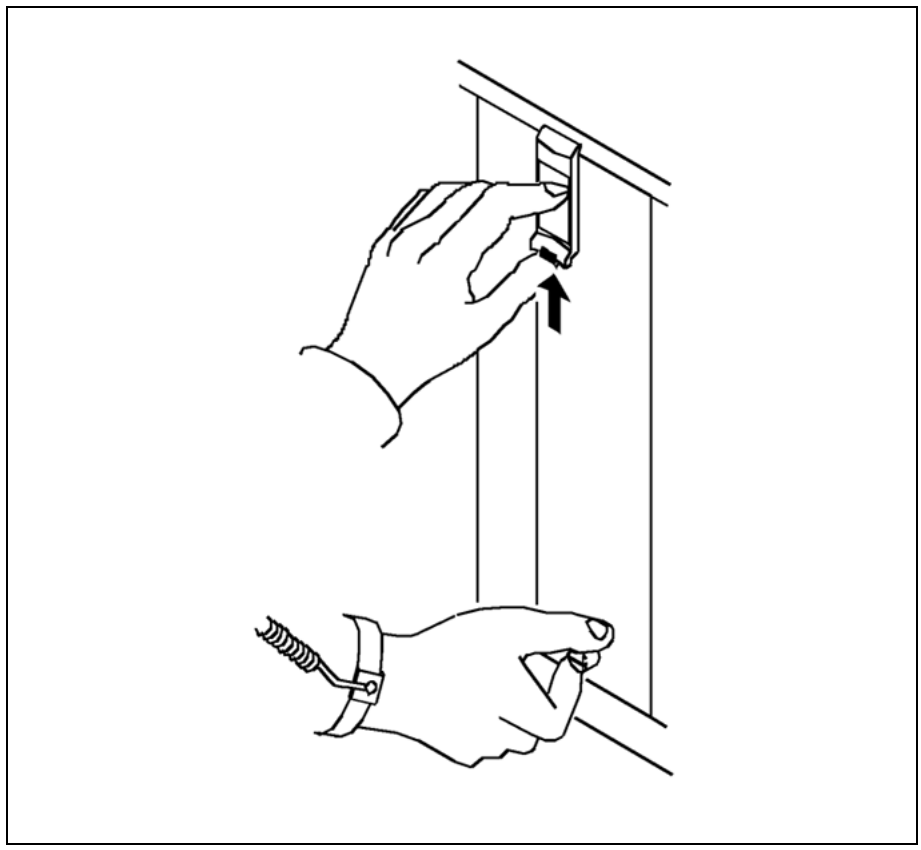
14 Wear an electrostatic discharge grounding wrist strap.

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.

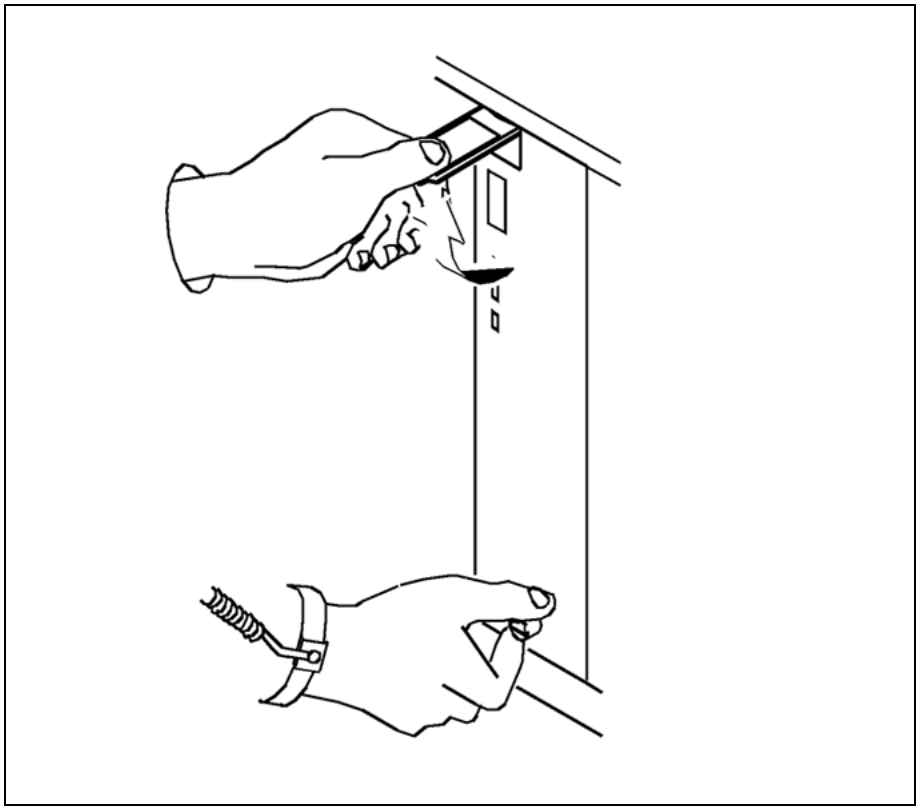
15 Make sure the LED of the module you want to upgrade is either red or off before you remove it.

16 Undo the thumbscrews located on the top and the bottom of the MFIO controller module to be upgraded. The thumbscrews are the captive type, and cannot be removed from the module.

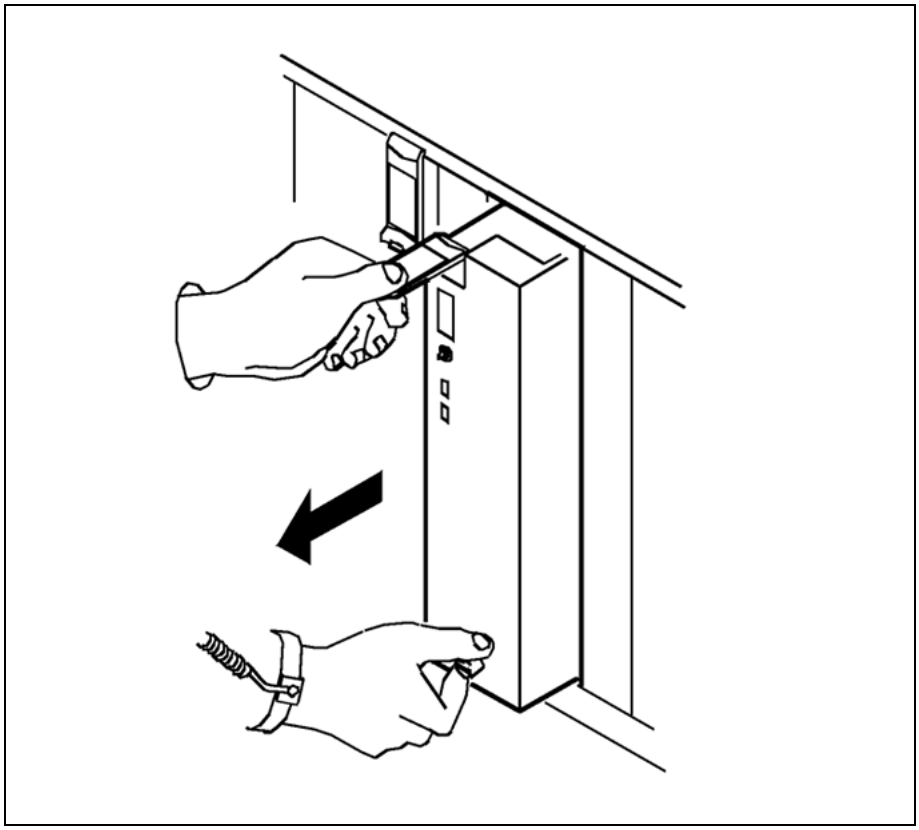
17 Depress the tip of the locking lever on the face of the MFIO controller module.



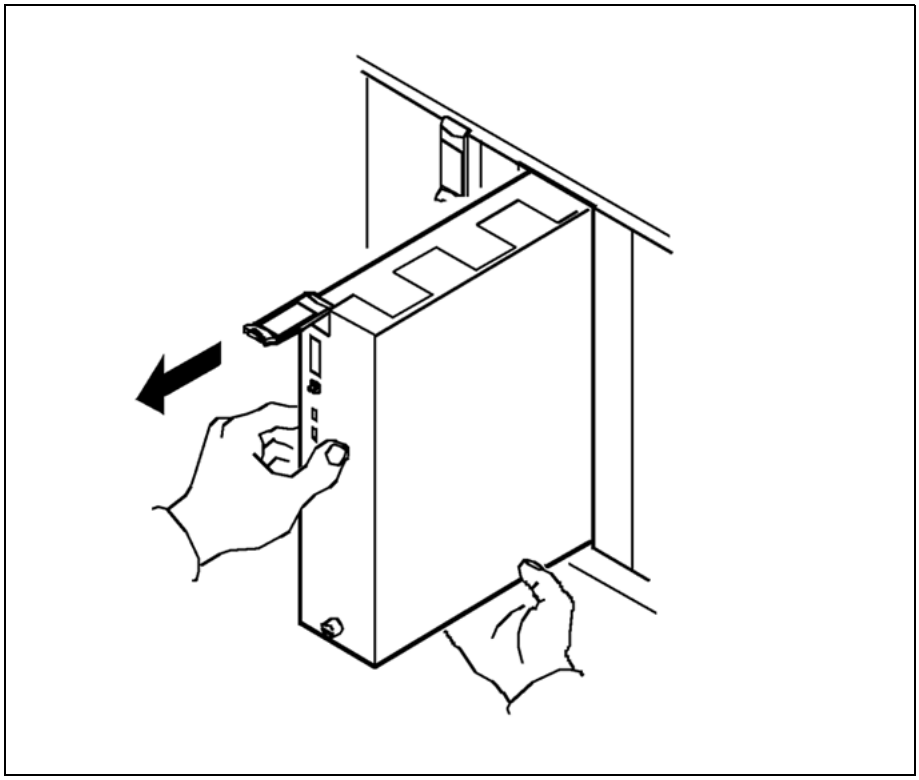
18 Open the locking lever on the face of the module by moving the lever outwards.



19 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the shelf.



20 Hold the card 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.

At the back of the CS 2000 Core Manager

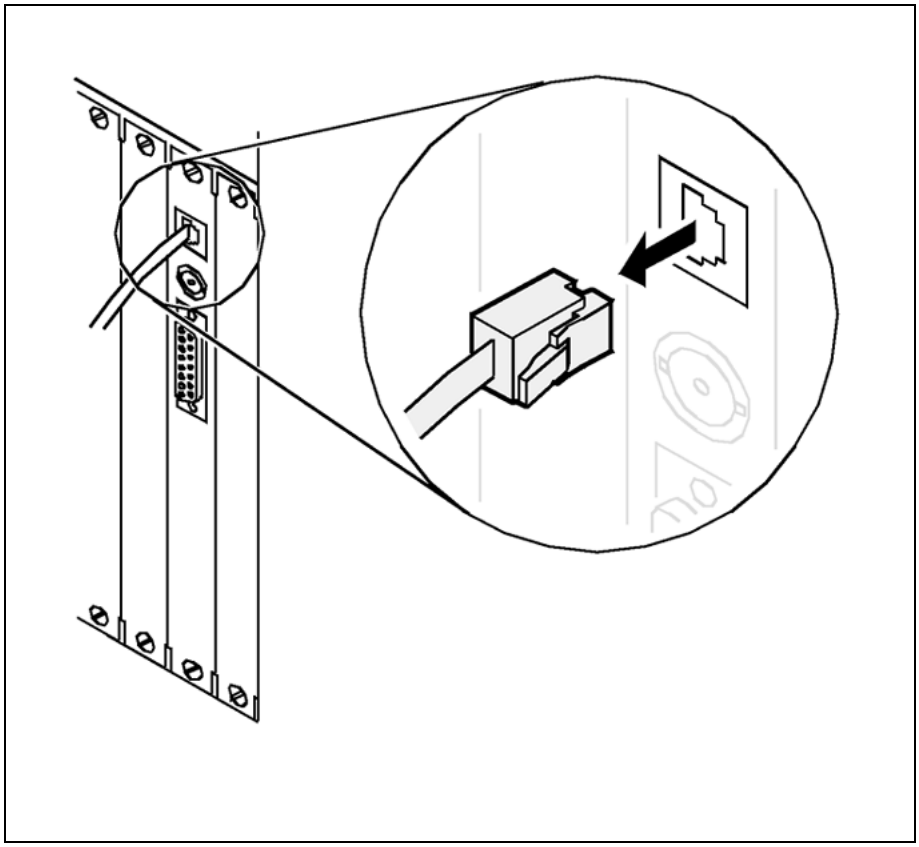
22 Determine if you are upgrading to UMFIO.

If you are	Do
upgrading to UMFIO	step 23
not upgrading to UMFIO	step 34

23 Removing the existing LAN personality module and replace it with the new personality module (NTRX50NK or NTRX50NN) that came with the new UMFIO module. This must be done before inserting the new UMFIO module. It is located at the rear of the I/O controller module to be upgraded.

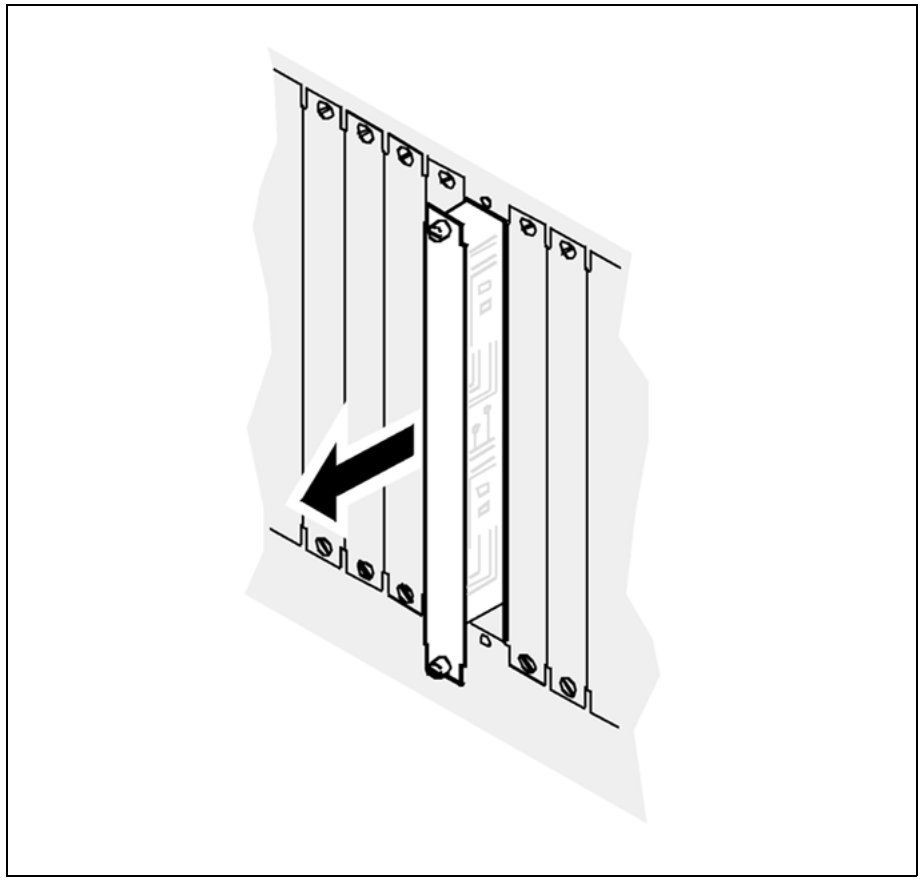
24 Label the Ethernet cable connected to the LAN personality module you want to replace.

25 Identify the correct LAN module (slot and PEC code) you wish to remove and disconnect the Ethernet cable, as shown in the following diagram.

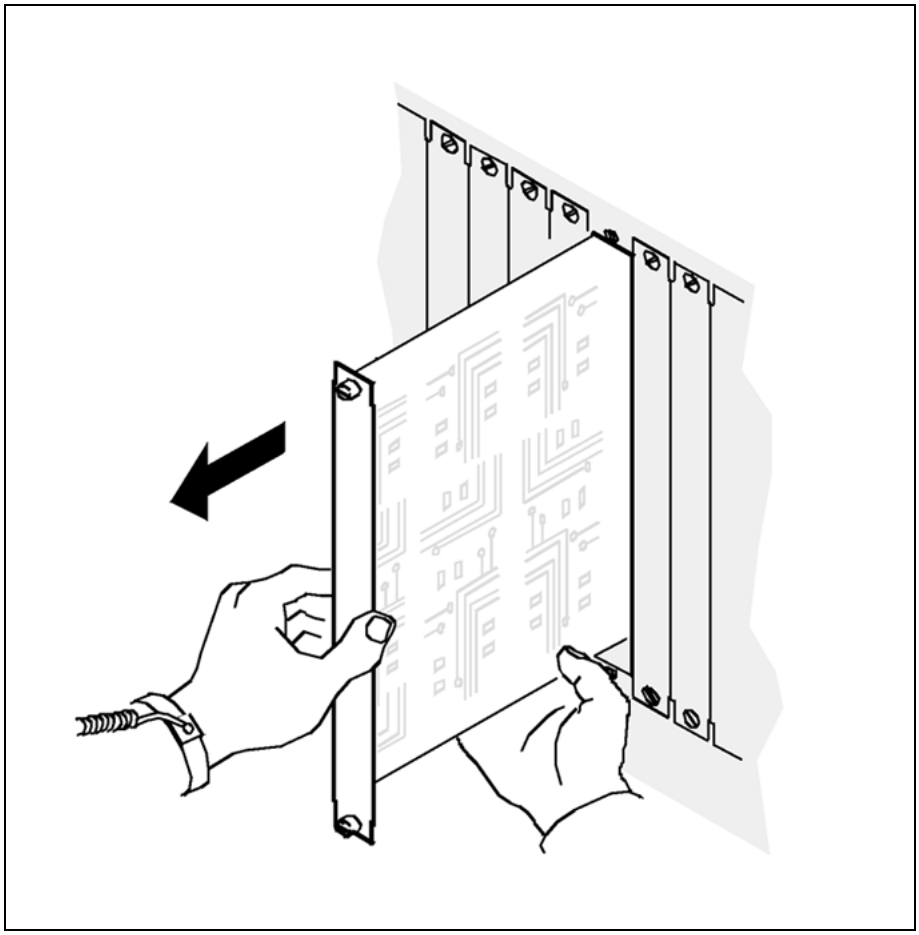


26 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module. The thumbscrews are the captive type, and cannot be removed from the module.

27 While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in. (5 cm) from the shelf.



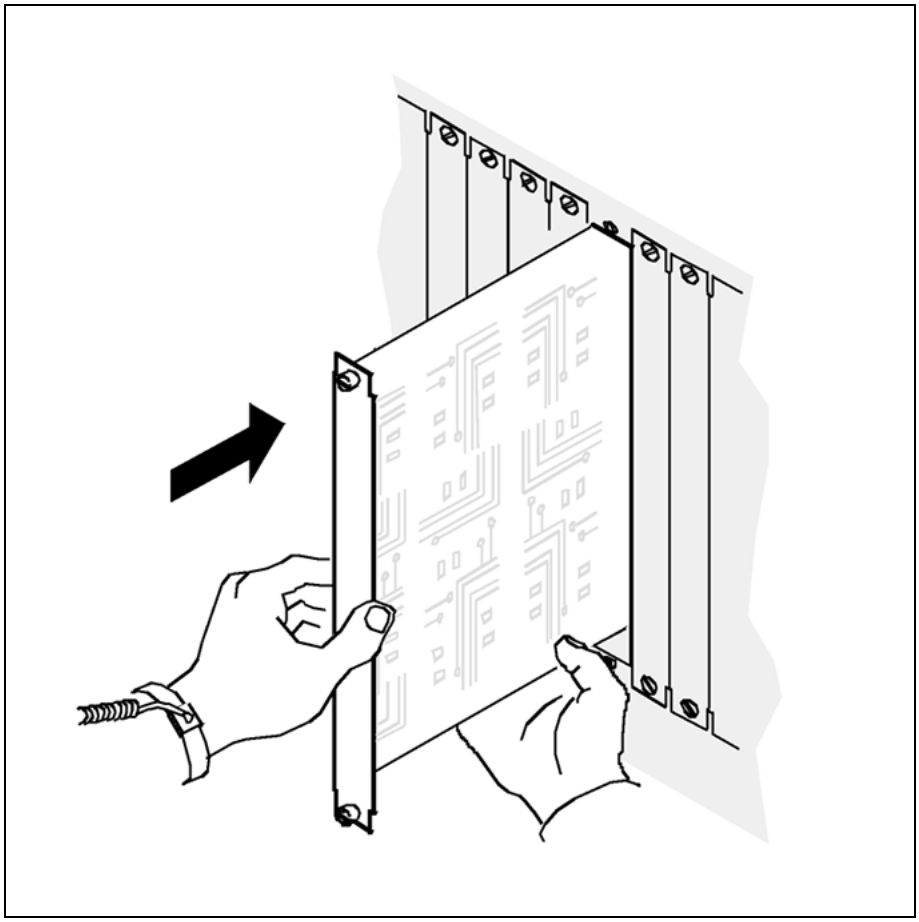
28 Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



29 Place the LAN personality module you have removed in an ESD protective container.

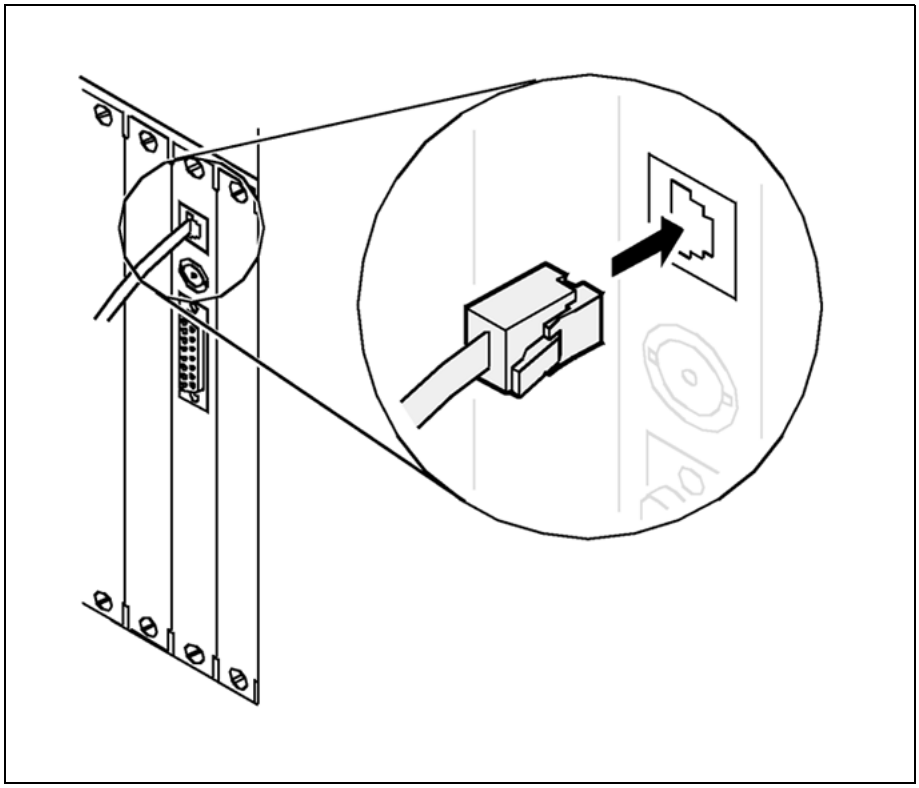
30 Insert the new LAN personality module (either NTRX50NK or NTRX50NN) into the shelf.

31 Gently slide the LAN personality module into the shelf until it is fully inserted.



32 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

33 Reconnect the Ethernet cable to the LAN personality module. You can remove the label you put on the cable in step 24.

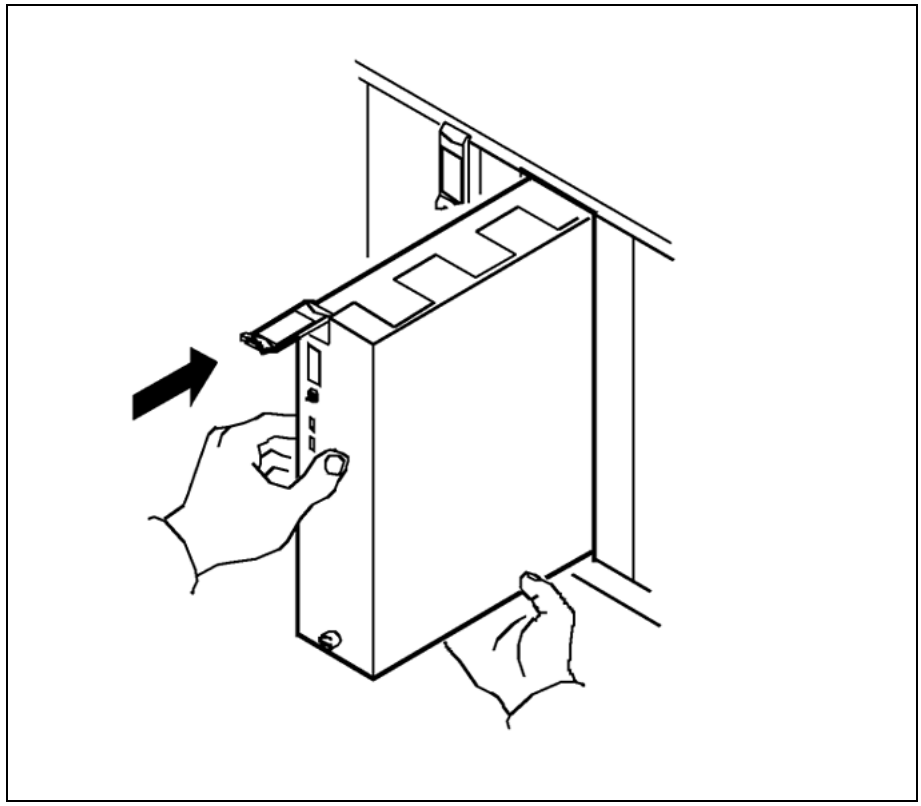


At the front of the CS 2000 Core Manager

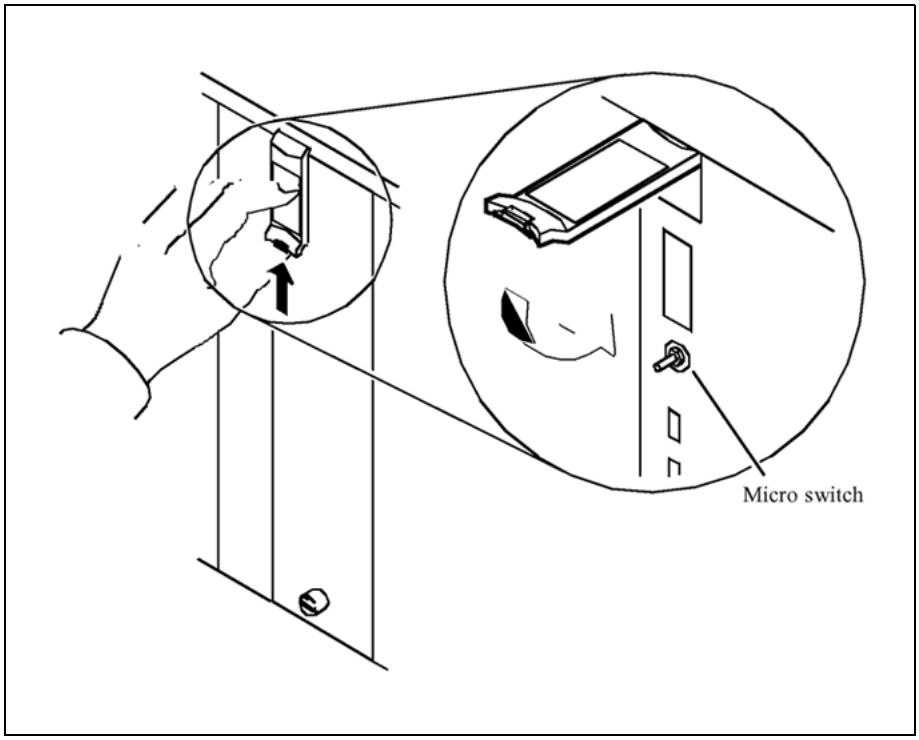
34 Insert the NTRX50NC MFIO / NTRX50NL UMFIO module into the shelf.

> ***Note:*** Replacements for the NTRX50NC are filled on a best-effort basis before and after the MD date of 31 December 2004. After 31 December 2004, the NTRX50NL is the replacement for the NTRX50NC.

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



36 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.



37 Tighten the thumbscrews on the module.

38 Return to the console.

```
Replace ORIGINAL MFIO I/O-2 (c1-f2) with UPGRADED MFIO
Enter 1 to continue, 99 to exit:
```

39 Continue the upgrade. Type `1` and press Enter.

If only one MFIO controller module is replaced, the system responds as follows:

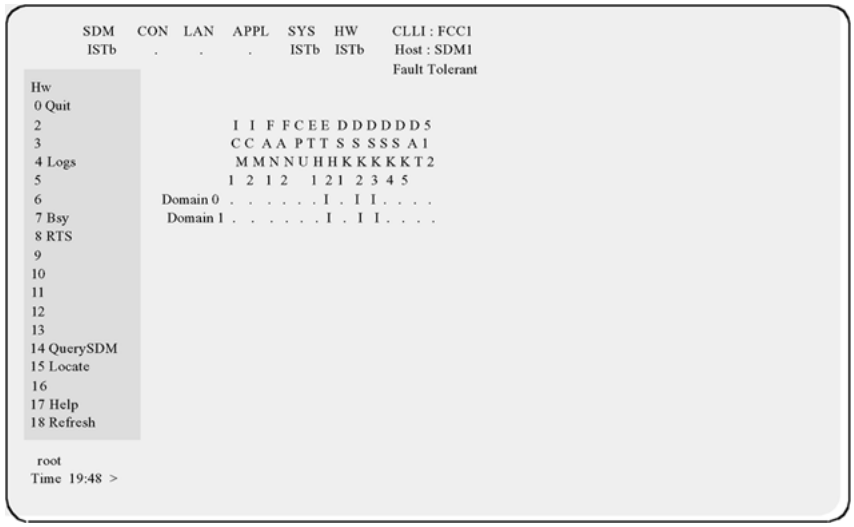
```
Transitioning forward from REPLACED to ONLINED
Transitioning forward from ONLINED to DEPENDENCIES_
ADDED
Transitioning forward from DEPENDENCIES_ADDED to
OFFLINED_AFTER_UPGRADE
Transitioning forward from OFFLINED_AFTER_UPGRADE to
ONLINED2
Transitioning forward from ONLINED2 to COMPLETE
>
```

If both the MFIO controller modules are replaced, the system responds as follows and the command 'ftrecfgpent' is executed to confirm if there is any Ethernet reconfiguration required once the upgrade for MFIO/UMFIO is completed for both the domains.

```
Transitioning forward from REPLACED to ONLINED
Transitioning forward from ONLINED to DEPENDENCIES_
ADDED
Transitioning forward from DEPENDENCIES_ADDED to
OFFLINED_AFTER_UPGRADE
Transitioning forward from OFFLINED_AFTER_UPGRADE to
ONLINED2
Transitioning forward from ONLINED2 to COMPLETE

Running the command 'ftrecfgpent'
```

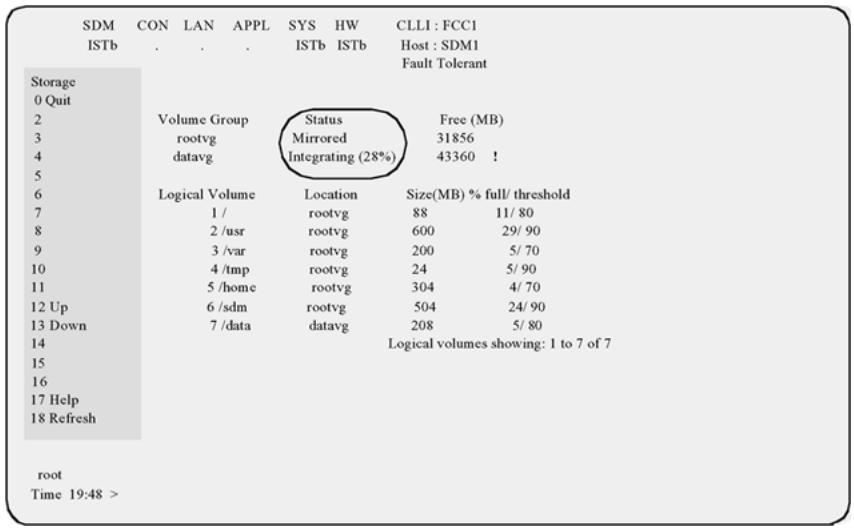
The system begins reintegration and you are automatically returned to the sdmmtc Hardware level.

Hardware menu level



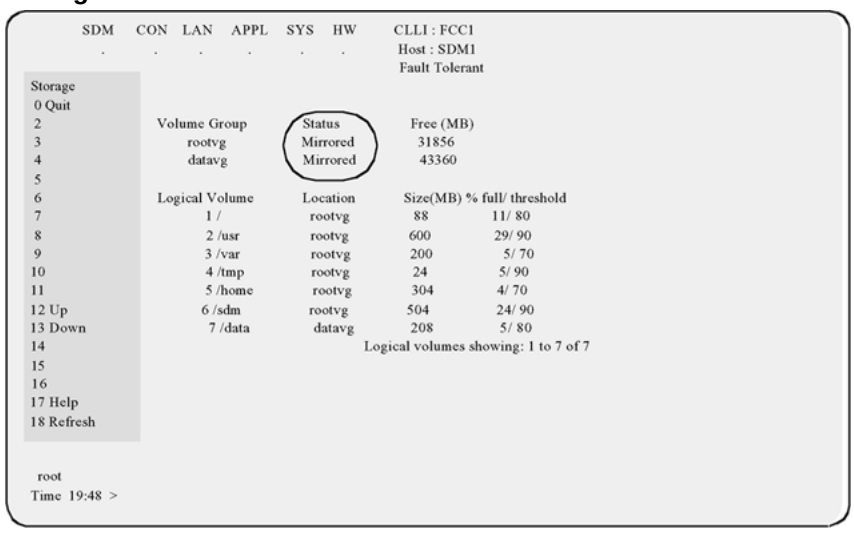
40 Monitor the system reintegration at the storage level, shown in the following figure.

Storage menu level



41 Once the system completes the reintegration, the status of the volume group changes to Mirrored.

Storage menu level



42 Verify that the correct module was used as a replacement:

```
locate
```

The system displays a list of hardware.

43 Confirm that the correct PEC is listed for the newly upgraded module.

44 Upgrade the MFIO / UMFIO module in the other domain by repeating steps 1 through 46 (if necessary, you can skip step 3).

45 Once the MFIO/UMFIO upgrade is completed successfully, perform the backup of the SDM using the procedure "Creating system image backup tapes (S-tapes) manually" in *CS 2000 Core Manager Security and Administration*, NN10170-611. S-tapes taken henceforth should be used to restore the SDM if required in the future, by following the procedure "Performing a full restore of the software from S-tape" in *CS 2000 Core Manager Fault Management*, NN10082-911.

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

—End—

Upgrading the DS512 controller module from NTRX50GA to GX

Purpose

Use this procedure to perform a DS512 controller module upgrade from an NTRX50GA to an NTRX50GX module.

This procedure allows the CS 2000 Core Manager applications to continue without interruption. During this procedure, one of the two DS512 controller modules remains in service while the other is being replaced. The state of applications running on the CS 2000 Core Manager is not a factor in this procedure. However, Nortel recommends that you perform this procedure during a roughage period.

Note: The NTRX50GA and NTRX50GX DS512 controller modules function identically, However, the NTRX50GX DS512 controller module has increased buffer memory with 16 kilobytes per link.

Prerequisites

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

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

Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	*CS 2000 Core Manager Security and Administration*, NN10170-611
Displaying actions a user is authorized to perform	*CS 2000 Core Manager Security and Administration*, NN10170-611

The NTRX50GX DS512 controller module requires software version SDMN0010 (or higher).

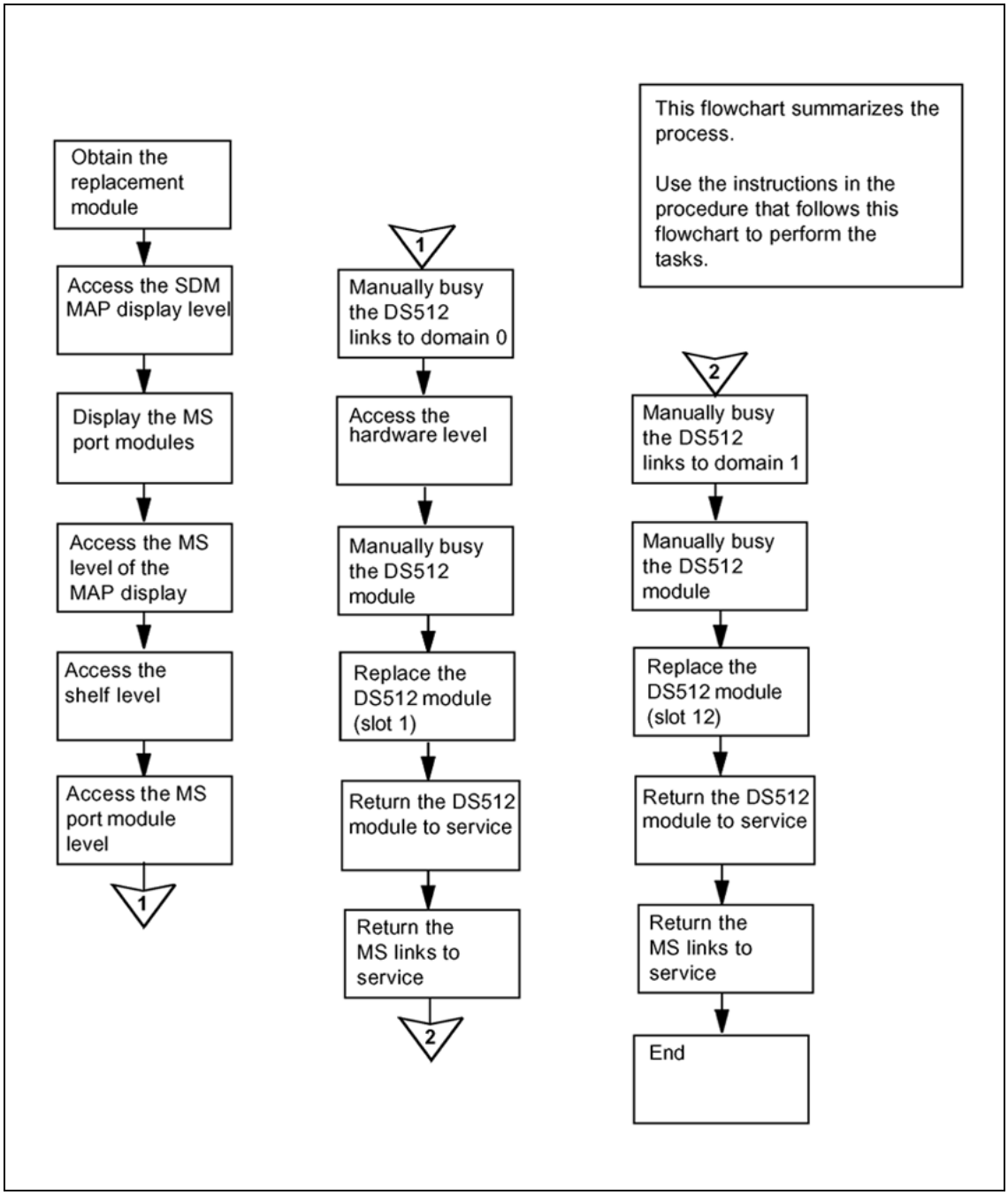
Before you begin this procedure, you must have available:

- two NTRX50GX controller modules
- packaging material in which to return the two NTRX50GA controller modules
- login capability for both the DMS MAP and CS 2000 Core Manager

Task flow diagram

The following task flow diagram provides a summary of the process. To upgrade the DS512 controller module, use the instructions in the procedure that follows the flowchart.

Task flow for Upgrading the DS512 controller module from NTRX50GA to NTRX50GX



Upgrading the DS512 controller module

Step Action

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

1 Obtain an NTRX50GX DS512 controller module. Make sure that the upgrade module has the correct product engineering code (PEC). The PEC is printed on the top locking lever of the module.

At the MAP display

2 Access the SDM level:

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

3 Display the card numbers that provide the DS512 links to the CS 2000 Core Manager:

```
trnsl
```

Example response

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

4 Record the card number associated with the CS 2000 Core Manager DS512 links. The 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 of the MAP display:

```
ms
```

6 Access the shelf level:

```
shelf
```

7 Access the card number level that is associated with the CS 2000 Core Manager DS512 links:

```
chain <card_number>
```

where

<card_number> is the card number you recorded in step 4.

8 Manually busy the DS512 link between MS plane 0 and the CS 2000 Core Manager DS512 controller module or domain 0:

```
bsy 0 link 0
```

Example response:

```
Request to MAN BUSY MS:0 shelf:0 chain:15 link:0
submitted.
Request to MAN BUSY MS:0 shelf:0 chain:15 link:0passed.
```

The state for the DS512 link changes to M for MS plane 0.

9 Manually busy the DS512 link between MS plane 1 and the CS 2000 Core Manager DS512 controller module on domain 0:

```
bsy 1 link 0
```

Example response:

```
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link: 0 passed.
```

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 a user authorized to perform config-admin actions.

11 Access the maintenance interface:

```
sdmmtc
```

12 Access the hardware (Hw) level:

```
hw
```

13 Busy the DS512 controller module:

```
bsy 0 512
```

If you are	Do
prompted to confirm the busy command	step 14
not prompted to confirm the busy command	step 16

14 Confirm the busy command:

```
y
```

At the front of the CS 2000 Core Manager

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.

15 Wear an electrostatic discharge (ESD) grounding wrist strap.

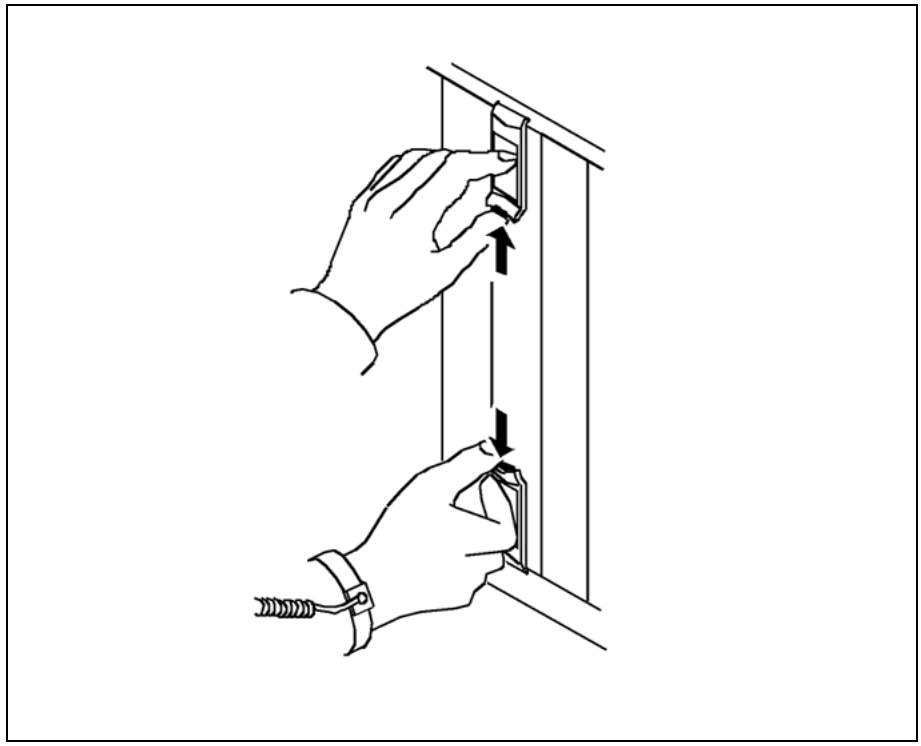
16 Locate the NTGX50GA card in slot 1.

17

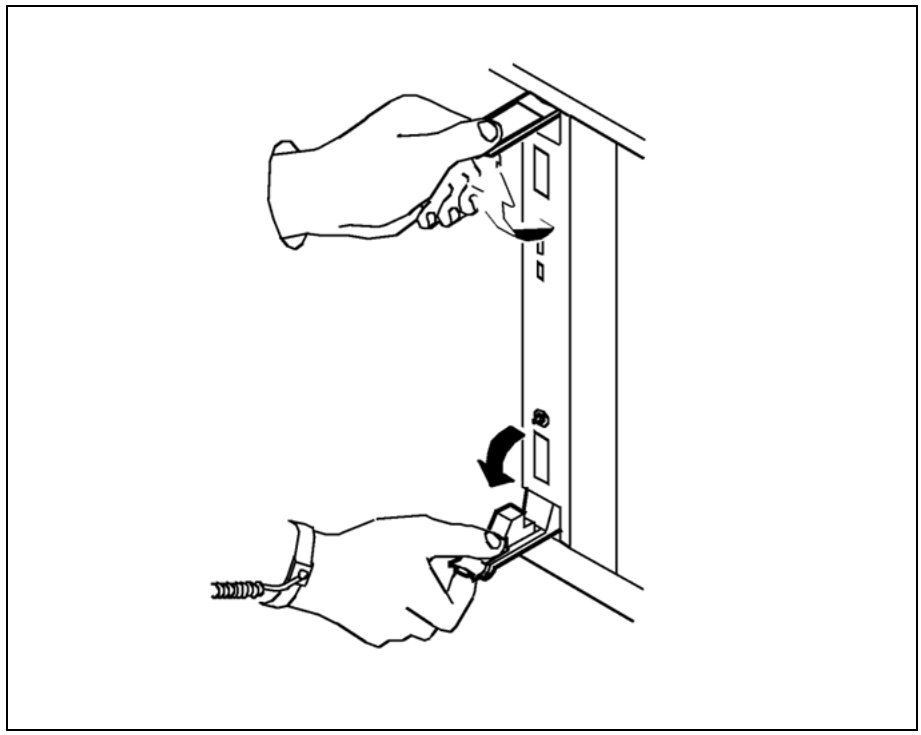
CAUTION
Potential service interruption
Unseat only the DS512 controller module that you busied, and not the corresponding DS512 controller module in the other I/O domain. The in-service LED on the busied module is off, and the out-of-service LED is on (red). If you remove the remaining in-service DS512 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. The thumbscrews are the captive type, and cannot be removed from the module.

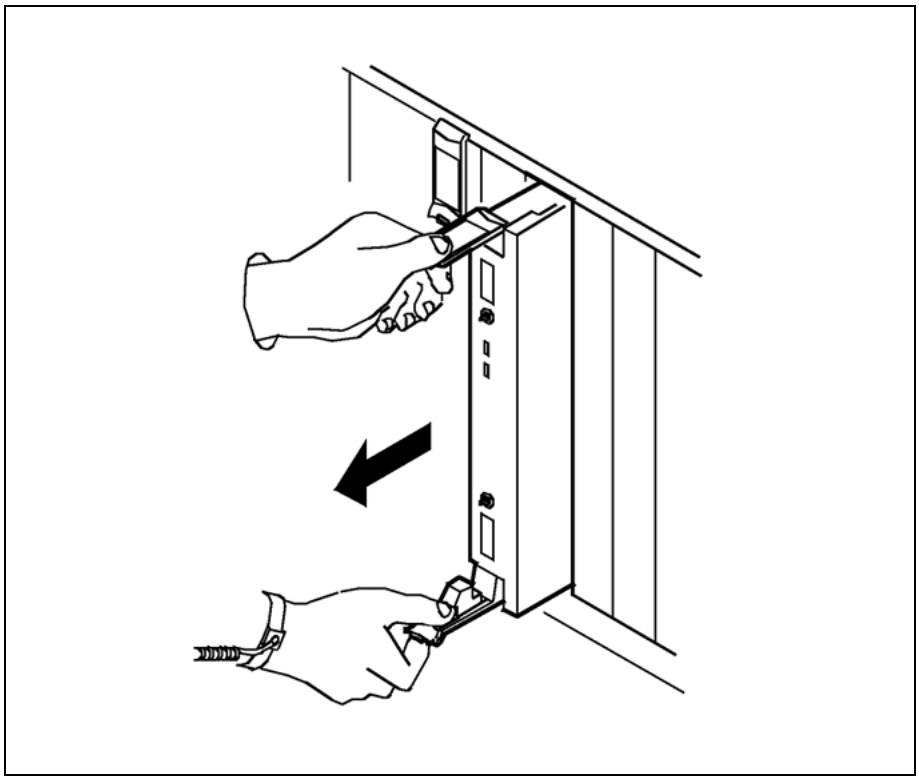
18 Depress the tips of the locking levers on the face of the DS512 controller module.



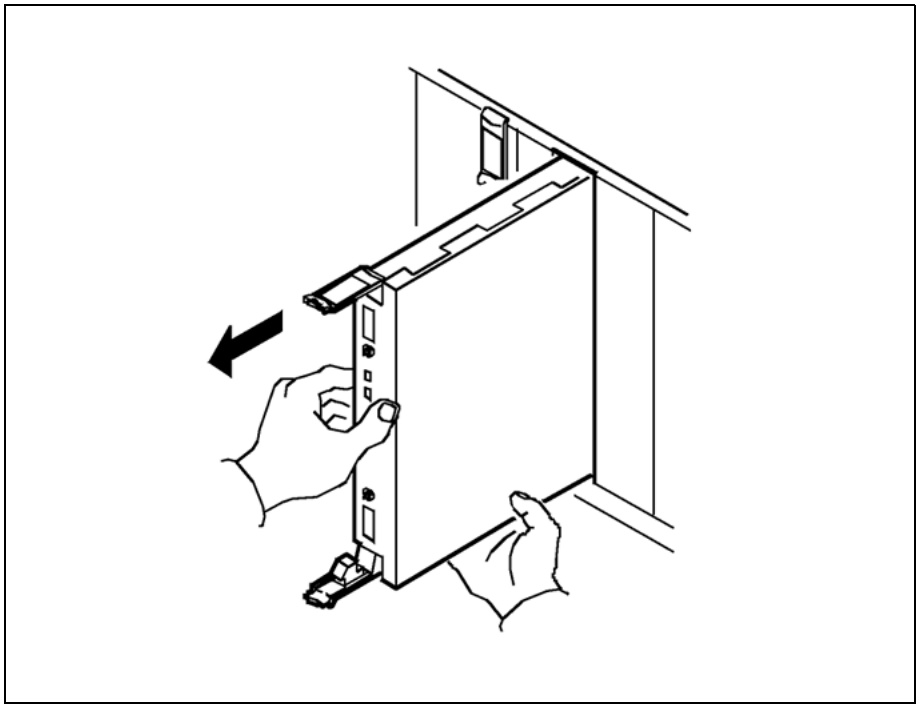
19 Open the locking levers on the face of the module by moving the levers outwards.



20 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5 cm) from the CS 2000 Core Manager shelf.



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



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

At the local or remote VT100 console

23 Exit the maintenance interface:

```
quit all
```

24 For the DS512 module you have removed, delete the information from the CS 2000 Core Manager configuration database:

```
ftds512clean <n>
```

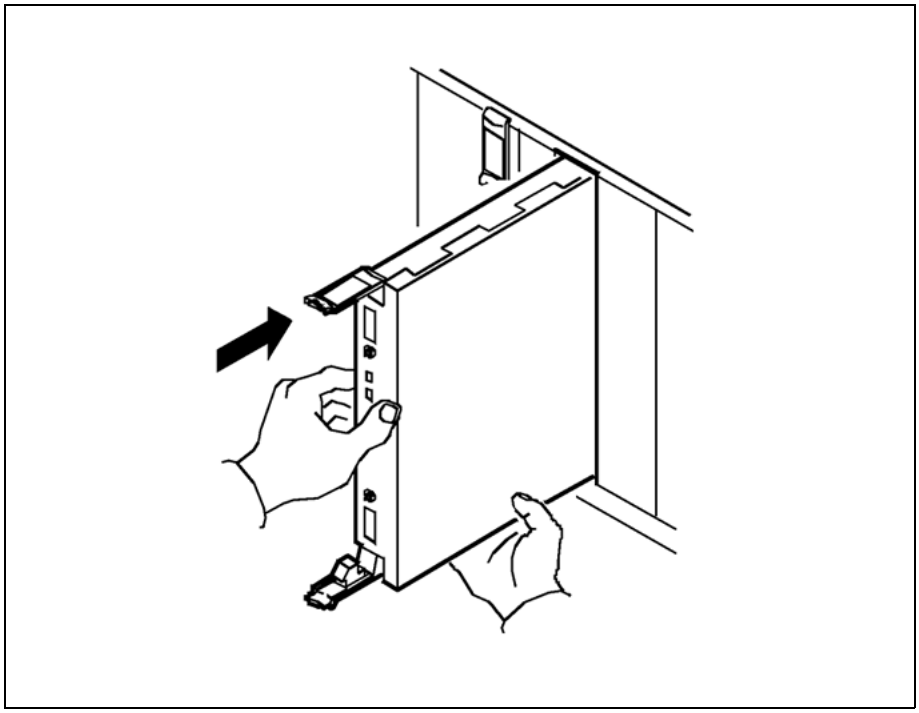
where

`<n>` is 0 if the removed module was in domain 0, and 1 for a module that was in domain 1.

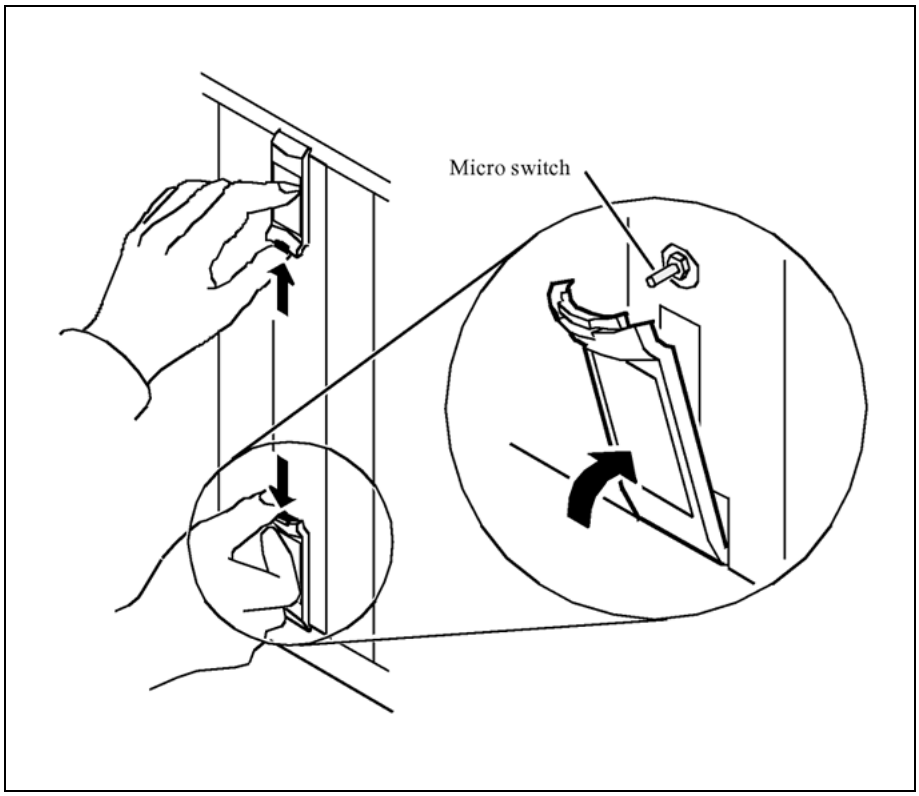
At the front of the CS 2000 Core Manager

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

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



27 To seat the module properly, make sure that both the top and bottom micro switches are lined up with the levers. Close the locking levers to secure the module.



28 Tighten the thumbscrews (if present) on the module.

29 Use the following table to determine your next step.

If	Do
you are replacing domain 0	step 30
you are replacing domain 1	step 42

At the local or remote VT100 console

30 Access the maintenance interface:

```
sdmmtc
```

31 Access the hardware (Hw) level:

```
hw
```

32 Return the DS512 controller module to service:

```
rts 0 512
```

Example response:

```
Hardware RTS : Domain 0 Device 512 - Command initiated.
Please wait...
```

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

Example response:

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

At the hardware menu level of the CS 2000 Core Manager maintenance interface, the state of the DS512 controller module changes to the in-service dot (.). The in-service LED on the DS512 controller module is on (green).

At the MAP display

33 Access the MS port module 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:

```
rts 0 link 0
```

Example response:

```
Request to RTS MS: 0 shelf: 0 chain:15
link:  0 submitted.
Request to RTS MS: 0 shelf: 0 chain:15 link: 0 passed.
```

The state for the DS512 link changes to the in-service dot (.) if the CS 2000 Core Manager DS512 link is in service. Otherwise, the state for the DS512 link changes to P.

34 Return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
rts 1 link 0
```

Example response:

```
Request to RTS MS: 1 shelf: 0 chain:15
link:  1 submitted.
Request to RTS MS: 1 shelf: 0 chain:15 link: 1 passed.
```

The state for the DS512 link changes to the in-service dot (.) if the CS 2000 Core Manager DS512 link is in service. Otherwise, the state for the DS512 link changes to P.

35 You can now replace the second NTRX50GA module with the second NTRX50GX module. Busy the DS512 link between MS plane 0 and the CS 2000 Core Manager DS512 controller module you wish to replace:

```
bsy 0 link 1
```

Example response

```
Request to MAN BUSY MS: 0 shelf: 0 chain:15
link:  0 submitted.
Request to MAN BUSY MS: 0 shelf: 0 chain:15
link: 0 passed.
```

The state for the DS512 link changes to M for MS plane 0.

36 Busy the DS512 link between MS plane 1 and the CS 2000 Core Manager DS512 controller module you wish to replace:

```
bsy 1 link 1
```

Example response:

```
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 0 chain:15
link: 0 passed.
```

The state for the DS512 link changes to M for MS plane 1.

At the local or remote VT100 console

37 Busy the DS512 controller module:

```
bsy 0 512
```

If you are	Do
prompted to confirm the busy command	step 38
not prompted to confirm the busy command	step 40

38 Confirm the busy command:

```
y
```

At the front of the CS 2000 Core Manager

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.

39 Wear an electrostatic discharge (ESD) grounding wrist strap.

40 Locate the NTRX50GA card in slot 12.

41 Replace the NTRX50GA module in slot 12 with the NTRX50GX module. To replace the module in slot 12, use steps 17 to 28, then continue with step 42.

At the local or remote VT100 console

42 At the hardware level, return the DS512 controller module to service:

```
rts 1 512
```

Example response:

```
Hardware RTS : Domain 1 Device 512 - Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 1 Device 512 - Command complete.
```

At the hardware level, the state of the DS512 controller module changes to the in-service dot (.). The in-service LED on the DS512 controller module is on (green).

At the MAP display

43 Access the MS port module level of the MAP display (accessed in step 7).

44 Return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
rts 0 link 1
```

Example response:

```
Request to RTS MS: 0 shelf: 0 chain:15
link:  0 submitted.
Request to RTS MS: 0 shelf: 0 chain:15 link: 0 passed.
```

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.

45 Return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced:

```
rts 1 link 1
```

Example response:

```
Request to RTS MS: 1 shelf: 0 chain:15
link:  1 submitted.
Request to RTS MS: 1 shelf: 0 chain:15 link: 1 passed.
```

The state for the DS512 link changes to the in-service dot (.) if the CS 2000 Core Manager DS512 link is in service. Otherwise, the state for DS512 link changes to a P.

At the local or remote VT100 console

46 Exit the maintenance interface:

```
quit all
```

47 Confirm that the new cards are properly installed:

```
locate
```

The system displays a list of CS 2000 Core Manager hardware. The NTRX50GX module is the hardware in slots 1 and 12.

If the system does not list the NTRX50GX modules, the card(s) may be faulty. Replace the NTRX50GX DS512 controller modules with the original NTRX50GA modules. To replace the modules, return to step 13 of this procedure and reinstall the NTRX50GA DS512 controller modules.

At the MAP display

48 Exit the MAP session:

```
quit all
```

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

—End—

Carrier VoIP

CS2000 Core Manager Configuration Management

Publication: NN10104-511
Document status: Standard
Document version: 08.04
Document date: 20 October 2006

To provide feedback or report a problem in this document , go to **http://www.nortel.com/documentfeedback**

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