CS 2000 Core Manager Configuration Management

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

Features changes

There are no feature changes in this release.

Other changes

There are no other changes in this release.

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

The CS 2000 Core Manager and Multiservice Data Manager (MDM) 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

```
  SDM      CON     512     NET     APPL    SYS      HW     CLLI: SNM0
  ISTb      •      . .     ISTb    ISTb    ISTb    ISTb    Host: wcary2p3
   M             . .                      M       M            Fault Tolerant
SDMConfig
 0  Quit
 2  Add          #   Commissioning Step       Status / Value
 3  Change       1   Passwords                Commissioned
 4  Delete       2   Login Greeting           wcary2p3 Console
 5               3   Time Zone                Eastern U.S.: Colombia <Cut -5>
 6  Next         4   Date & Time              Thu Aug 29, 2002 13:42:05
 7  Prev         5   Hostname                 wcary2p3
 8               6   CLLI and Location Code   SNM0: 1 A 2 3
 9  List         7   Network Security         Commissioned
 10 Step         8   Ethernet Connectivity    Commissioned
 11              9   DS512 Connectivity       Commissioned
 12 Up           10  X25 Connectivity         Uncommissioned
 13 Down         11  Gateway IP Address       47.135.213.1
 14              12  Core Communication Path  Commissioned
 15                                  Commissioning Steps: 1 to 12 of 17
 16
 17 Help      Use Up or Down to scroll through the list, and the Step #
 18 Refresh   command to go to a particular commissioning step.

 Time 13:42  >
```

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 on page 4.

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)

Command options for commissioning a component

If you want to	Enter
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
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

Commissioning procedures

Component	Procedure	Document
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”	Upgrades
	“Decommissioning X.25 ports [on UMFIO or SYNC module]”	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 MDM for fault data)

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

Prerequisites

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

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

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 MDM.

3 Obtain the port number for the pserver application on each of the 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 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 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 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 MDM filters defined.
Do you want to specify MDM filters? [y/n]
```

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

f When prompted, enter the host name of the first 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...
```

12

ATTENTION

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

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.

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 core manager port number)
- a file device (a file on the 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 on page 22.
- delete an existing device, refer to the procedure Deleting a device using logroute on page 29.
- modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters on page 84.

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

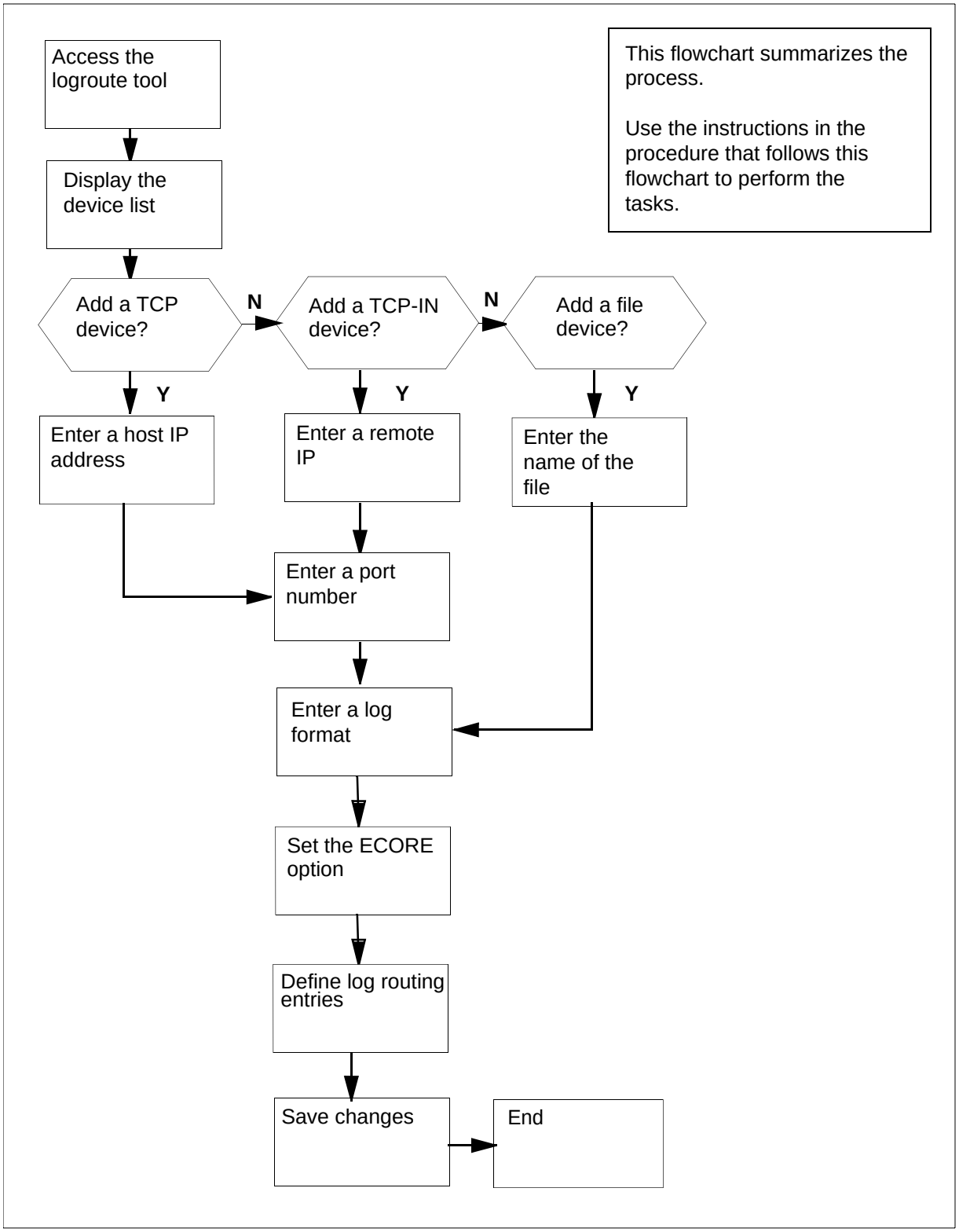
Logging on to the Core and Billing Manager 850

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

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



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 log delivery destinations

At any workstation or console

1 Log into the core manager. Refer to Prerequisites on page 12 for details.

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 the 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).

Note 1: 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

Note 2: The default format is STD.

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

Note: 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

Note: 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 on page 77. 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.

Note 1: An example of a log type is “PM”. This entry will suppress or un-suppress all PM logs.

Note 2: 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.

Note 3: 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 ***Note:*** 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.

Note: 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.

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 on page 77. 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 on page 84.

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

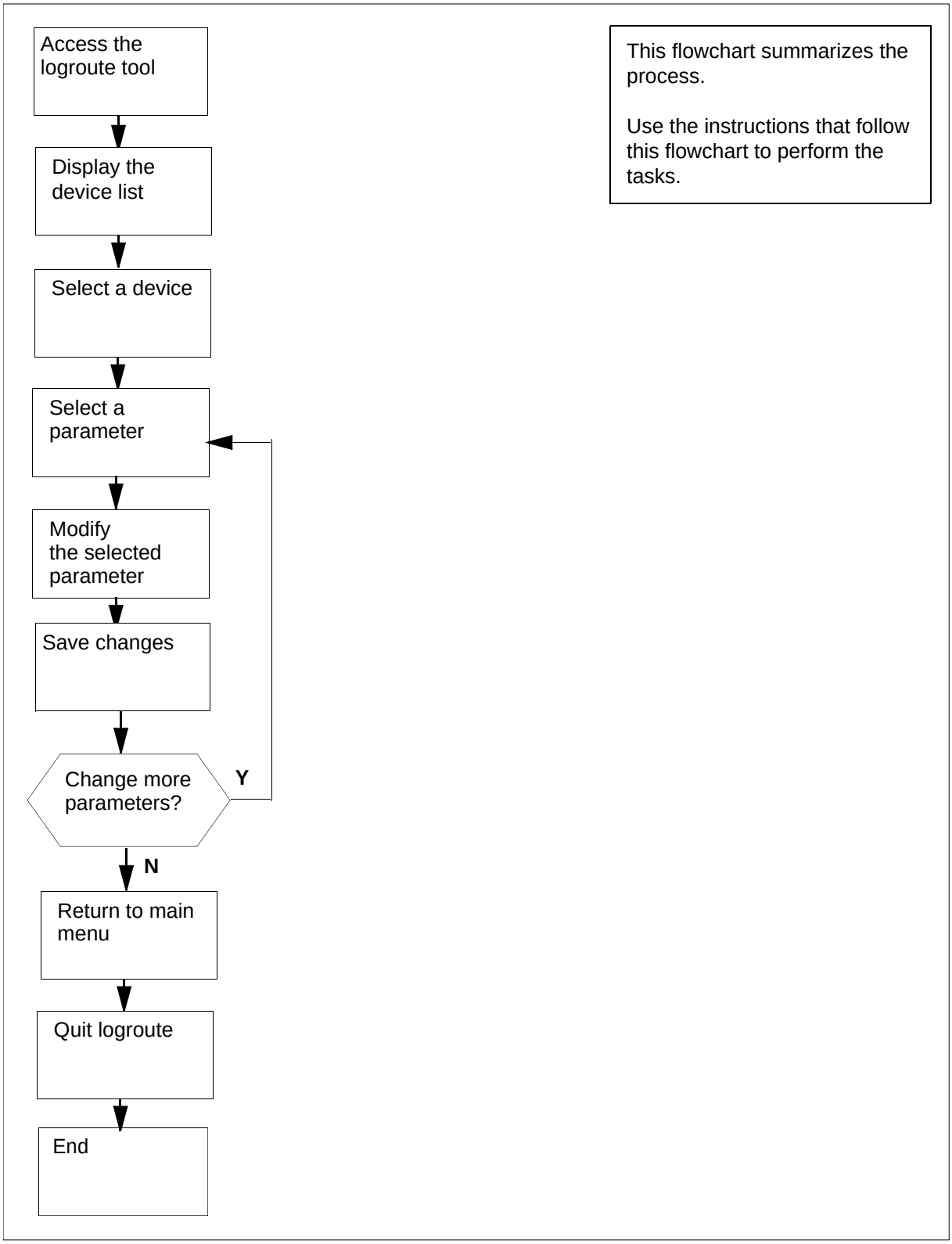
Logging on to the Core and Billing Manager 850

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

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



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

Modifying a log device using logroute

At the VT100 console

1 Log into the core manager. Refer to Prerequisites on page 22 for details.

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 example above):

```
                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).

Note: 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).

Note: 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.

Note: 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.

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

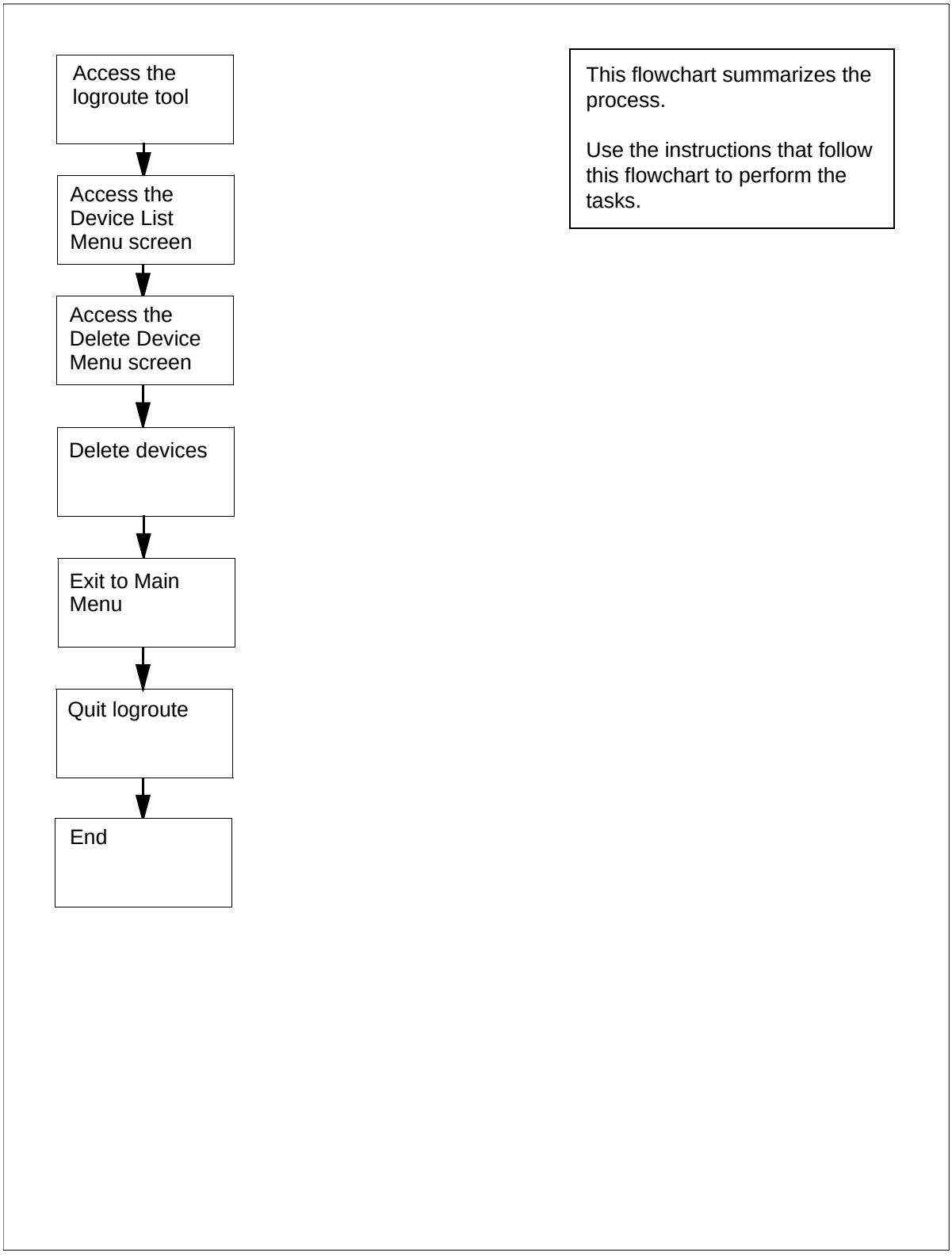
Logging on to the Core and Billing Manager 850

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

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



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 device using logroute

At the VT100 console

1 Log into the core manager. Refer to Prerequisites on page 29 for details.

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 ==>
```

Note: 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
```

Note: 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.

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

Logging on to the Core and Billing Manager 850

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

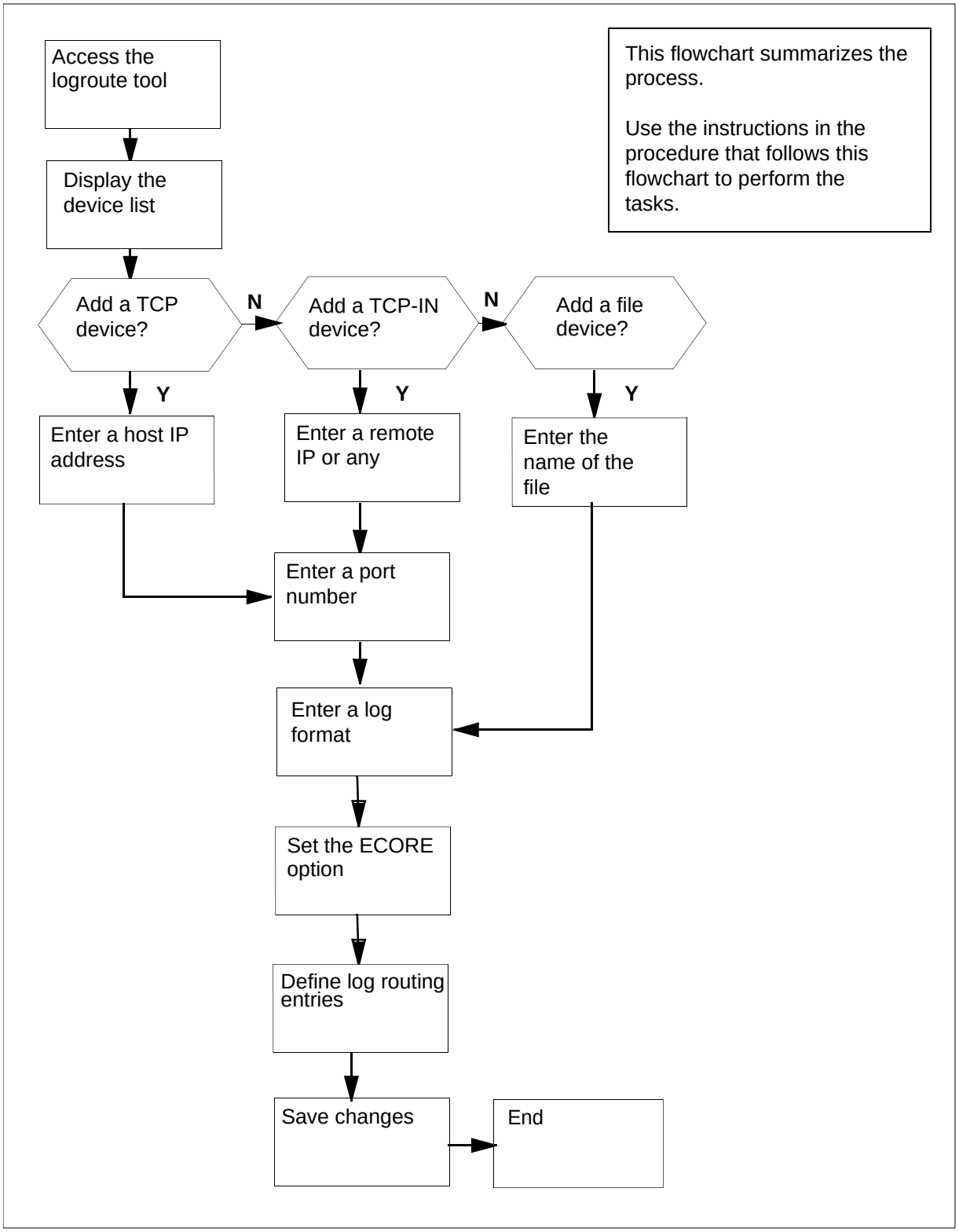
System requirements

The Passport Log Streamer application should be configured on the core manager to retrieve logs from the MDM. To configure the Passport 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*. To configure the Passport Log Streamer application on the Core and Billing Manager 850, use the procedure Installing optional software on a CBM 850 in *Upgrading the Core and Billing Manager 850*, NN10347-461.

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



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

At any workstation or console

1 Log into the core manager. Refer to Prerequisites on page 34 for details.

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.

Note: 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.

Note: 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.

Note: 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.

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

Logging on to the Core and Billing Manager 850

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

System requirements

The Passport Log Streamer application should be configured on the core manager to retrieve logs from the MDM. To configure the Passport 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*. To configure the Passport Log Streamer application on the Core and Billing Manager 850, use the procedure Installing optional software on a CBM 850 in *Upgrading the Core and Billing Manager 850*, NN10347-461.

Procedure

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

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.

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

At the VT100 console

1 Log into the core manager. Refer to Prerequisites on page 57 for details.

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.

Note: 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 File
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 File
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 File
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 File
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 File
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.

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

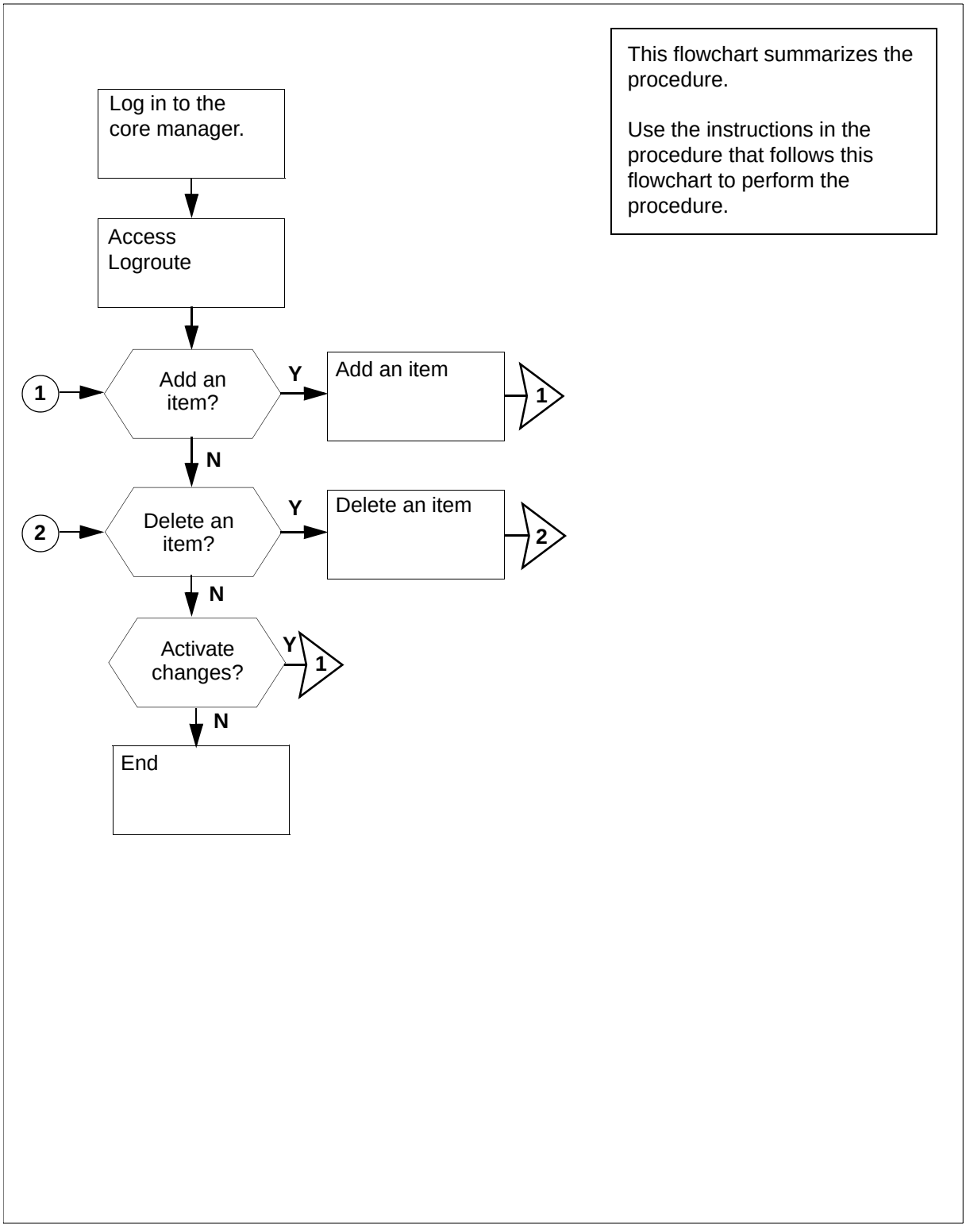
Logging on to the Core and Billing Manager 850

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

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



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

Specifying the logs delivered from the CM to the core manager

At the VT100 console

1 Log into the core manager. Refer to Prerequisites on page 77 for details.

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

Note: 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).

Note 1: An example of a log type is “PM”. This entry will suppress or un-suppress all PM logs.

Note 2: 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.

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.

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

- Configuring log delivery destinations on page 12
- Modifying a log device using logroute on page 22

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

- log_office_id (office name)

  Note: 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)

  Note: 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

Note: 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

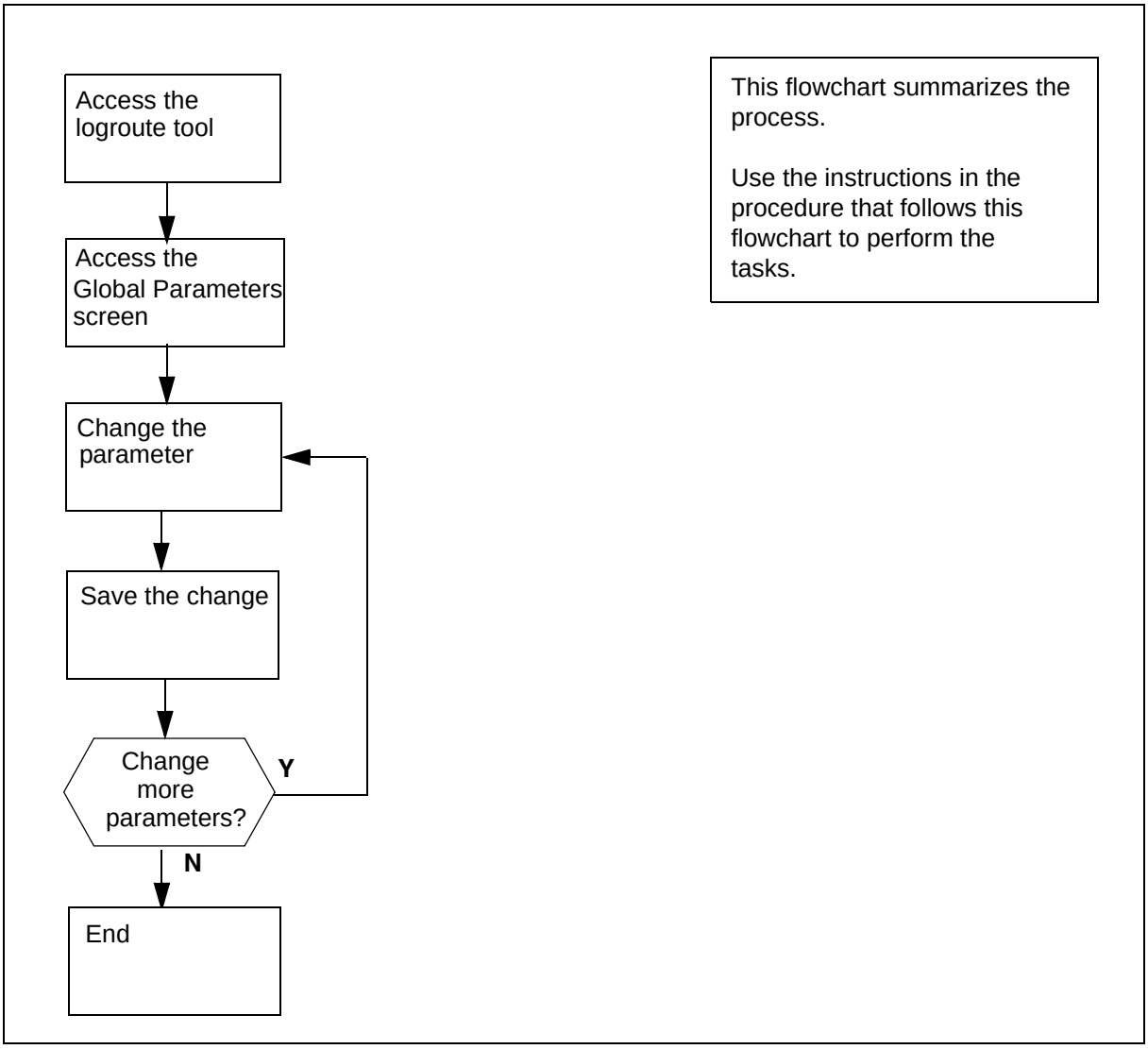
Logging on to the Core and Billing Manager 850

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

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



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 Log Delivery global parameters

At the VT100 console

1 Log into the core manager. Refer to Prerequisites on page 86 for details

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 ==>
```

Note: 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) ==>
```

Note 1: 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.

Note 2: 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.

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.

Note 1: For the Core and Billing Manager, you will need to resize the GDD volume (/cbmdata/00/gdd) based on the following engineering rules:

- for an End-Office: 220 MBytes/day * #RetentionDay.
- for a Tandem PT-IP Office: 100 Mbytes/day * #RetentionDay.
- For the installations specified above you will also need to resize the data volume (/cbmdata/00) using these rules if a file device is configured to capture all the logs and the global parameter "Maximum Size action" has been set to ROTATE.

Note 2: 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

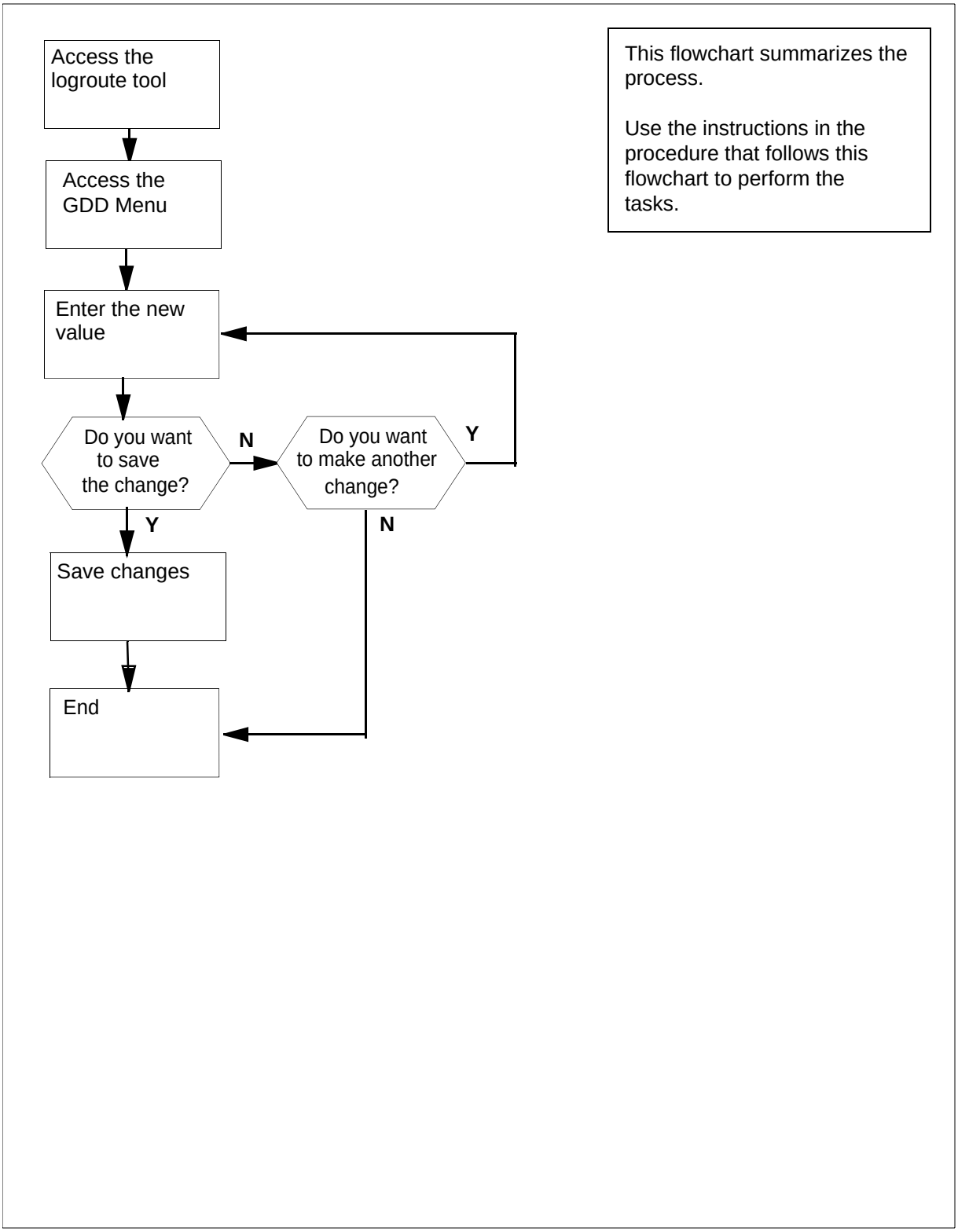
Logging on to the Core and Billing Manager

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

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



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 GDD parameter using logroute

At the VT100 console

1 Log into the core manager. Refer to Prerequisites on page 91 for details.

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.

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.

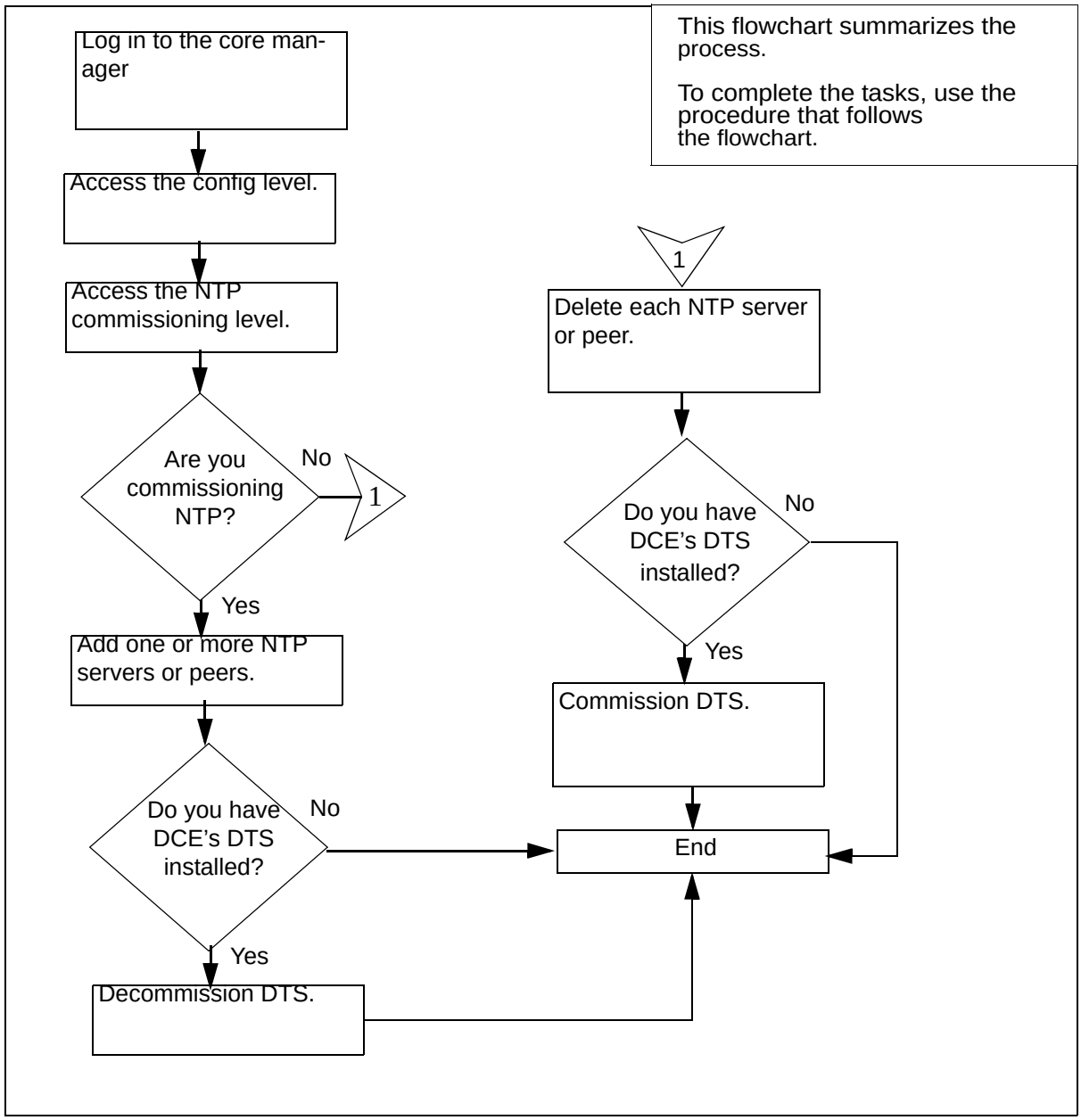
Prerequisites

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

At the local VT100 console

1 Log into the core manager. Refer to Prerequisites on page 98 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.

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.

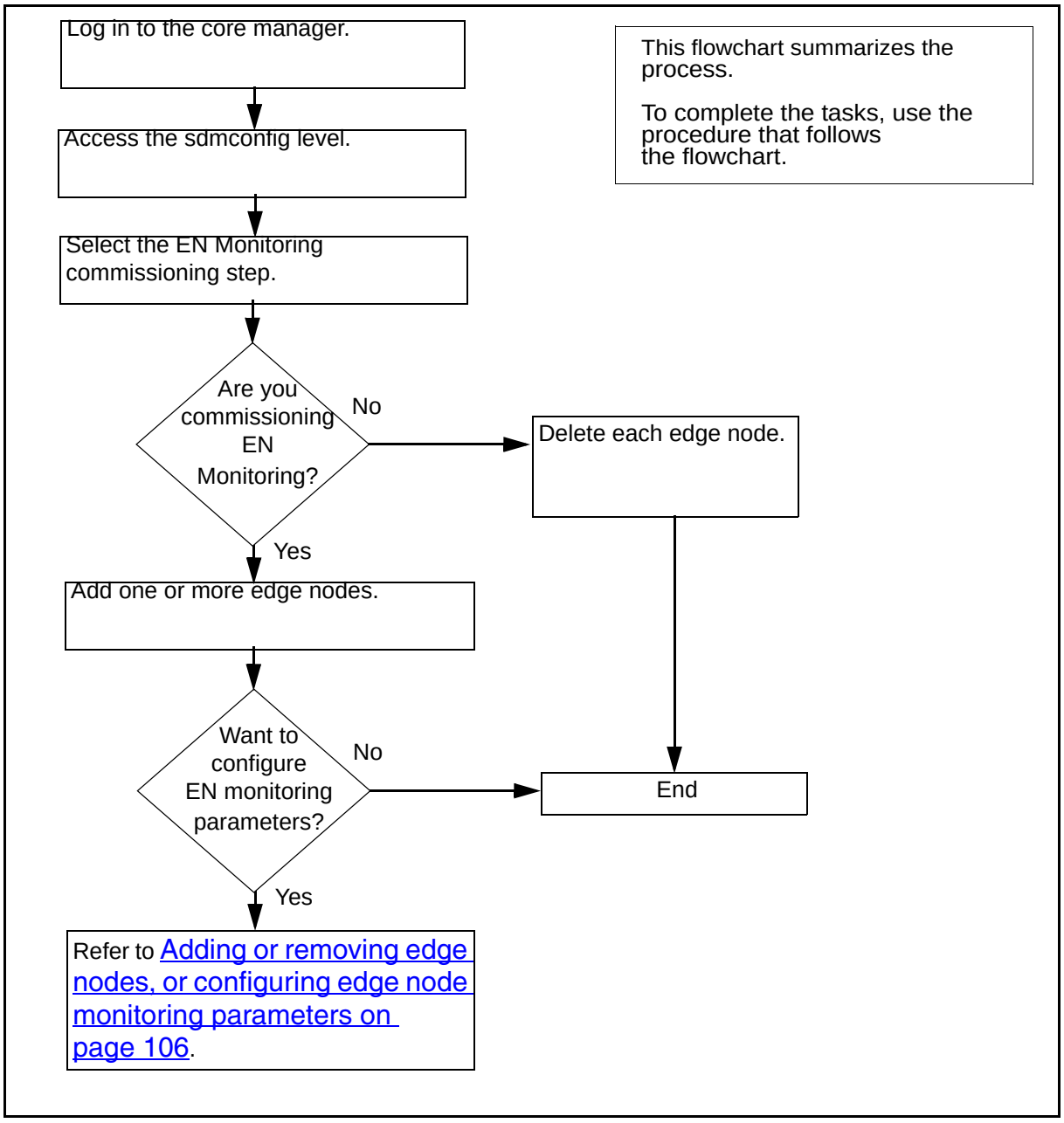
Procedures related to this procedure

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

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 on page 106
do neither of the above actions	you have completed this procedure

Decommissioning edge node monitoring

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

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.

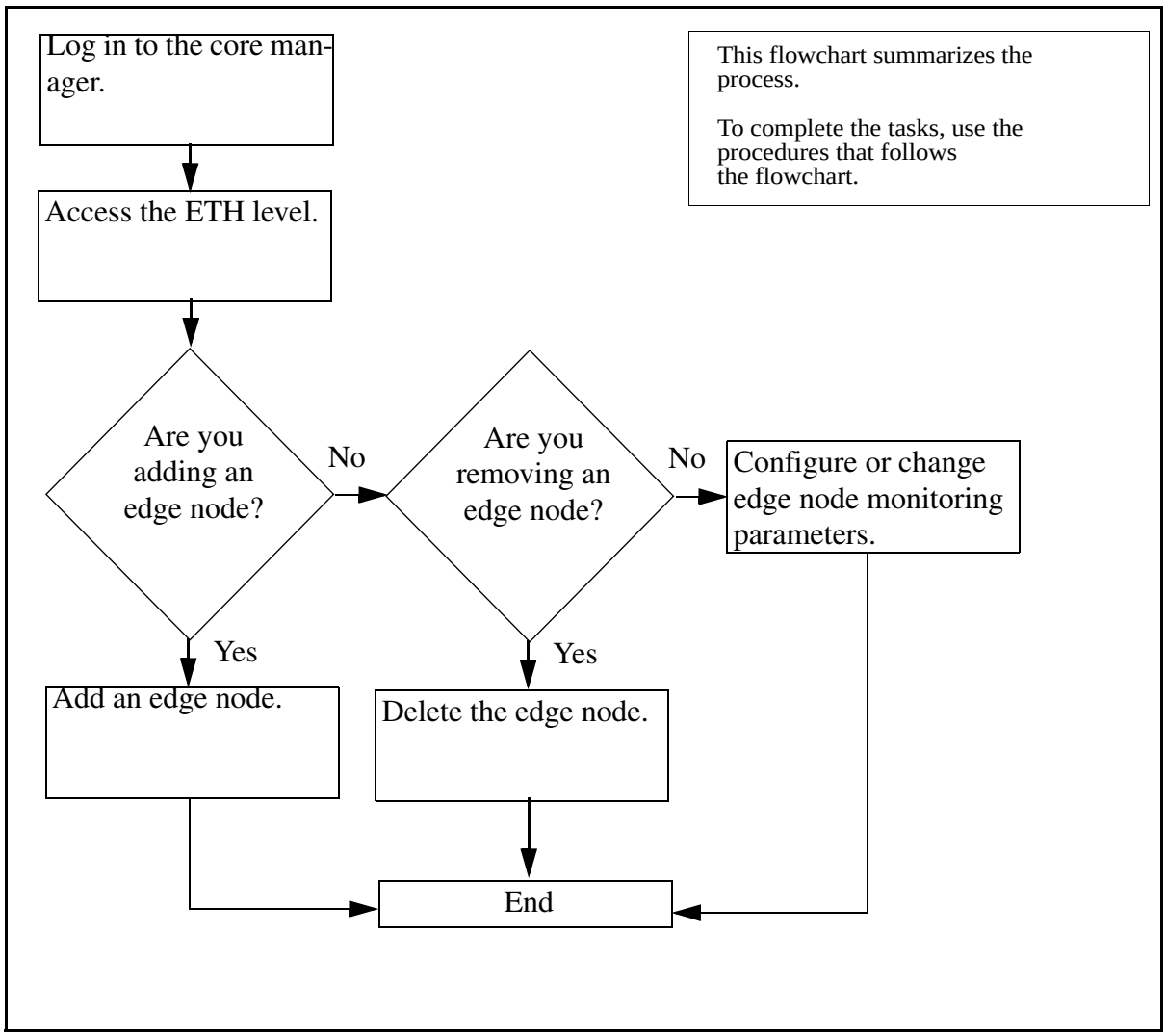
Procedures related to this procedure

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

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 on page 110
do neither of the above actions	you have completed this procedure

Removing an edge node

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

Configuring or changing edge node parameters

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

Adding or removing an NTP server or peer

Purpose

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

Note 1: You can add up to three NTP servers or peers.

Note 2: 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

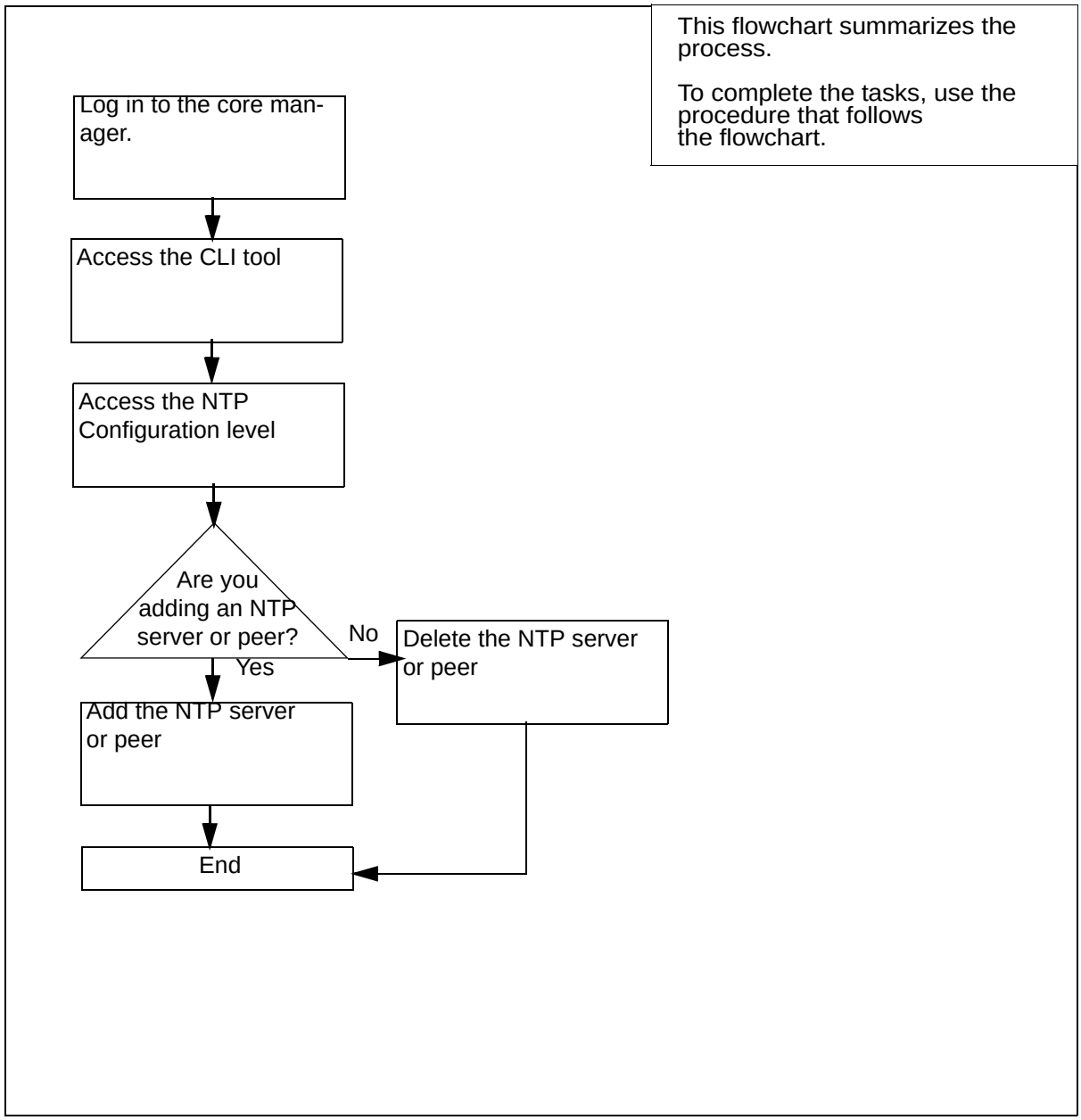
Logging on to the Core and Billing Manager 850

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

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



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

Adding or removing an NTP server or peer

At the local VT100 console

1 Log into the core manager. Refer to Prerequisites on page 112 for details.

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**

Note 1: 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.

Note 2: A peer can act as a server.

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

Note: Please don't use the IP address as an NTP host name (tag or alias).

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.

Note: 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.

```
sdmcbmmtc ntp
```

16 You have completed this procedure.

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).

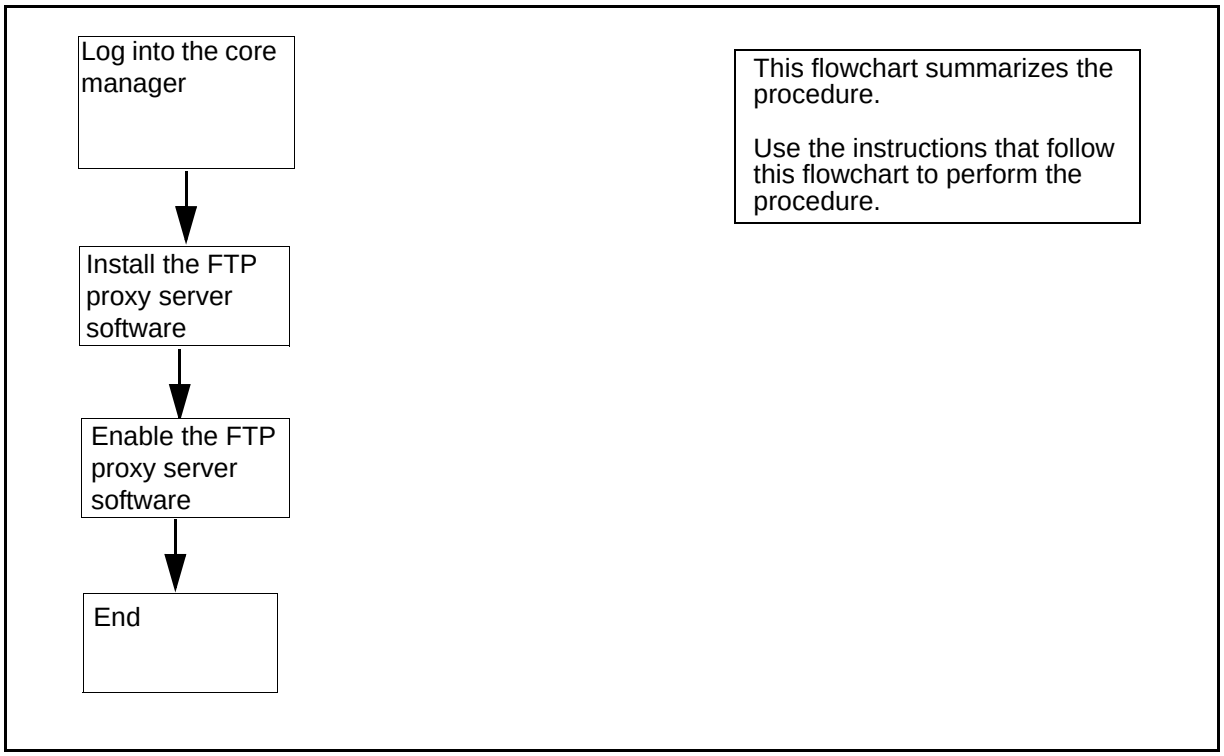
ATTENTION
Before you can perform an installation using SWIM, you must have the core manager base software installed on the core manager.

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

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.

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

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.

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

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
```

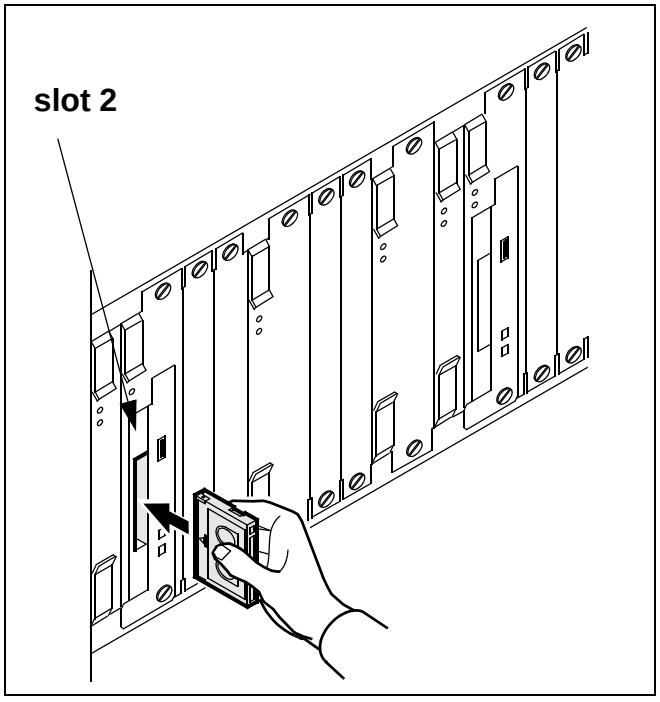
3 Access the SWIM level:

```
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 on page 125.

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

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.

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 Installing the ETA application server software on the core manager on page 122.

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

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.

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 on page 137.

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.

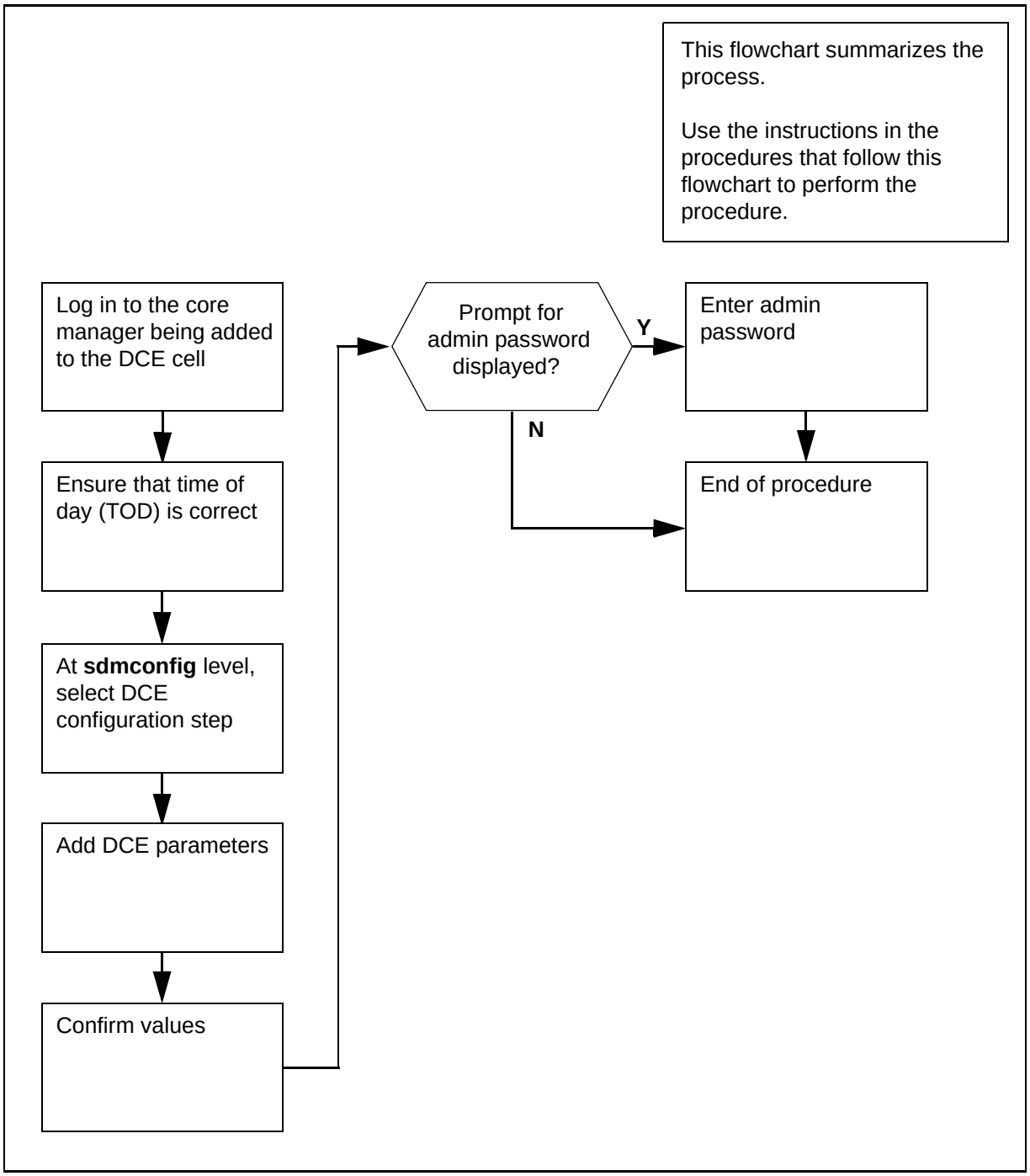
Note 1: You cannot commission DCE until after you have commissioned the LAN. If you try to commission DCE before commissioning the LAN, the system displays an error message. For information about LAN commissioning, refer to the procedure “Commissioning SDM-LAN connectivity”.

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

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

If you want to	Do
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.

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).

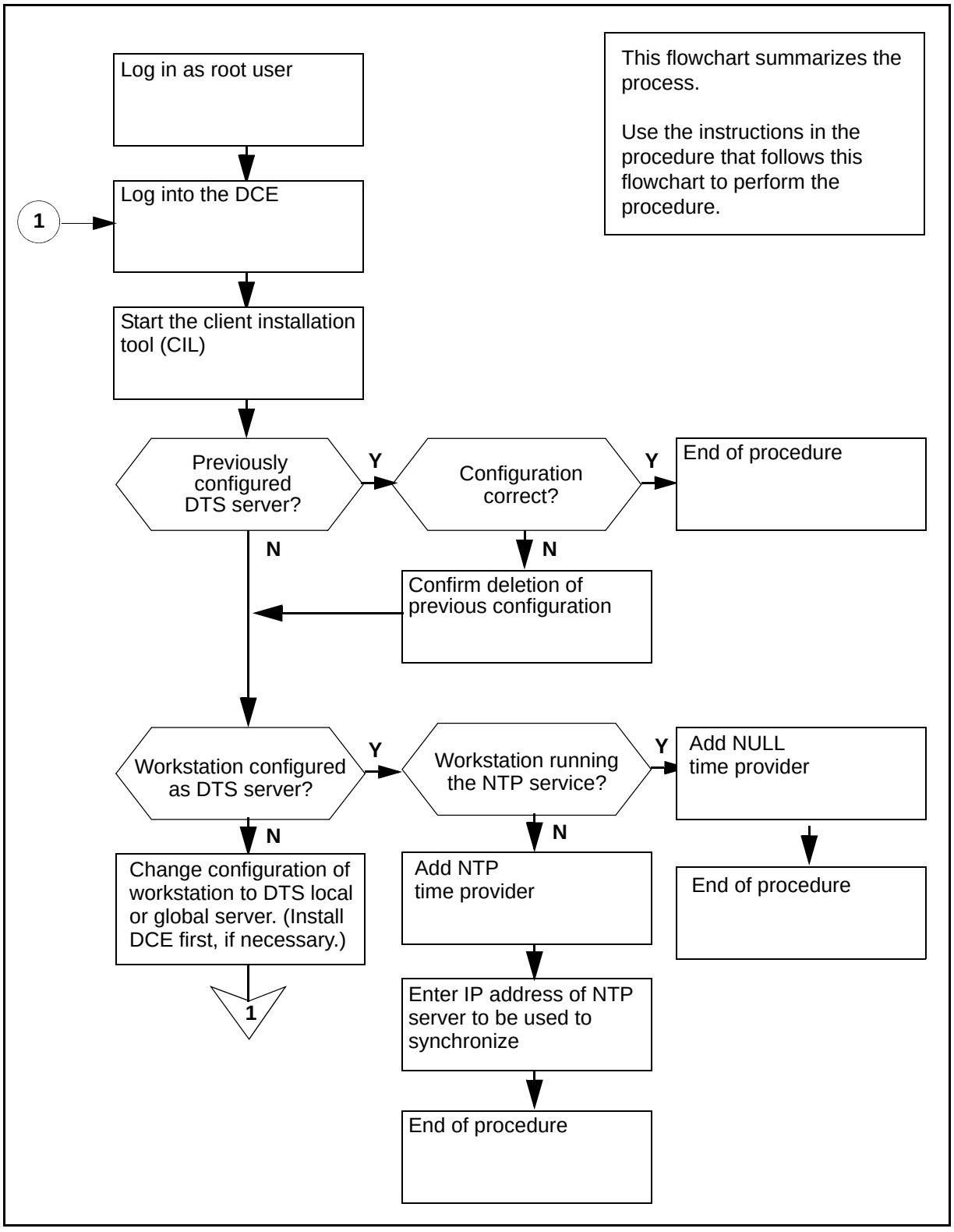
Prerequisites

Before performing this procedure, you must install the client installer and launcher (CIL). Refer to the procedure Installing CIL on a client workstation on page 178.

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

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
"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.

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

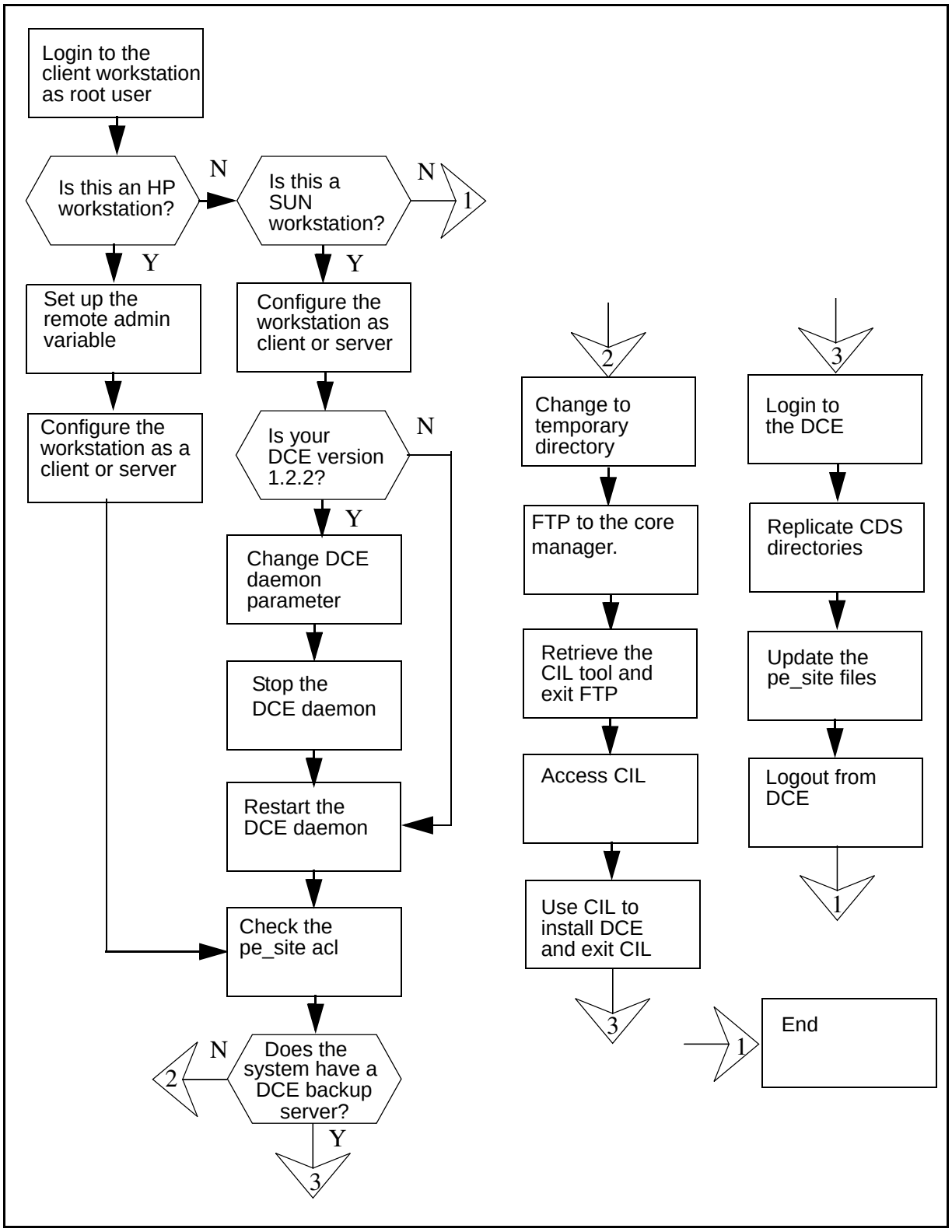
ATTENTION
This procedure can only be performed if your operating system is HP-UX or SunOS. If you are using a different operating system, do not attempt to perform this procedure.

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

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/dced-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.

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 on page 129.

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.

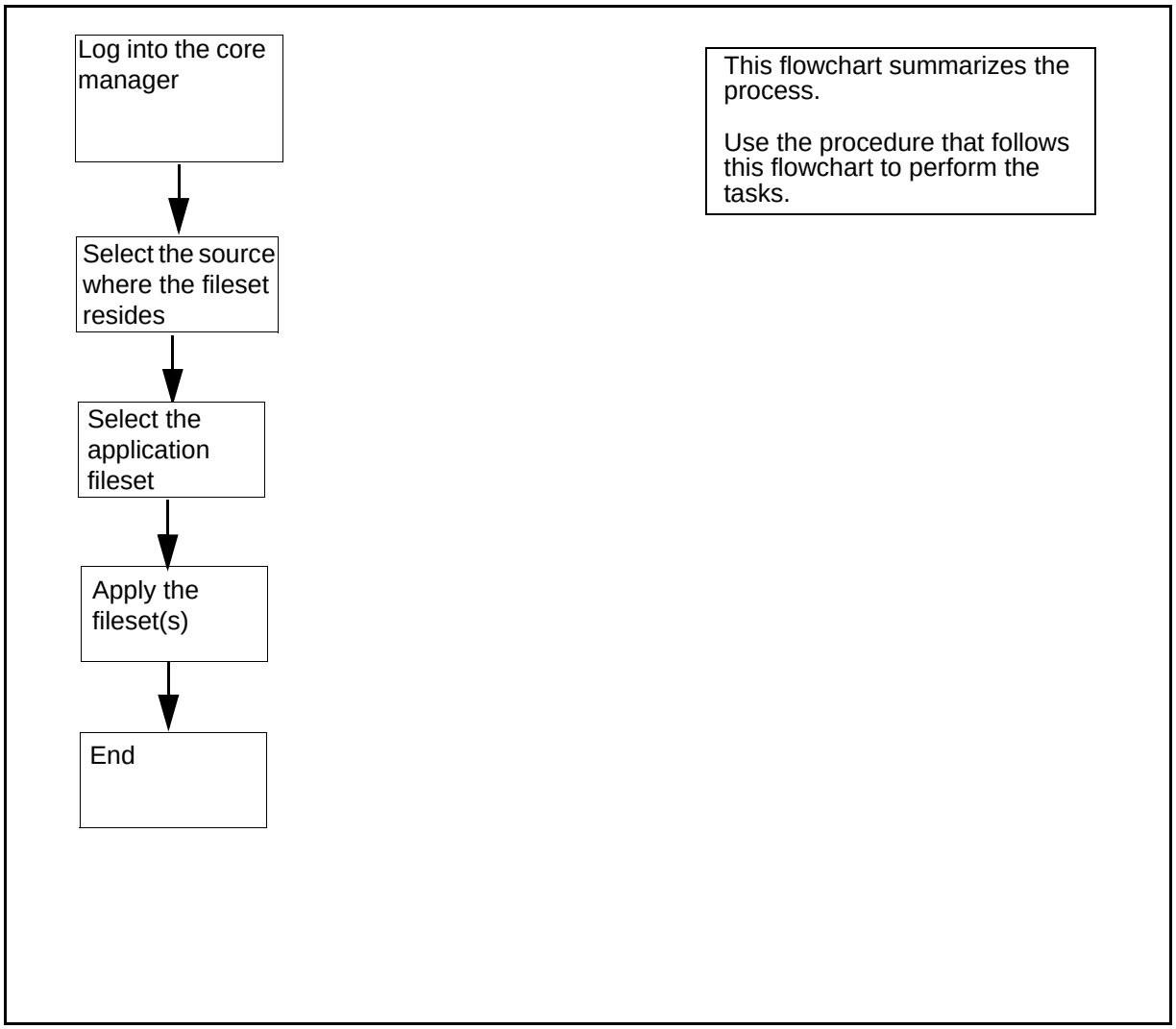
The sub-administrator account requires the following privileges:

- 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

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
```

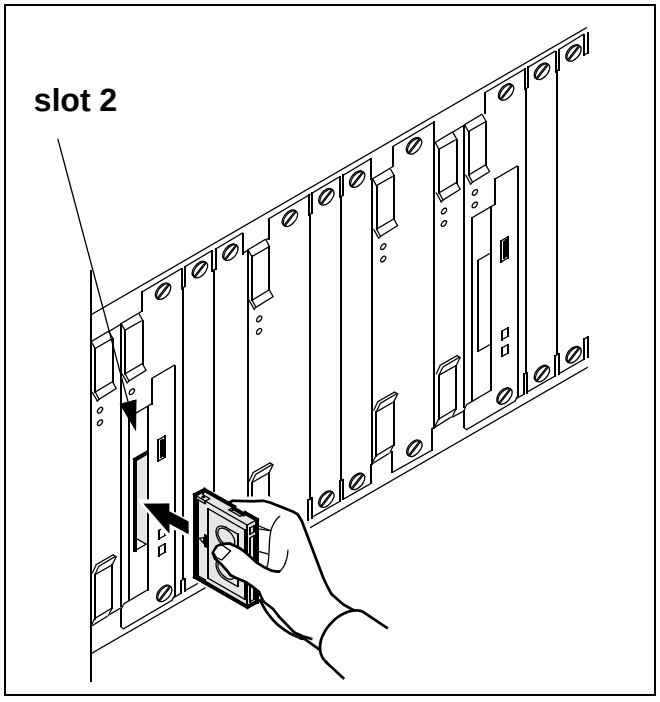
3 Access the SWIM level:

```
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.

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 on page 154.

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
`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.

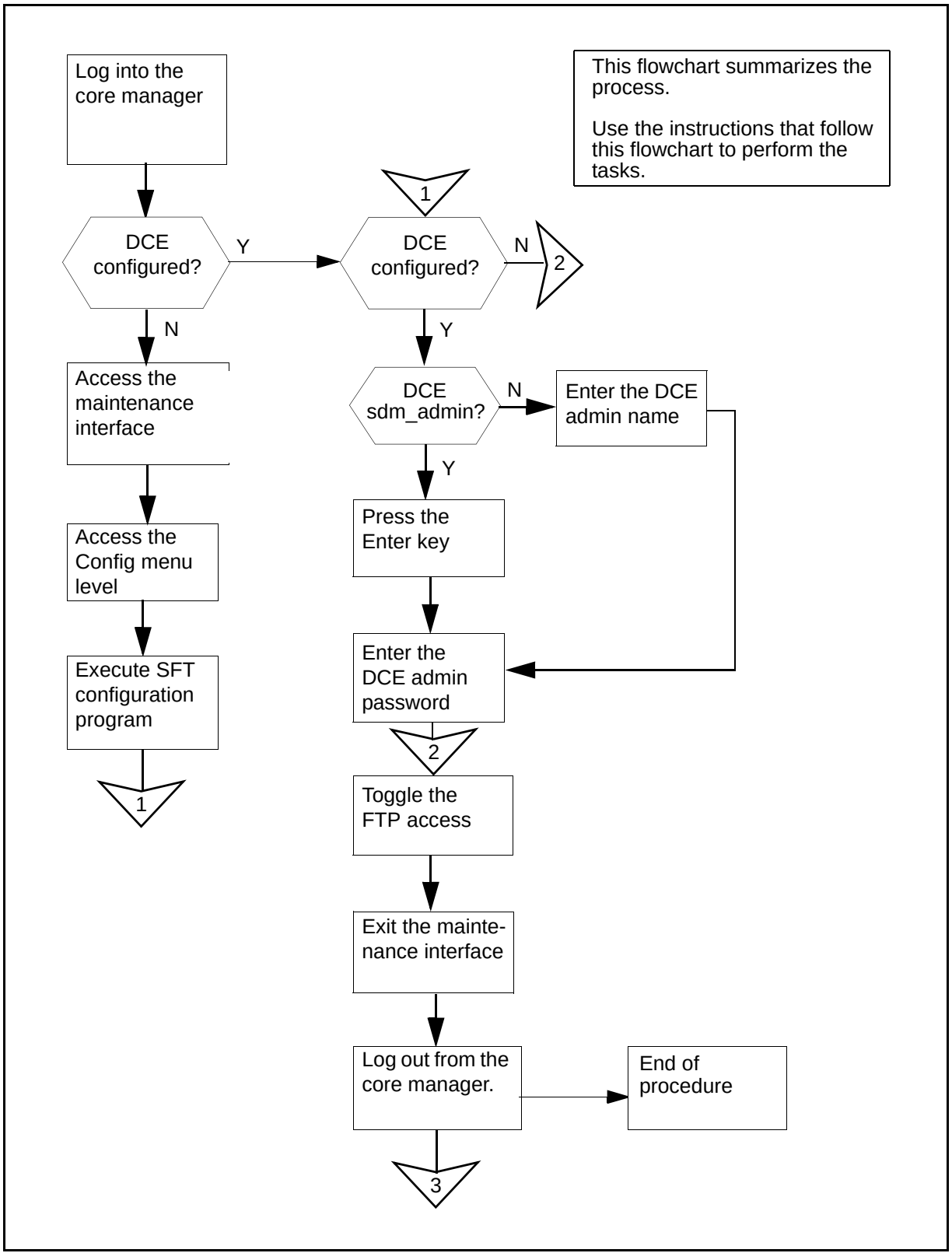
The sub-administrator account requires the following privileges:

- 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

At any workstation or console

1

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.

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.

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

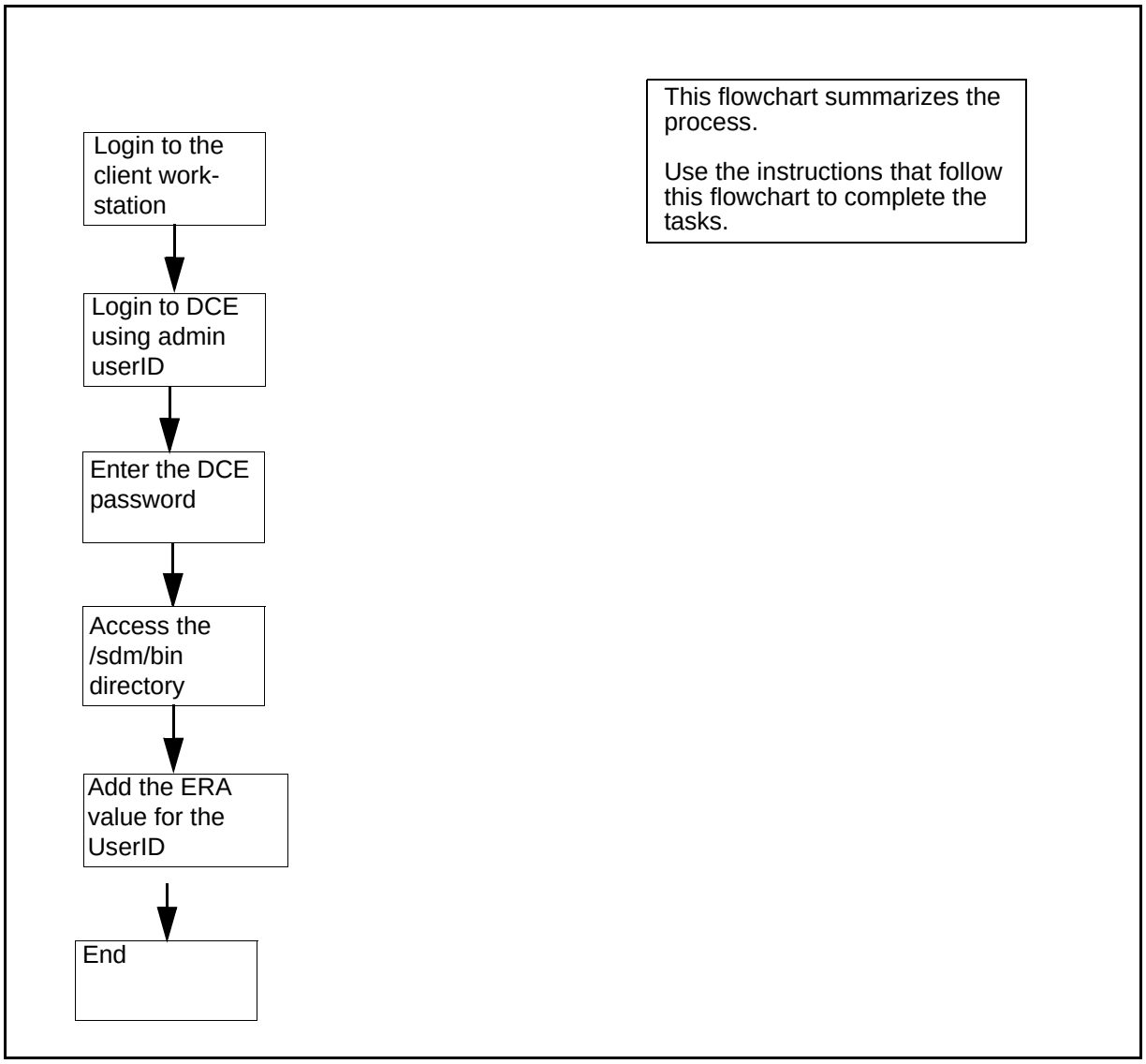
The DCE administrator must create and configure the DCE user accounts before a user can access the SFT servers using the SFT clients. If you are using SFT in FTP (non-DCE) mode, ignore this section.

Task flow diagrams

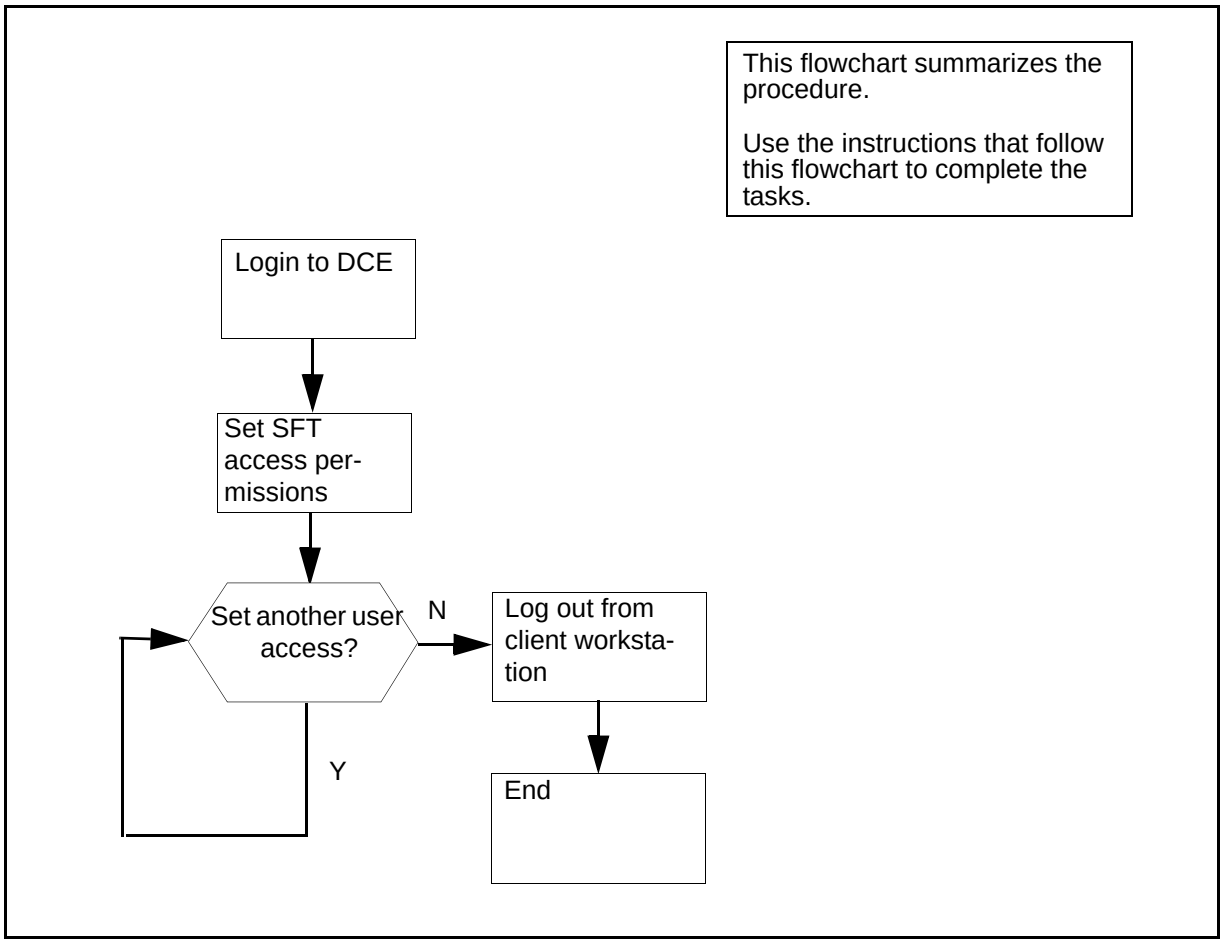
The following task flow diagrams summarize the process. Use the instructions in the procedures that follow the flow charts to complete the tasks.

- 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

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.

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

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

If you	Do
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.

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.

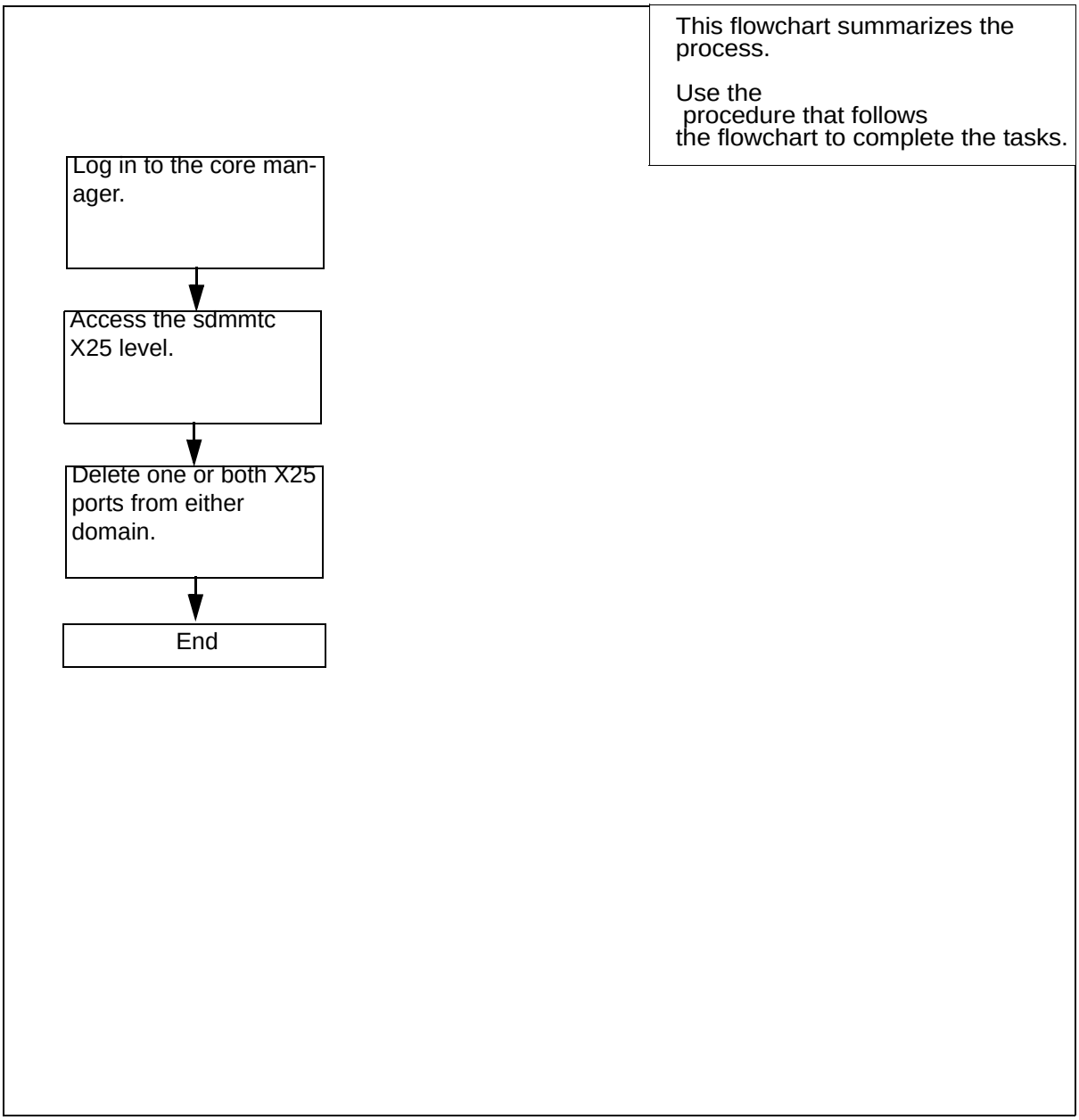
Procedures related to this procedure

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

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.

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:

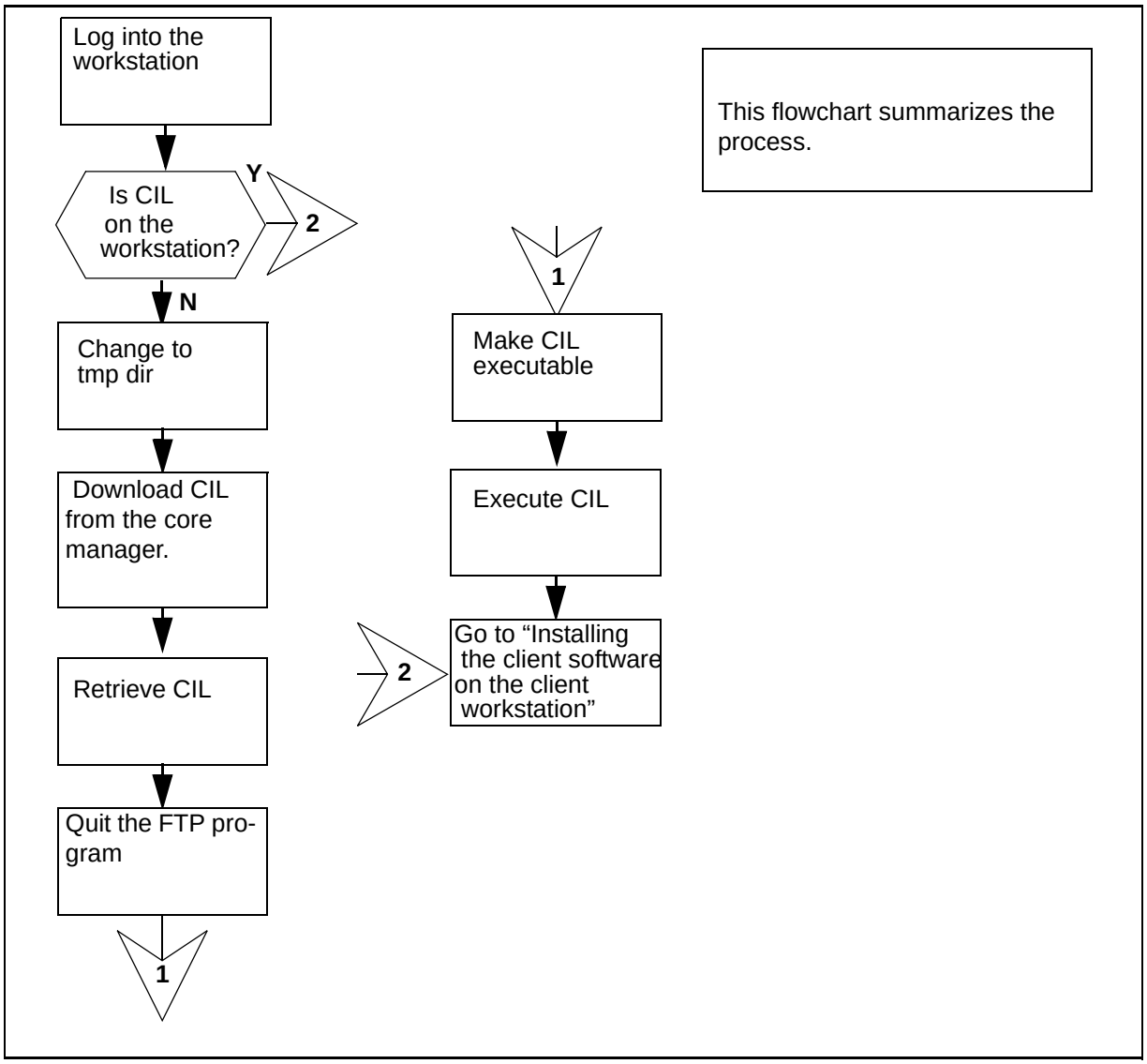
- the platform of the client workstations
- the internet protocol (IP) address of the client workstations
- the client software fileset names

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

At the local or remote VT100 console

1

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.

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 on page 185.

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

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
```

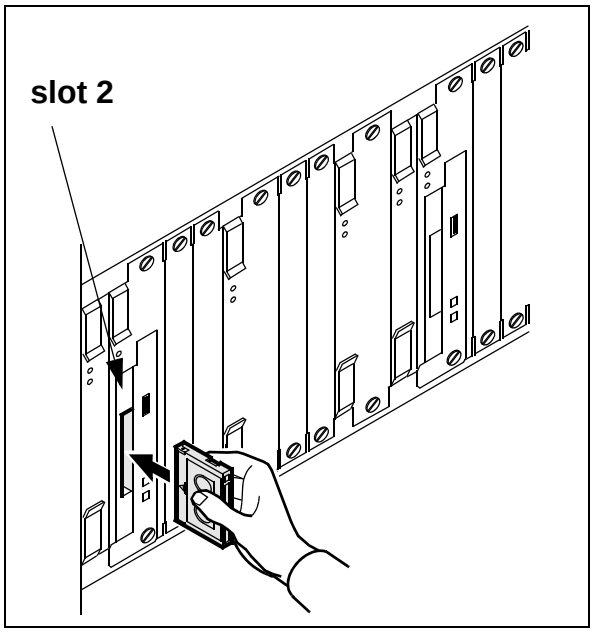
3 Access the SWIM level:

```
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.

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 on page 178.

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

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.

Installing the logreceiver tool on a client workstation

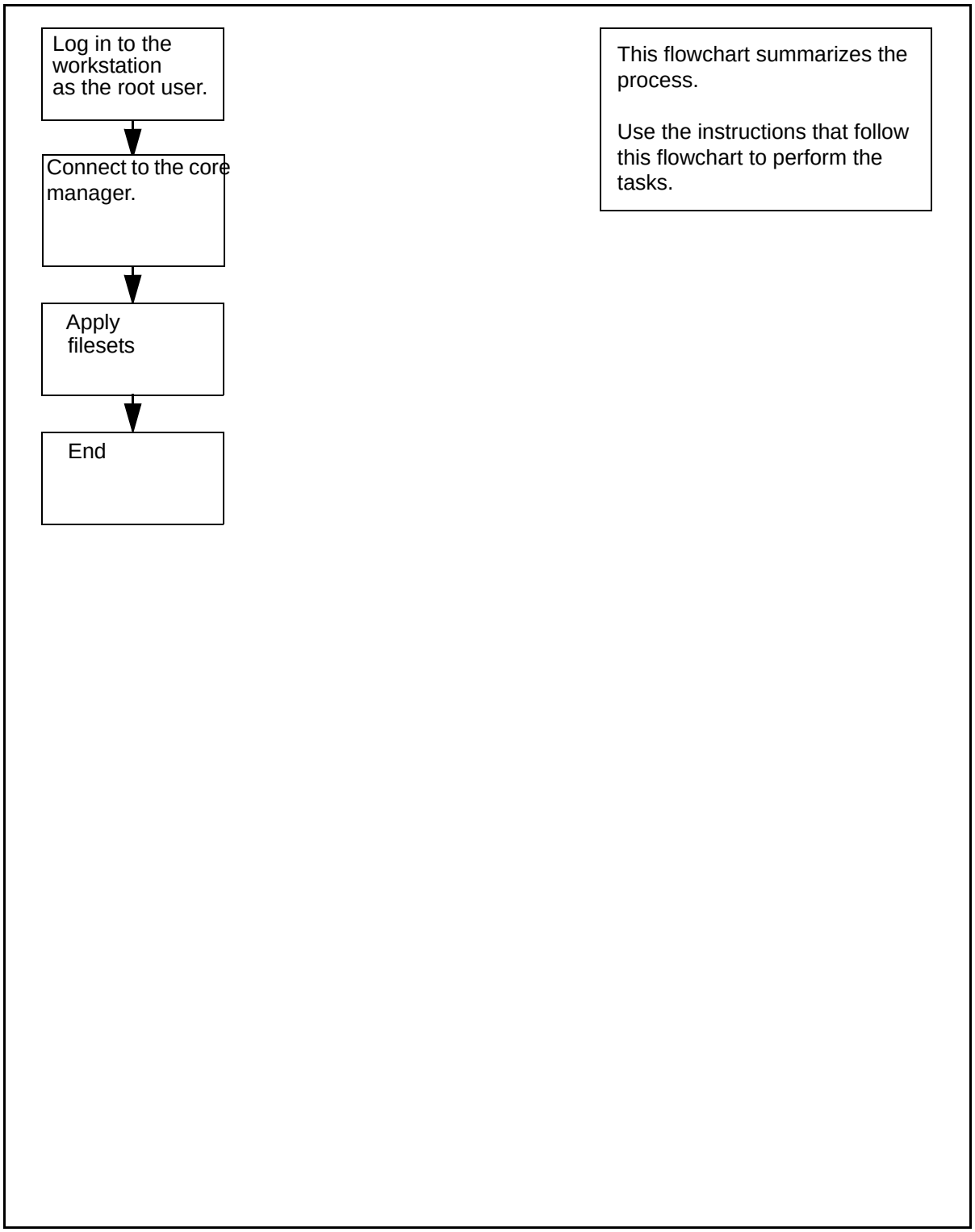
Purpose

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

At the local or remote VT100 console

1

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.

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.

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

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

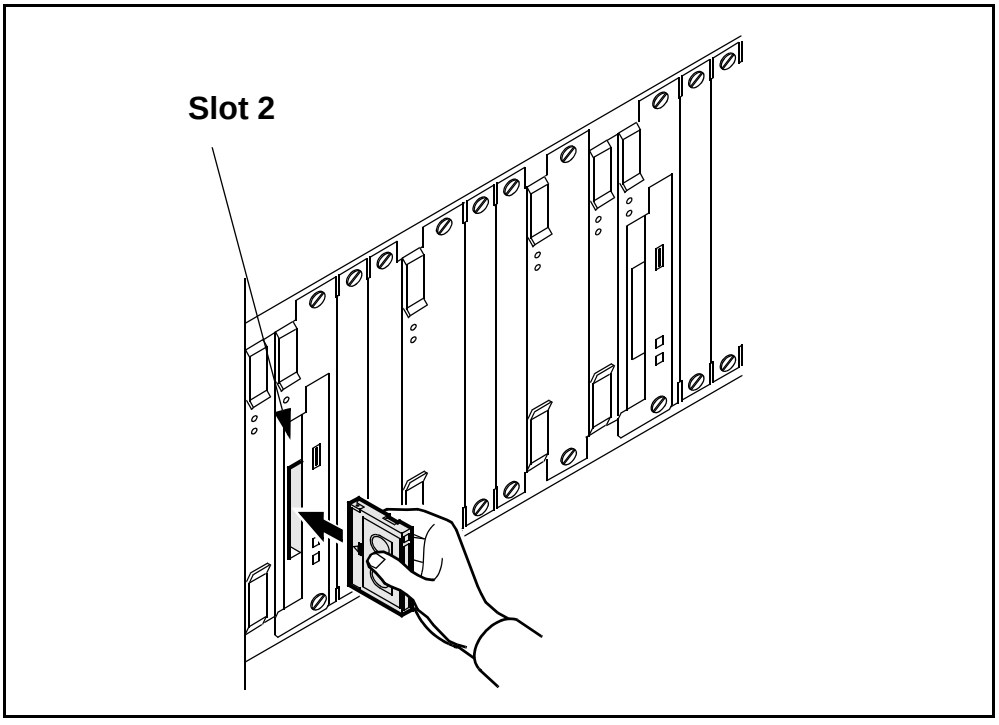
swim

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.

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.

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.

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.

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.

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 outbound connection security for OMDD

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 the login ID and password for the root user.

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 '10.10.10.10' 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 '10.10.10.10' (RSA) to the list of known hosts.

9 Press ctrl + C to terminate the program.

10 Exit the telnet session:

```
exit
```

11 You have completed this procedure.

Troubleshooting

Possible error scenarios that may occur when you are performing this procedure and the steps to perform in addressing these problems are listed below:

- 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.

  Note: 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.

Note: 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.

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
- ability to perform diskut commands

Note 1: This procedure should be performed before you first perform the procedure, “Configuring core access for SBRM”.

Note 2: 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

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

Note 1: If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

Note 2: If Enhanced Password Control is in effect on the CM and 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.

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, Creating the backup user ID on the core for SBRM on page 205 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

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 Carrier VoIP 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, Creating the backup user ID on the core for SBRM on page 205

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, Creating the backup user ID on the core for SBRM on page 205

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.

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 SPFS-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

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.

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 Installing the ETA application server software on the core manager on page 122.

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

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.

Removing an ETA server from a core manager

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.

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.

Note 1: CMFT is supported only on clients running Solaris 7, Solaris 8, or Solaris 9.

Note 2: SCP and SSH must be installed before you can install CMFT. The version of SSH that is installed must support the SSH 2.0 protocol.

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

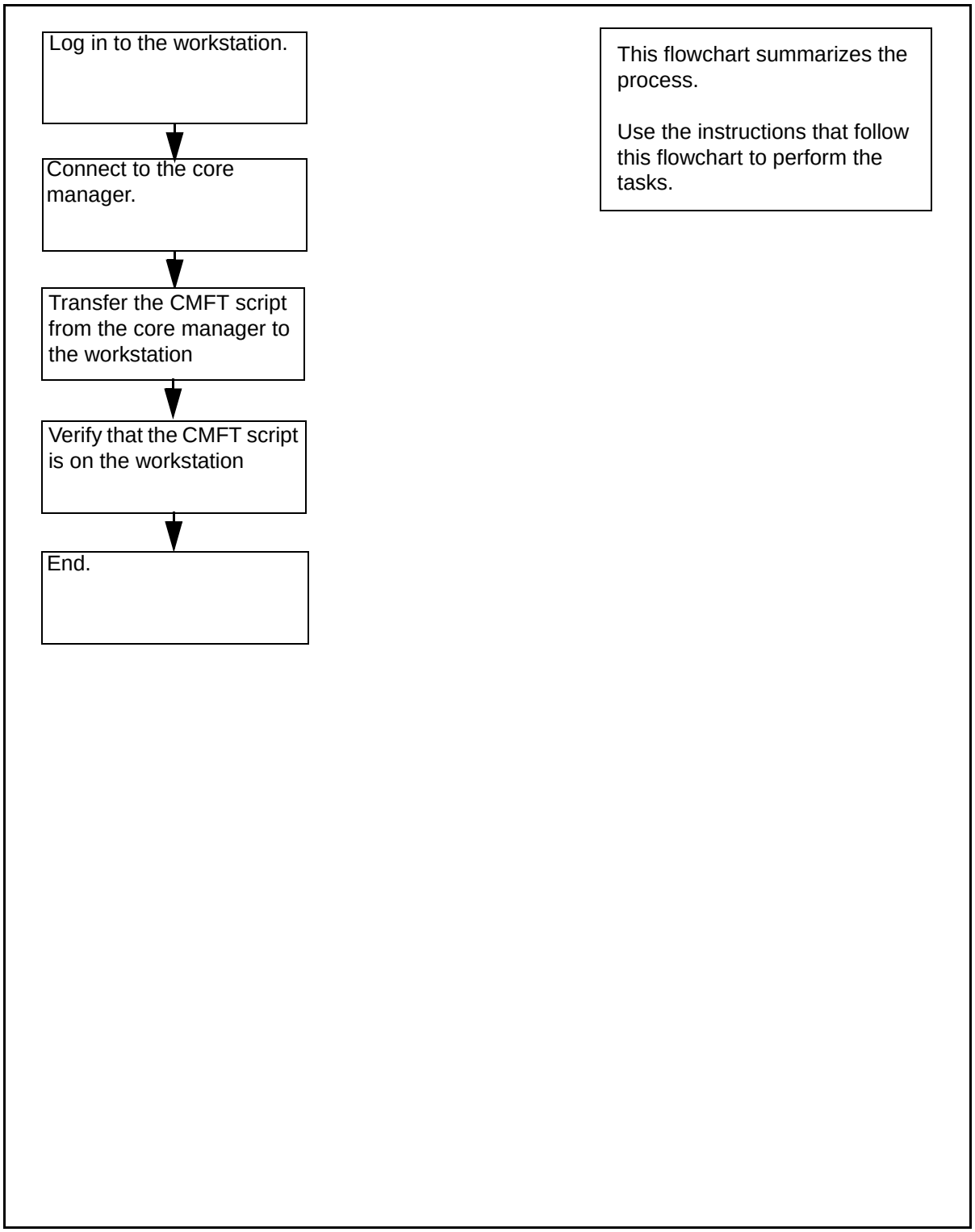
Logging on to the Core and Billing Manager 850

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

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



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 CMFT on a client workstation

At the local or remote VT100 console

1 Log in to the client workstation.

2 Get the CMFT script from the core manager:

```
scp
root@<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.

Installing SCFT

Purpose

Use this procedure to install SCFT (SSH Core File Transfer).

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

Installing SCFT

At the local or remote VT100 console

1 Log into the core manager. Refer to Prerequisites on page 220 for details.

2 Access the maintenance interface:

```
sdmmtc
```

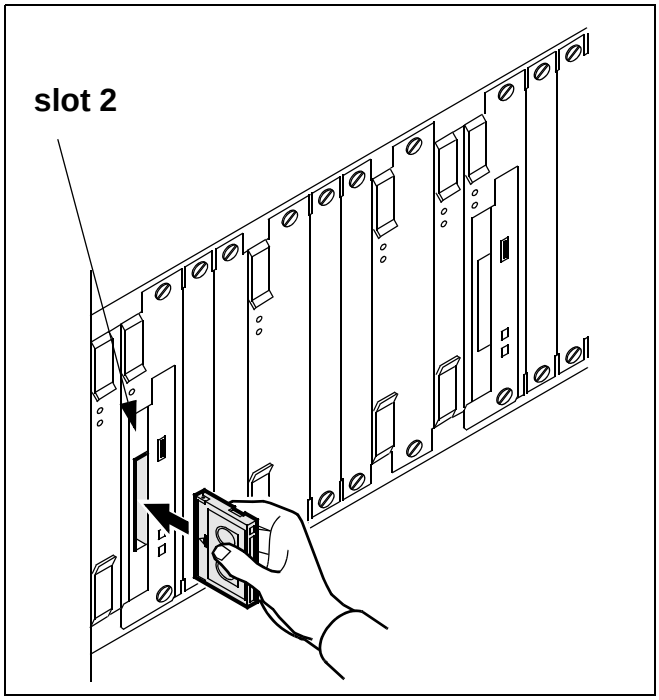
3 Access the SWIM level:

```
swim
```

4 Use the following table to determine your next step.

If you are installing the software from	Do
a tape	insert the 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 SSH Core File transfer fileset:

`select <n>`

where

<n>
is the number next to the SSH Core File transfer fileset

7 Apply the selected fileset:

`apply`

8 Confirm the Apply command:

`y`

9 You have completed this procedure.

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

At the local or remote VT100 console

1 Log into the core manager. Refer to Prerequisites on page 223 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.

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

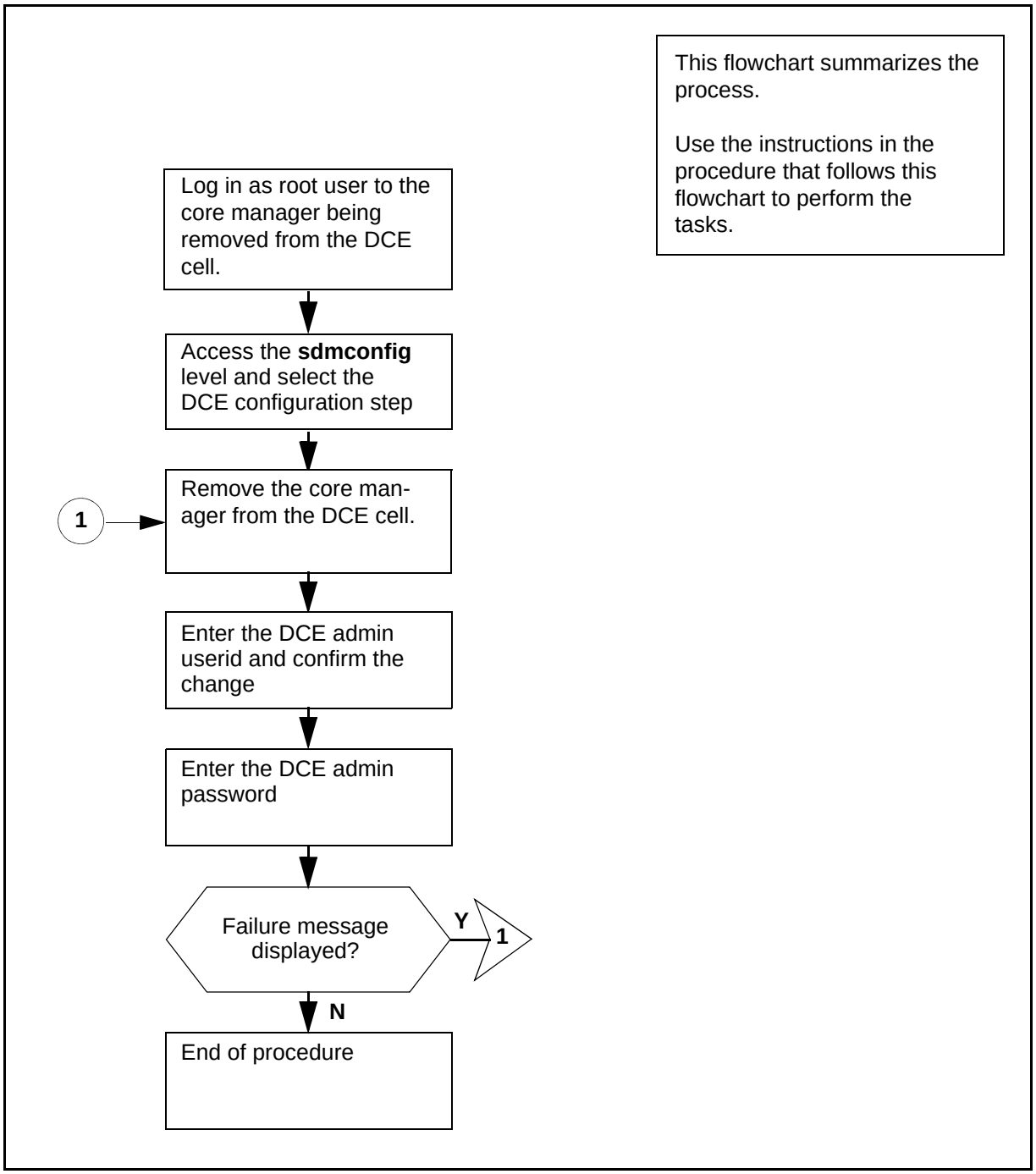
sub administrator account, refer to the DCE procedure “Creating SDM administration account”.

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

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.

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 on page 154.

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

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

If the list	Do
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.

Restricting the SFT port range

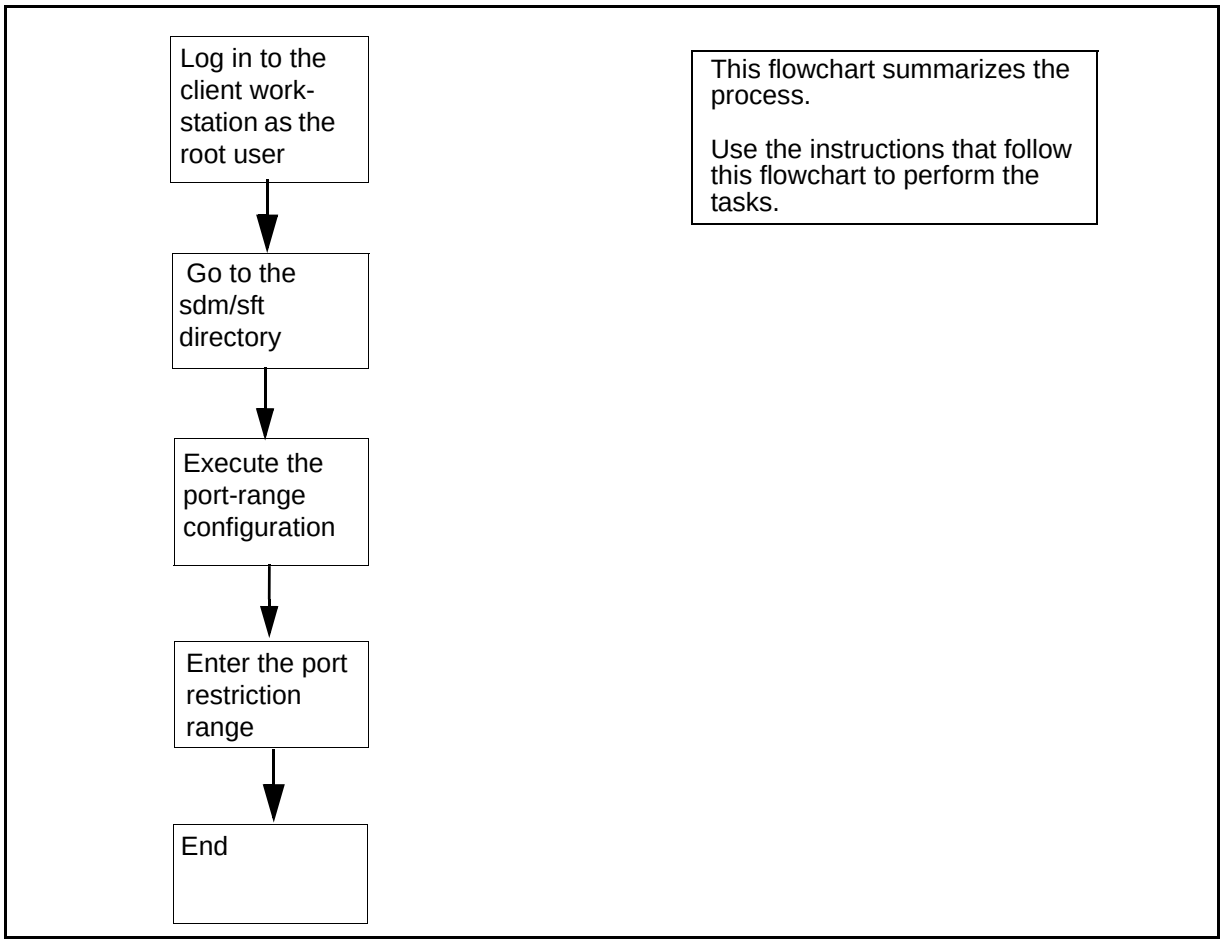
Purpose

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

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.

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

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.

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

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 /
```

3

CAUTION

The following command will stop all processes that have open files in the designated file system (that is, in <file_system_name>).

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.

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.

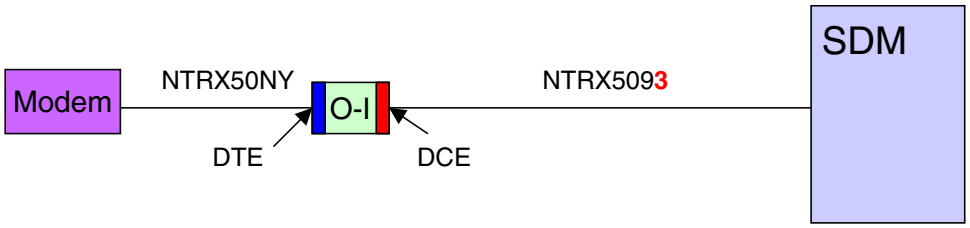
Refer to the following table to determine which procedure you should use to change console connections with O-I.

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 on page 243
change from a local to a remote console connection	the procedure Changing from a local to a remote console connection with O-I on page 245

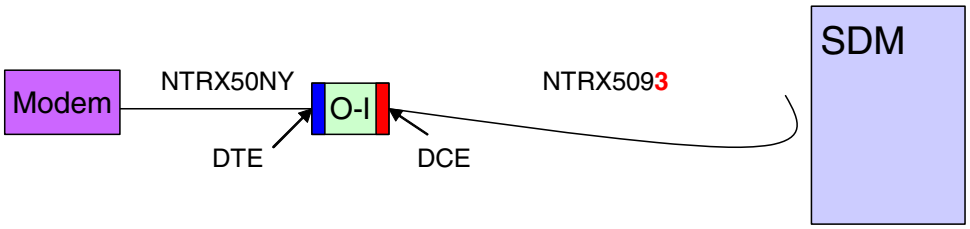
Changing from a remote to a local console connection with O-I

At the core manager

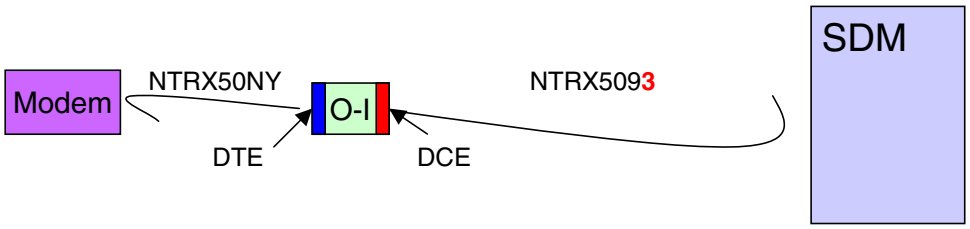
1 The following figure shows an existing remote console connection. Be sure that you are familiar with the configuration, then go to step 2.



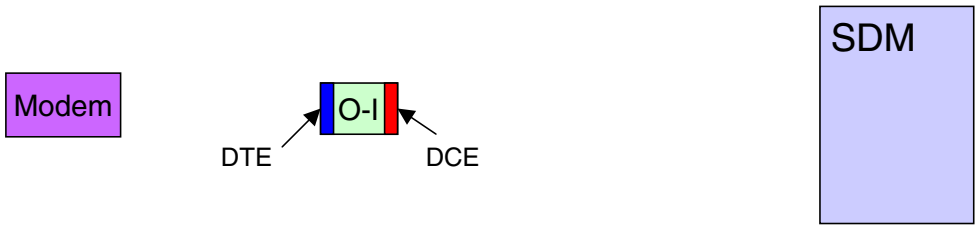
2 Disconnect the NTRX5093 from SP0.



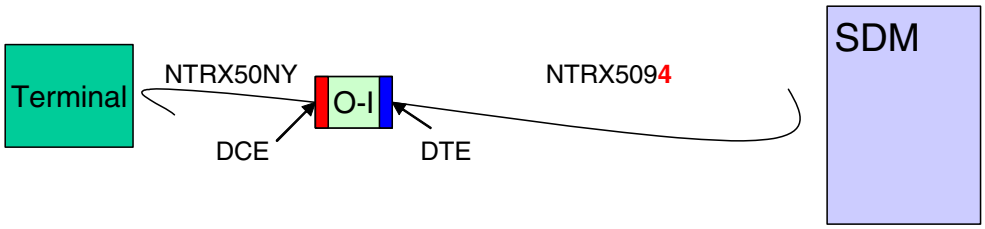
3 Disconnect the NTRX50NY from the modem.



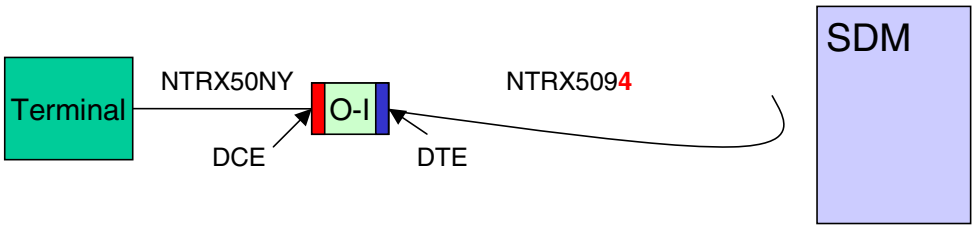
4 Disconnect NTRX50NY from the DTE side of the O-I, and NTRX5093 from the DCE side of the O-I.



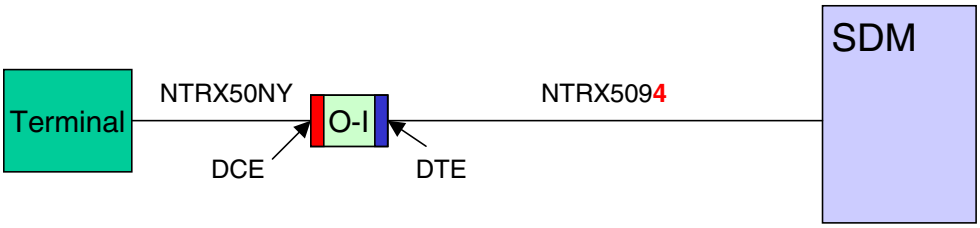
5 Connect the NTRX50NY to the DCE side of the O-I. Connect the NTRX5094 to the DTE side of the O-I.



6 Connect the NTRX50NY to the terminal.



7 Connect the NTRX5094 to SP0.

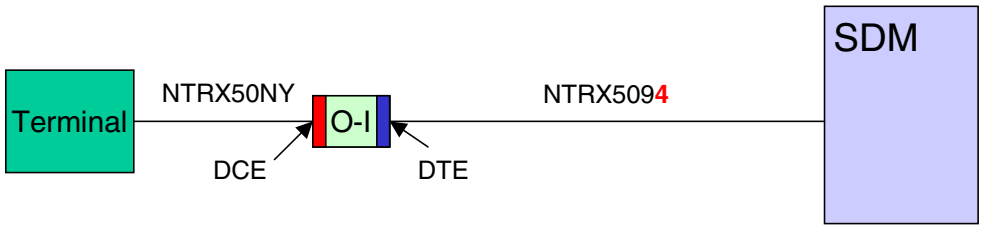


8 You have completed this procedure.

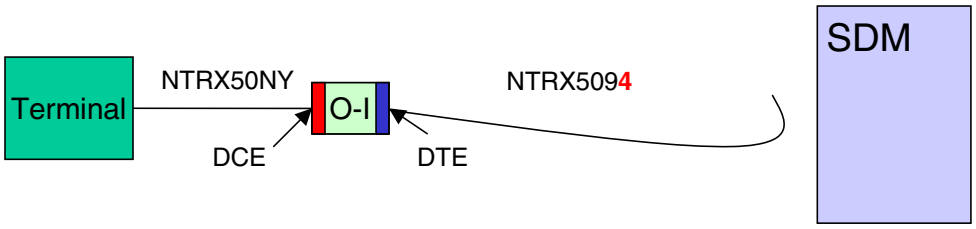
Changing from a local to a remote console connection with O-I

At the core manager

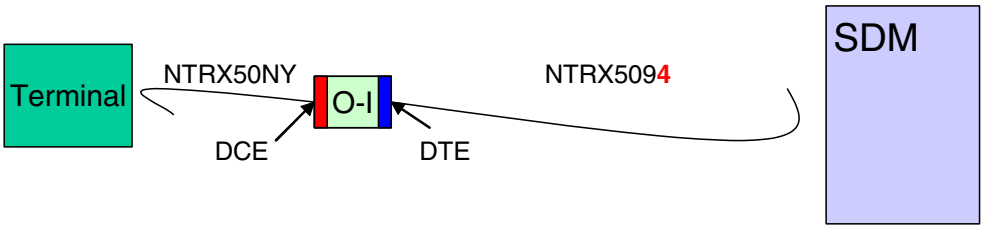
1 The following figure shows an existing local console connection. Be sure that you are familiar with the configuration, then go to step 2.



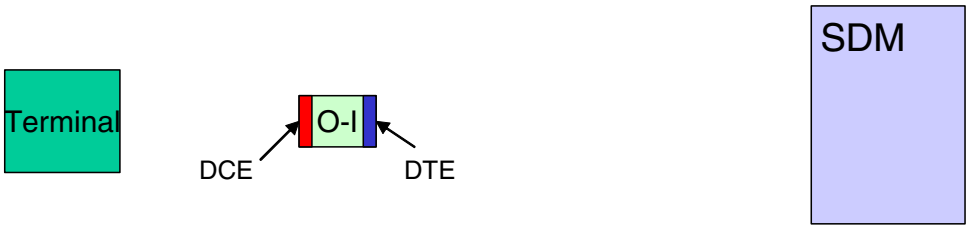
2 Disconnect the NTRX5094 from the SP0.



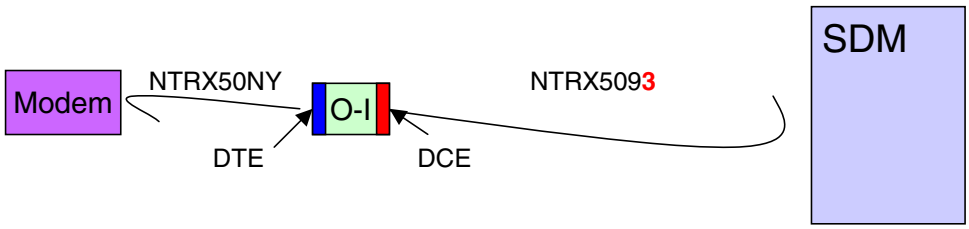
3 Disconnect the NTRX50NY from the terminal.



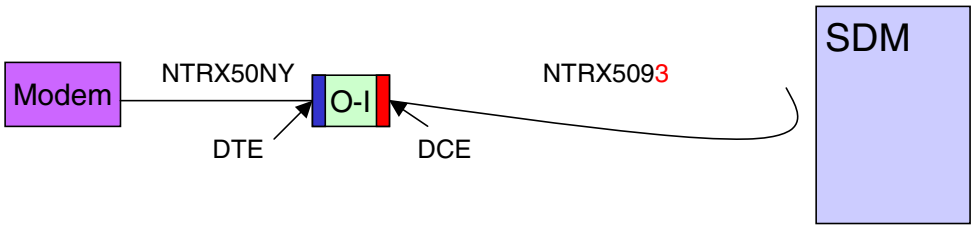
4 Disconnect NTRX50NY from the DCE side of the O-I and NTRX5094 from the DTE side of the O-I.



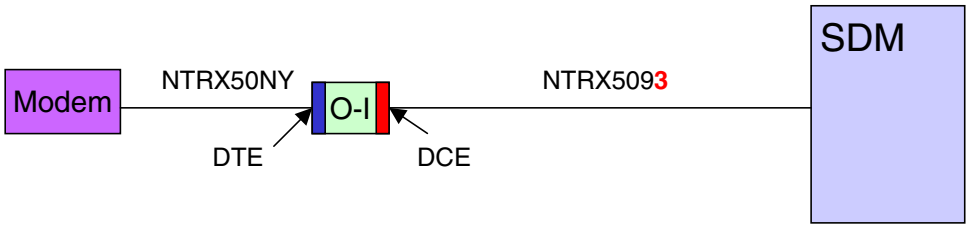
5 Connect the NTRX50NY to the DTE side of the O-I. Connect the NTRX5093 (SDM modem cable) to the DCE side of the O-I.



6 Connect the NTRX50NY to the modem.



7 Connect the NTRX5093 to SP0.



8 You have completed this procedure.

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

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.