# SDM Configuration Management

## Configuration management strategy

The Succession network configuration management strategy is to offer 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 SDM.

## Tools and utilities

The SDMConfig level contains commands for commissioning the SDM. The SWIM level of the SDM 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 SDM. To use the tool, you must log on to the SDM as a root user, and enter the **SDMCONFIG** command. The system displays the SDMConfig level and the commissioning status of the components of the SDM. 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>**<br><br>*where*<br>**<n>** is the number of the commissioning step assigned to the component that you want to commission<br><br>***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 SDM, 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**<br><br>***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**<br>*or*<br>**q** (quit), or **0** |
| Quit the commissioning program | **quit all** |

## Configuration management procedures

For configuration management procedures, refer to the modules for specific SDM 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”<br>• “Configuring an SDM in a DCE cell”<br>• “Removing an SDM from a DCE cell” | Configuration Management |
| Edge Nodes | • “Commissioning or decommissioning edge node monitoring”<br>• “Adding or removing edge nodes, or configuring edge node monitoring parameters” | Configuration Management |
| Network Time Protocol | • “Commissioning or decommissioning Network Time Protocol” | Configuration Management |
| Passthru Users | • “Adding or removing Passthru users” | Security and Administration |

**Commissioning procedures**

| Component | Procedure | Document |
|---|---|---|
| Password | • “Changing a user password” | Security and Administration |
| Time Zone | • “Changing the system time zone and daylight savings time parameters | Security and Administration |
| X25 Connectivity | • “Commissioning or recommissioning X.25 connectivity” | Upgrades |
| | • “Decommissioning X.25 ports [on UMFIO or SYNC module]” | Configuration Management |

# Installing the log delivery application

The following procedure outlines the steps that must be performed to install the log delivery application on the SDM.

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

- Log delivery service
- Log delivery service client
- Generic data delivery

Prior to performing this procedure, ensure that there are no disk faults on the SDM.

### Installing 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 Succession office | step 1 |
| any other Succession office | step 2 |

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

**3** Switch user to root using the root ID and password.

**4** 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 5 |
| in a directory | retrieve the filesets from the directory, and continue with step 6 |

**5** Access the Apply level of the SDM 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

**6** 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

**7** Install the filesets:

```
> apply
```

**8** Confirm the apply command:

```
> y
```

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

**9** Configure the Passport Log Streamer application as follows:

***Note:*** If you previously had the Succession 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** When prompted, enter the IP address for the first Preside MDM node, then the second.

*Examples*

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

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

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

*Examples*

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

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

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

**c** When prompted, indicate whether you want to receive MDM logs.

| If | Do |
|---|---|
| y (yes) | substep d |
| n (no) | substep e |

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

*Example response*

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

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

**e** When prompted, indicate whether you want to specify Preside MDM log filters.

| If | Do |
|---|---|
| y (yes) | substep f |
| n (no) | substep h |

**f** When prompted, type the number of filters you want to specify, and press the Enter key.

**g** When prompted, enter the required set of Preside MDM 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.

**h** The system displays the following message:

```
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.

Indicate whether you want to specify Passport 8600 log filters: **`y`** or **`n`**.

| If | Do |
|---|---|
| y (yes) | substep i |
| n (no) | substep k |

**i** When prompted, type the number of filters you want to specify, and press the Enter key.

**j** 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.

**k** When prompted, confirm the configuration data you entered:

**`> y`**

*Response*

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

**10** Begin to bring the Log delivery service application into service. Access the Application (Appl) level:

**`> appl`**

**a** Busy the application fileset:

**`> bsy`** ***`<fileset_number>`***

*where*
fileset_number is the number next to the following application fileset:

- Log delivery service

**b** Return the application fileset to service:

**`> rts`** ***`<fileset_number>`***

*where*
fileset_number is the number next to the application fileset 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.

**11** 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 will forward user-defined streams of logs.

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 an SDM port number)
- a file device (a file on the SDM)

***Note 1:*** You can configure up to 30 Log Delivery output devices.

***Note 2:*** 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 20.

***Note 3:*** If you want to delete an existing device, refer to the procedure Deleting a device using logroute on page 27.

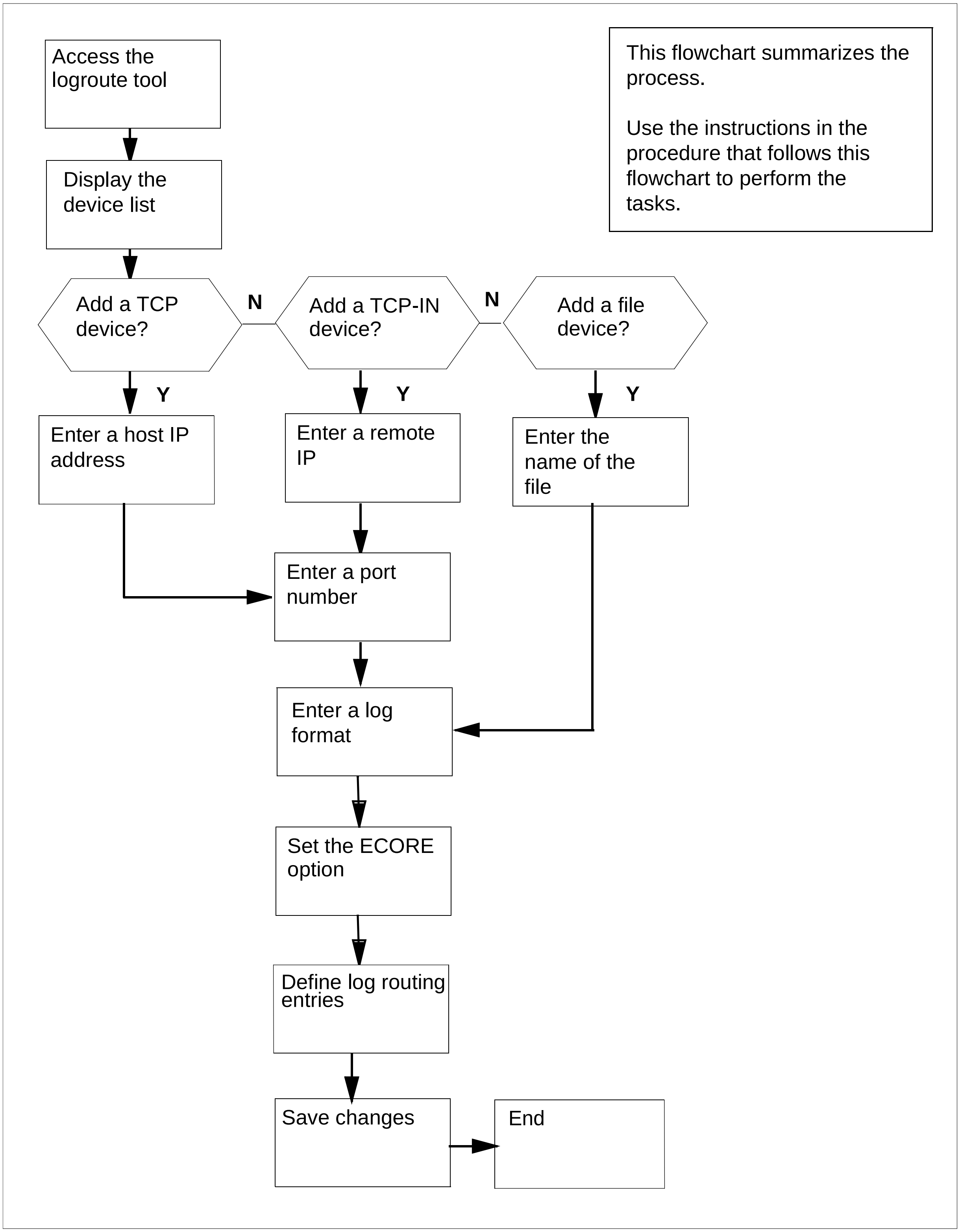
***Note 4:*** If you want to modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters on page 38.

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.

## 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



### Configuring log delivery destinations

#### *At any workstation or console*

**1** Log in to the SDM.

**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 ==>
```

***Note:*** 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.

**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 9 |
| file device | step 12 |

6 Start adding a TCP device:

**> 1**

*Example response*

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

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




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

7 Enter a host IP address.

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

Continue with step 14.

9 Start adding a TCP-IN device:

**> 2**

*Example response*

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

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




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

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

11 When prompted, enter an SDM 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.

16 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 SDM on page 32. Logs suppressed at the CM cannot be unsuppressed for a specific device.

*Response*

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

**17** 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.

*Response*

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

| If you | Do |
|---|---|
| want to add more routing entries<br>***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 16 |
| do not want to add more routing entries | enter **`n`**, and go to step 18 |

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

> **`y`**

The new device will be added to the system.

*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.

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

| If you | Do |
|---|---|
| want to add more devices | go to step 5 |
| do not want to add more devices | go to step 20 |

**20** Return to the Device List Menu screen:

**> 5**

**21** Return to the Logroute Main Menu screen:

```
> 6
```

**22** Quit the logroute tool:

```
> 6
```

**23** 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.

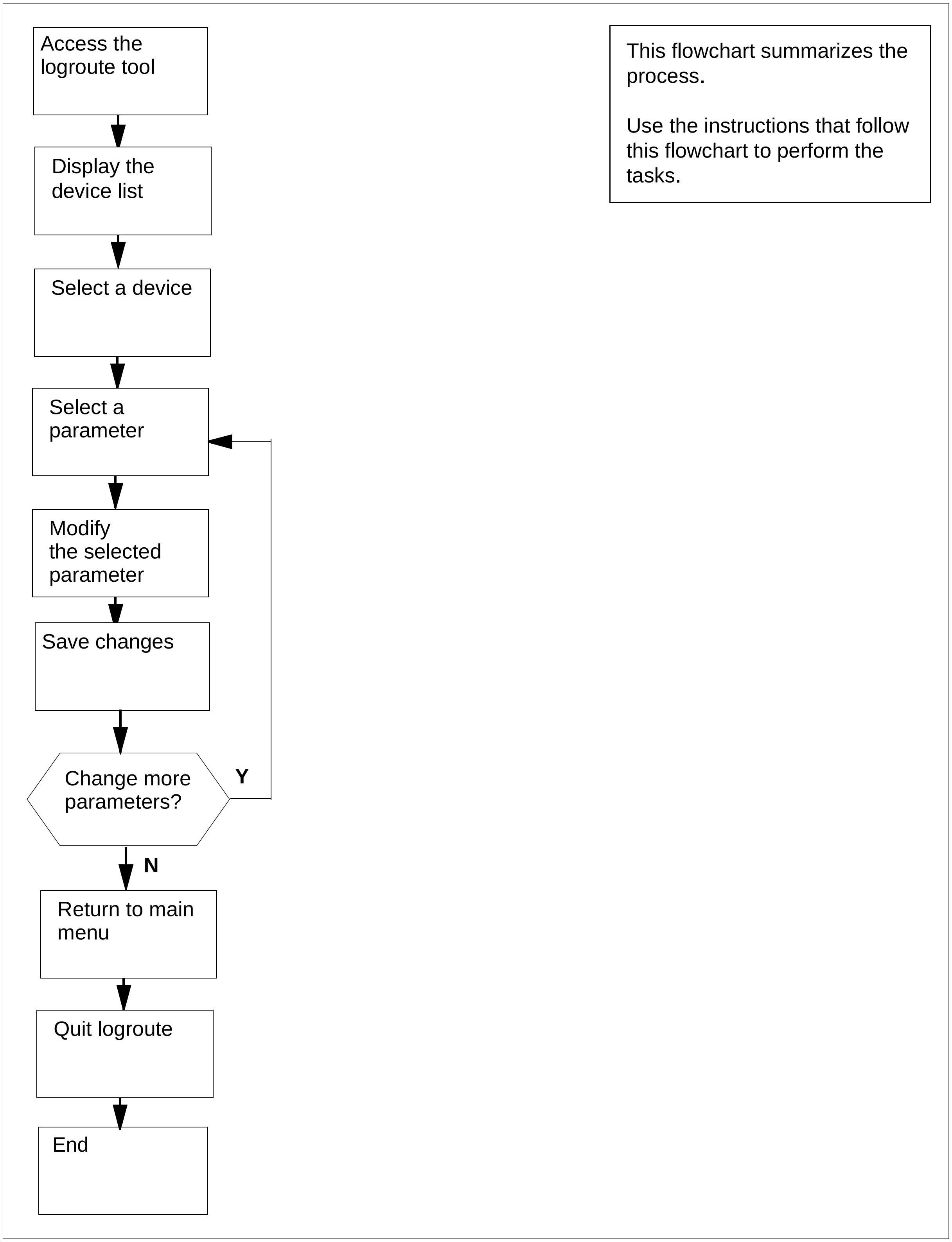
***Note 1:*** The routing rules you enter for each device only accommodate the set of logs defined in the procedure Specifying the logs delivered from the CM to the SDM on page 32. Logs that are being suppressed at the CM cannot be un-suppressed for a specific device.

***Note 2:*** If you want to modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters on page 38.

## 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



# Procedure

### Modifying a log device using logroute

***At the VT100 console***

**1** Log in to the SDM.

**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 will be 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.

> ***Note:*** 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.

*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.

*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
```

*Response*

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

**17** Confirm the save command:

```
> y
```

*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.

18 Use the following table to determine your next step.

| 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 19 |

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

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

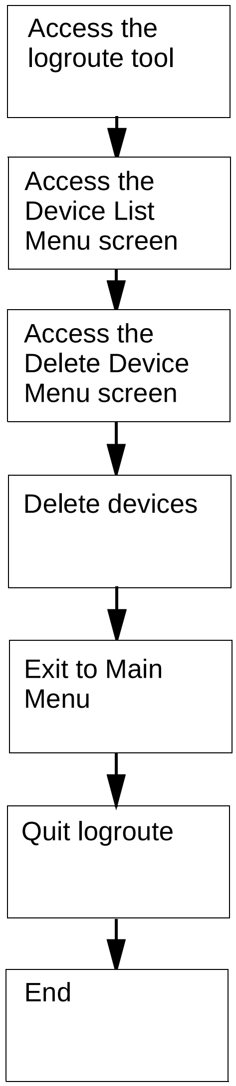
Use this procedure to delete a log device using the Log Delivery Application Commissioning Tool (logroute). This procedure allows you to delete any one of the following devices:

- a TCP device (an IP and port address on the network)
- a TCP-IN device (a port on the SDM)
- a file device (a file on the SDM)

## 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




This flowchart summarizes the process.

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

# Procedure

### Deleting a device using logroute

***At the VT100 console***

**1** Log in to the SDM.

**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**

*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.

# Specifying the logs delivered from the CM to the SDM

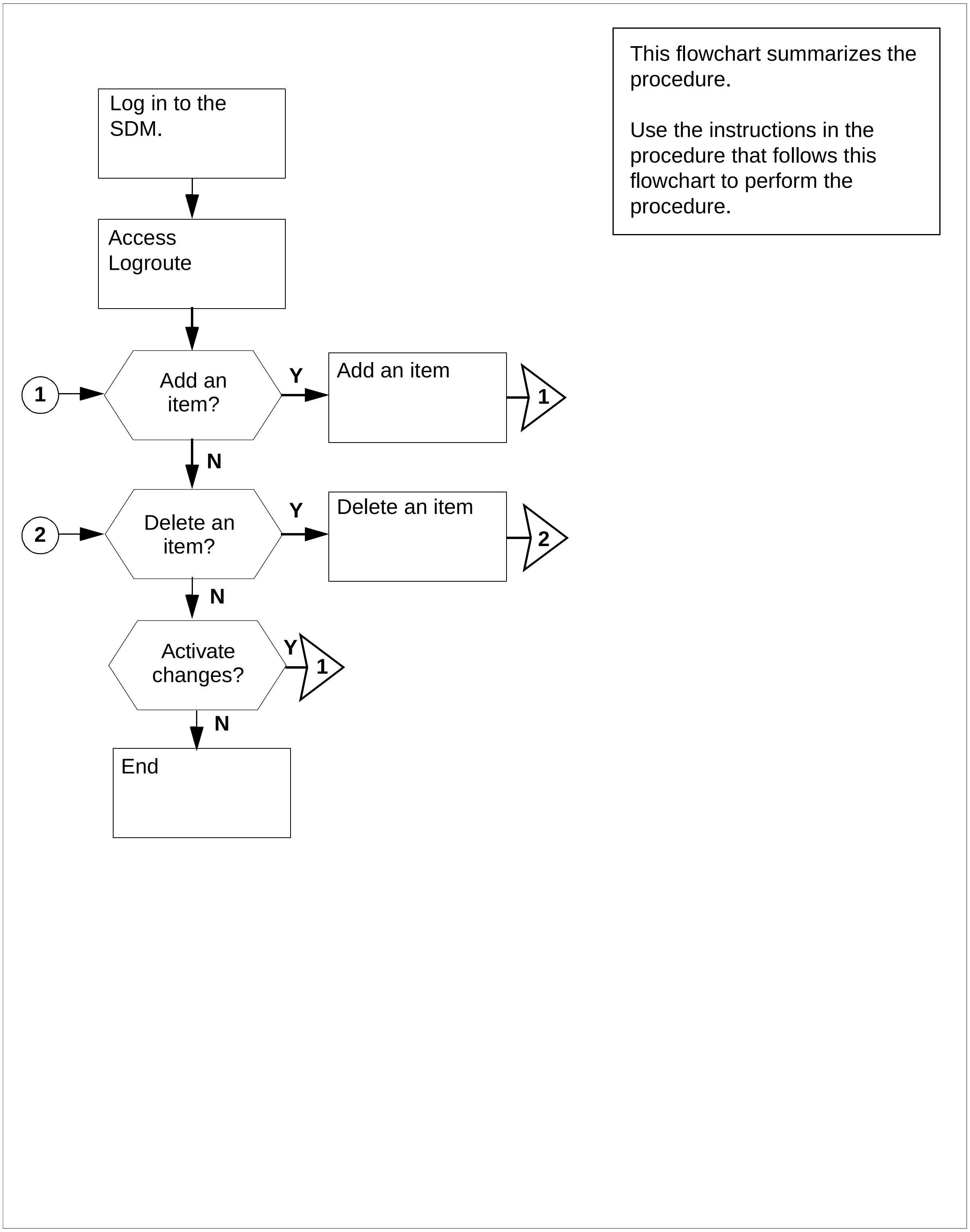
## Purpose

Use this procedure to define which logs will be delivered from the computing module (CM) to the SDM. 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.

## 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 SDM



## Procedure

### Specifying the logs delivered from the CM to the SDM

***At the VT100 console***

**1** Log in to the SDM.

**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 ==>
```

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

| If you want to | Do |
|---|---|
| add routing report to the list | step 5 |
| delete routing report from the list | step 10 |

**5** 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*

```
                    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 or the
Succession Log Delivery application for the CM configuration
to take effect.
```

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

| 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") ==>
```

**7** 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.

*Response*

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

**8** Save your changes:

```
> y
```

The new item is added to the list.

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

| If you | Do |
|---|---|
| want to add more entries to the list | step 6 |
| do not want to add more entries to the list | step 14 |

**10** 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 ==>
```

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

*Response*

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

**12** Confirm the delete command:

**> y**

*Response*

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

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

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

| If you | Do |
|---|---|
| want to delete more entries from the list | step 11 |
| do not want to delete more entries from the list | step 14 |

**14** Return to the CM Config File Menu screen:

**> abort**

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

| 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 16 |

**16** Return to the Logroute Main Menu screen:

**> 5**

**17** Quit the logroute tool:

**> 6**

**18** 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. If the global parameters do require modification, use this procedure to change the configuration. 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 11
> - Modifying a log device using logroute on page 20

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 Networks 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.

  If you enter CLLI, the CLLI name of your system will be attached to all logs.

  If you enter 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, your system’s CLLI will be 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 (Meg): 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:

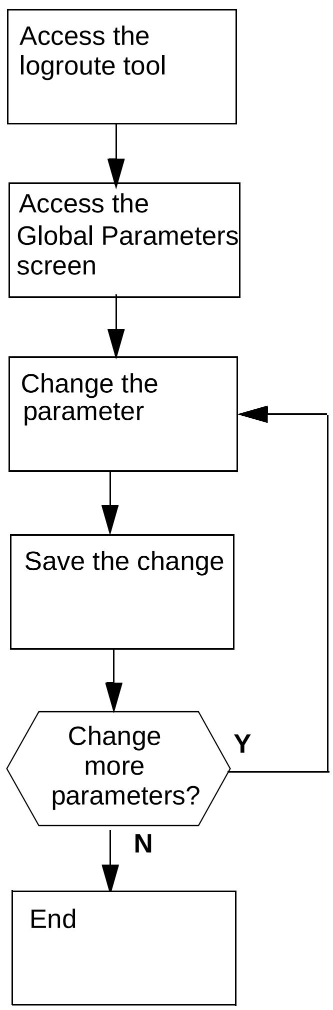
- incoming end of line character: default is 10 which corresponds to a line feed character (go to the next line)
- outgoing end of line characters: default is 10 13 which represents a line feed (go to the next line) followed by a carriage return
- start of log characters: default is 10 13 which represents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

## 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**




This flowchart summarizes the process.

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

## Procedure

### Configuring Log Delivery global parameters

***At the VT100 console***

**1** Log in to the SDM. Use the maint user ID and password, then switch user to root using the root ID and password.

**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.

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

| If you | Do |
|---|---|
| want to change another global parameter | step 4 |
| do not want to change another global parameter | step 12 |

**12** Return to the Logroute Main Menu:

**`> 13`**

**13** Quit the logroute tool:

**`> 6`**

**14** 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.

> 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:*** 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.

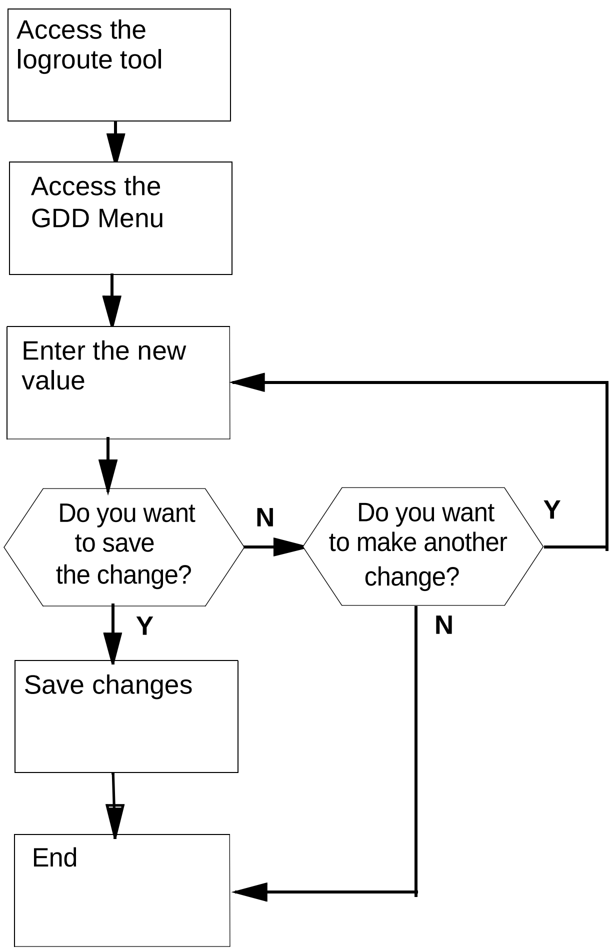
## Task flow diagram

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

This flowchart summarizes the process.

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



### Configuring GDD parameter using logroute

#### *At the VT100 console*

**1** Log in to the SDM.

**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**

*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.

*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**

*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.

*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 SDM.

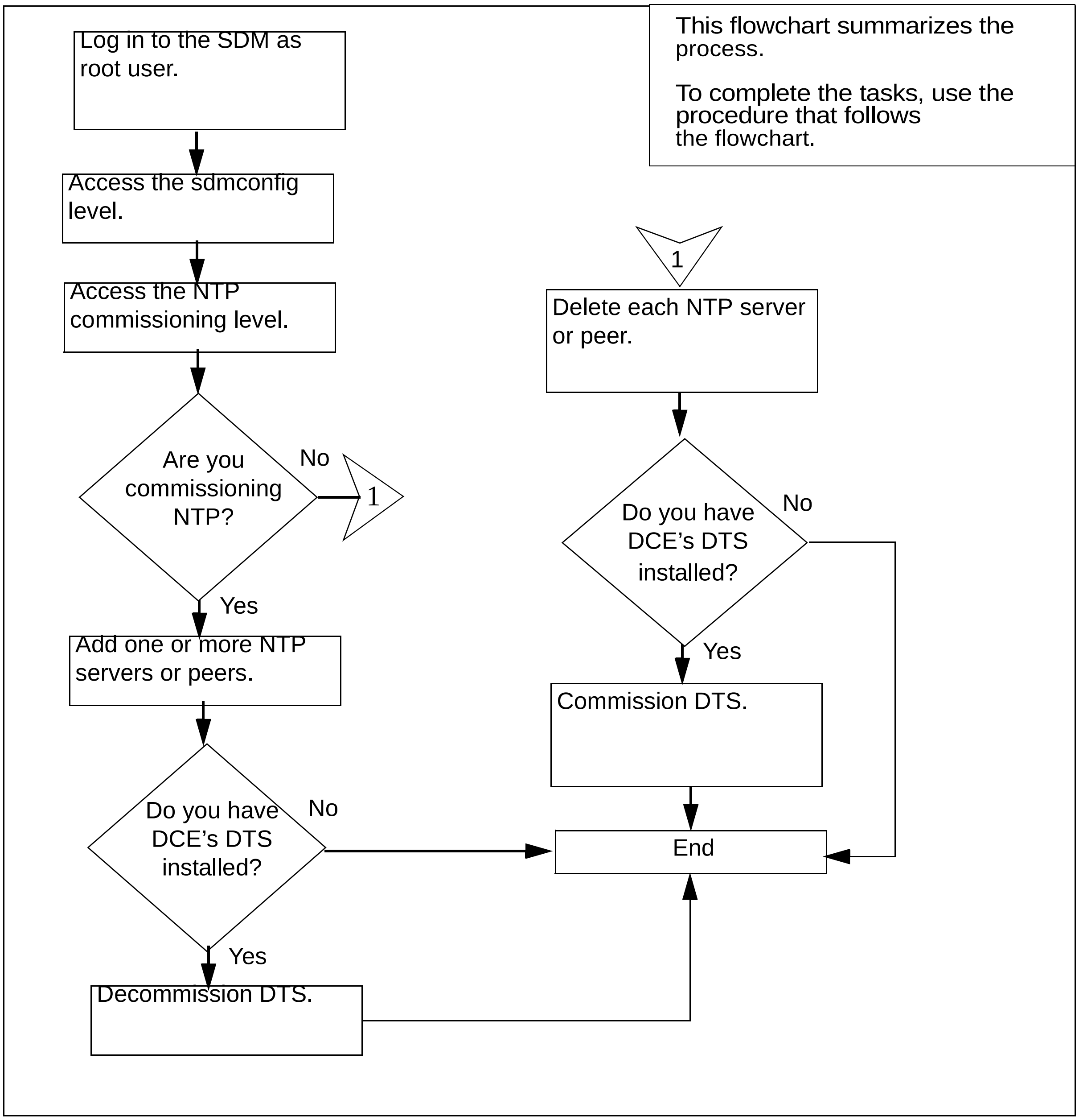
## Prerequisites

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




# Procedure

### Commissioning or decommissioning NTP

#### *At the local VT100 console*

**1** Log into the SDM as a root user.

**2** Access the CLI tool:

**`# cli`**

**3** Access the CLI configuration level:

**`> <#>`**

*where*

**<#>**
is the number next to the CLI configuration level.

**4** Access the NTP configuration level:

**`> <#>`**

*where*

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

| If you are | Do |
|---|---|
| commissioning NTP | step 5 |
| decommissioning NTP | step 7 |

**5** Add an NTP server or peer:

**`> <#>`**

*where*

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

**6** Enter the IP address of the server or peer.

***Note 1:*** A peer can act as a server.

***Note 2:*** 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.

**7** Add or remove additional servers or peers, or exit.

| If you want to | Then |
|---|---|
| add additional servers or peers | step 5 |
| remove all NTP servers or peers | step 8 |
| remove only selected NTP servers or peers | step 10 |
| 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 this step |
| exit | go to step 12 |

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

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

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

15 Access the SDM RMI level to see the response.

**# sdmmtc ntp**

16 You have completed this procedure.

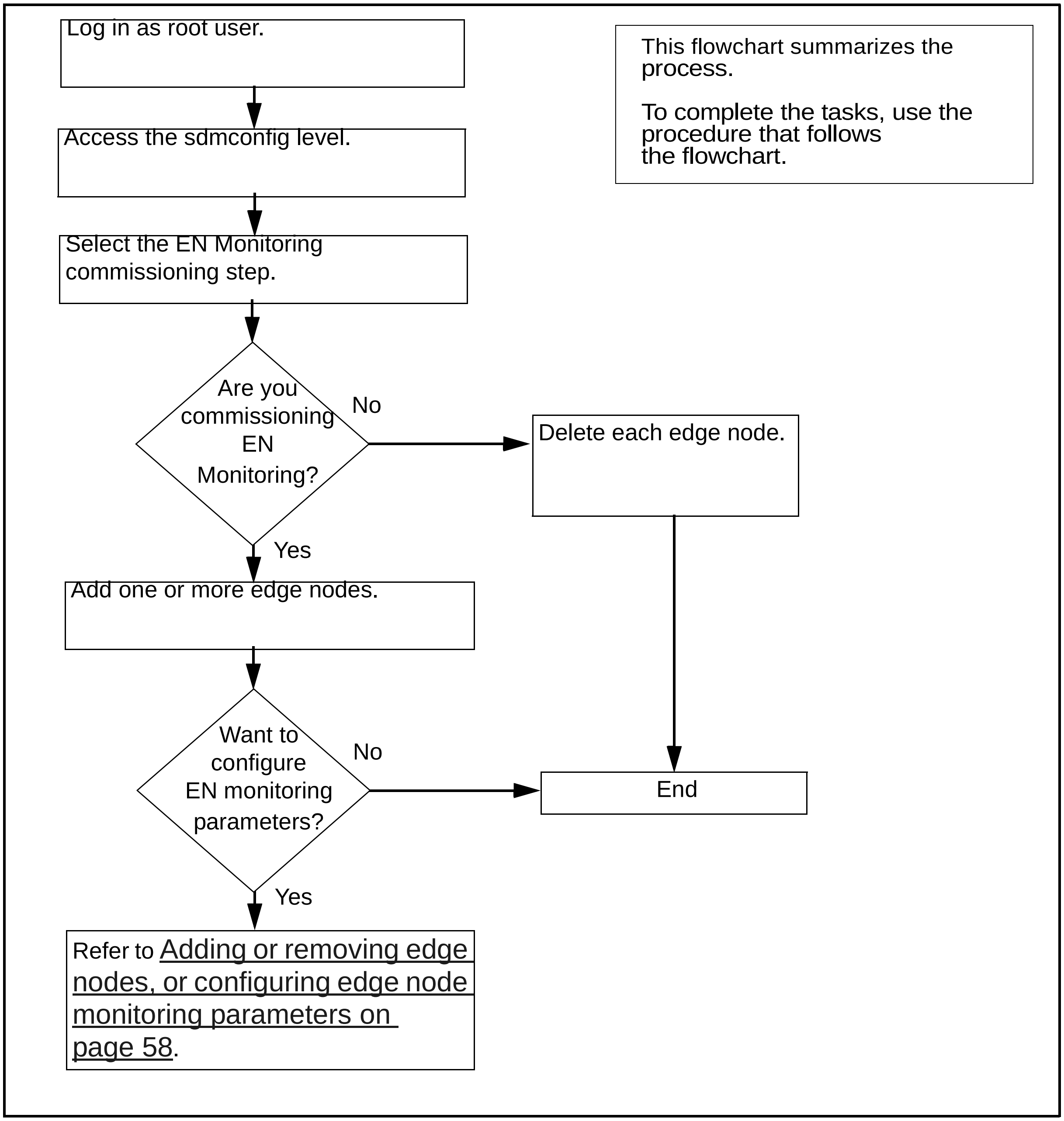
# Commissioning or decommissioning edge node monitoring

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

## 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



# Procedures

### Commissioning edge node monitoring

***At the workstation or console***

1 Log into the SDM as a root user.

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 58 |
| do neither of the above actions | you have completed this procedure |

## Decommissioning edge node monitoring

### *At the workstation or console*

**1** Log into the SDM as a root user.

**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 |

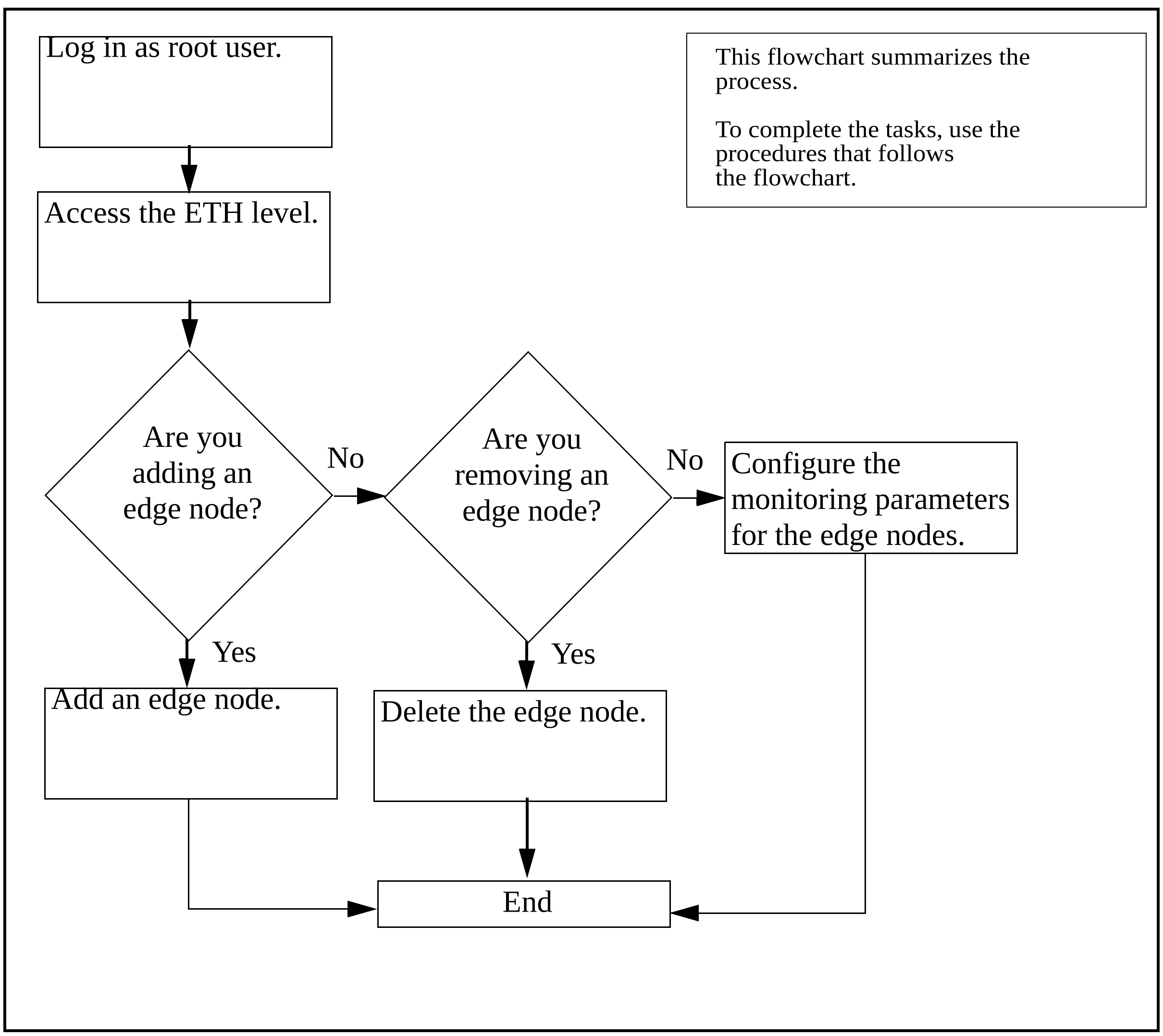
# Adding or removing edge nodes, or configuring edge node monitoring parameters

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

## 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**



## Procedures

### Adding an edge node

***At the workstation or console***

**1** Log into the SDM as a root user.

**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 edge node parameters on page 60 |
| do neither of the above actions | you have completed this procedure |

### Removing an edge node

***At the workstation or console***

**1** Log into the SDM as a root user.

**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 edge node parameters

***At the workstation or console***

**1** Log into the SDM as a root user.

**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)

**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.

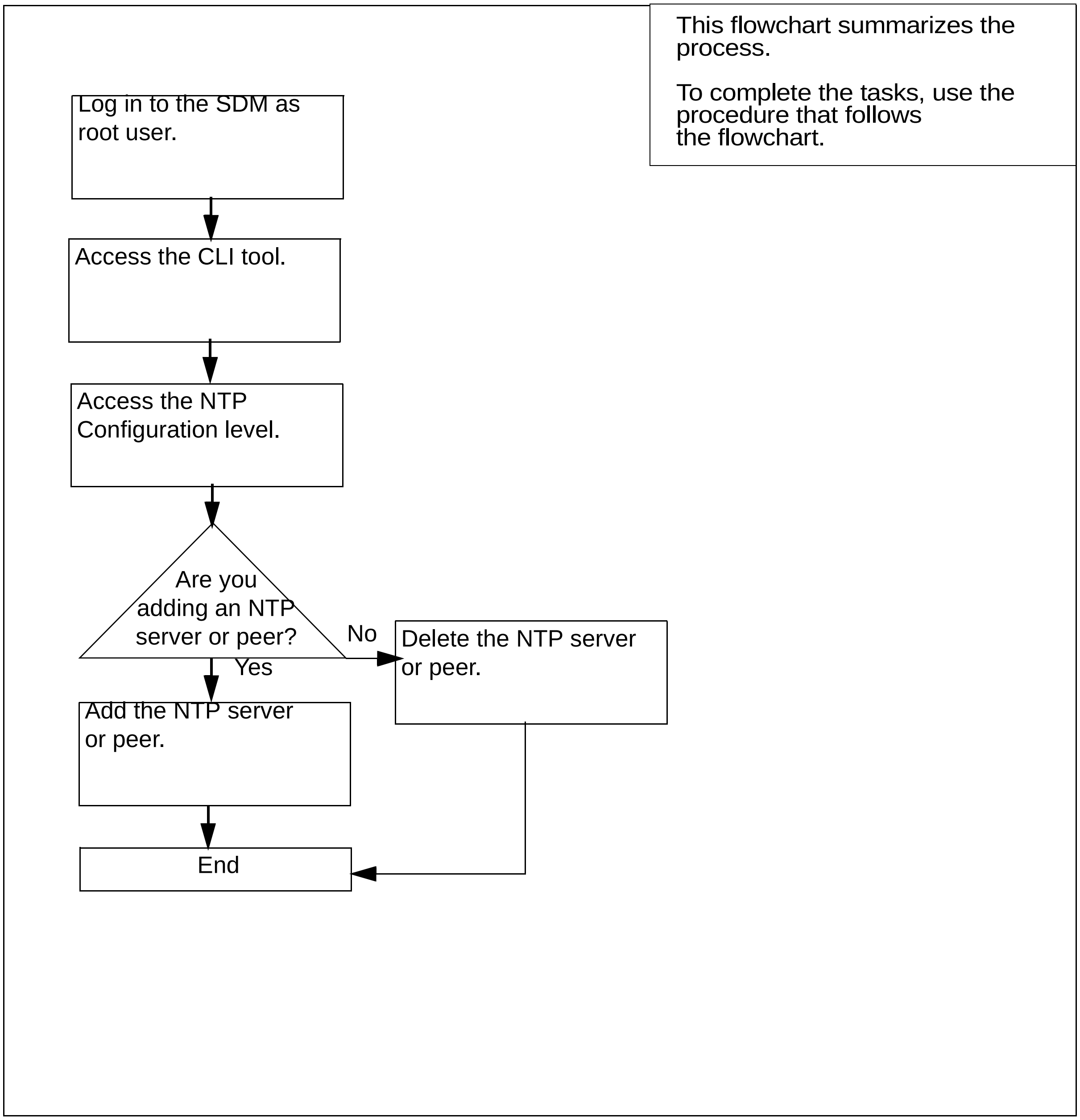
***Note 1:*** You can add up to three NTP servers or peers.

***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.

## 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




# Procedure

### Adding or removing an NTP server or peer

#### *At the local VT100 console*

**1** Log into the SDM as a root user.

**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 | **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 this step |
| exit | go to step 12 |

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

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

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

**15** Access the SDM RMI level to see the response.

```
# sdmmtc 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 SDM disk.

## Prerequisites

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

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

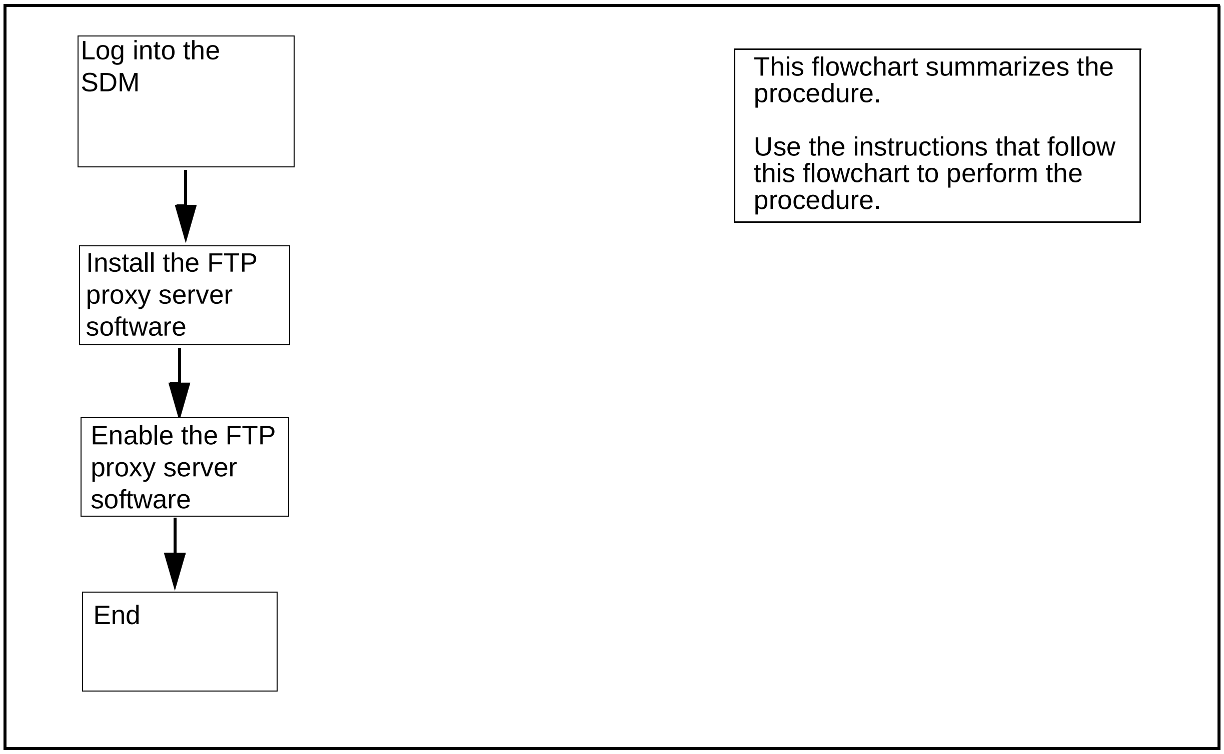
**ATTENTION**
Before you can perform an installation using SWIM, you must have the SDM base software installed on the SDM.

**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




### Installing the FTPProxy server software

#### *At the local or remote VT100 console*

**1** Log into the SDM.

**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.

Goto 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

Use this procedure to remove an FTP proxy server when the FTP proxy application is not required on the SDM.

**Removing an FTP proxy server**

***At the local or remote VT100 console***

**1** Log into the SDM as the maint user.

**2** Access the maintenance interface by typing

`# cbmmtc`

and pressing the Enter key.

**3** Select the filesets to delete by typing

**> select *<ftp_proxy_server_fileset>***

and pressing the Enter key.

*where*

***<ftp_proxy_server_fileset>***
is the number associated with the fileset you want to remove

**4** Delete the filesets by typing

`> 8 or remove`

and pressing the Enter key.

**5** Confirm that you want to delete the filesets by typing

`> y`

and pressing the Enter key.

The system deletes the filesets, displaying a message when the removal is complete.

**6** Exit from the maintenance interface by typing

`> quit all`

and pressing the Enter key.

**7** Log out from the SDM by typing

`> exit`

and pressing the Enter key.

**8** You have completed this procedure.

# Installing the ETA application server software on the SDM

## 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 SDM Enhanced Terminal Access (ETA) server software only.

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

## Prerequisites

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

## Procedure

**Installing the ETA application server software on the SDM**

***At the local or remote VT100 console***

**1** Log into the SDM as root user.

**2** Access the maintenance interface:

```
# sdmmtc
```

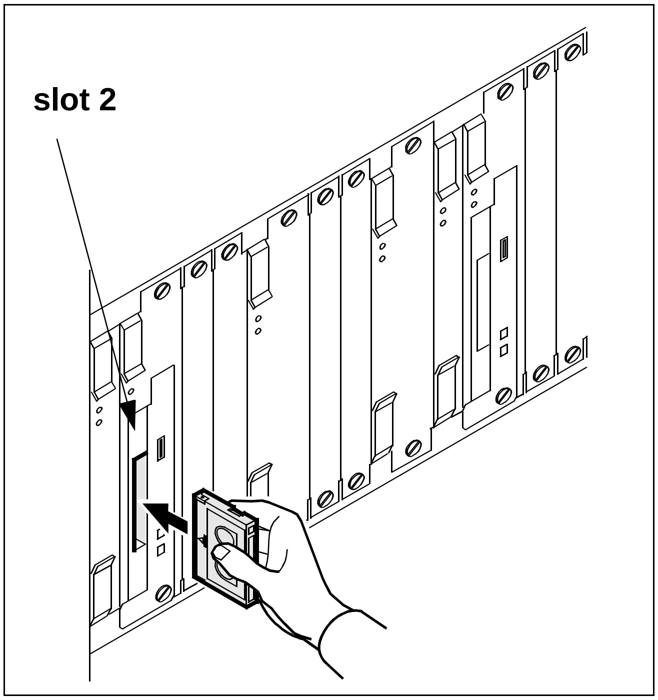
**3** Access the SWIM level:

```
> 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<br><br>***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 74.

# Configuring the ETA application server software

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

**Configuring the ETA application server software**

***At the SDM:***

**1** Log into the SDM as the root user.

**2** Access the SDM 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 SDM maintenance interface:

```
> quit all
```

**9** Log out from the SDM:

```
# exit
```

**10** You have completed this procedure.

# Starting the ETA server on the SDM

## 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 SDM, the ATA and ETA clients provide secure terminal access to the MAP/CI terminal and the SDM sessions. ATA and ETA clients cannot access the ETA server until the ETA server is installed.

## Prerequisites

Before you begin this procedure, you must complete the installation procedures described in Installing the ETA application server software on the SDM on page 71.

**Starting the ETA server on the SDM**

***At the local or remote VT100 console***

**1** Log into the SDM as the maint user.

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

**7** You have completed this procedure.

# Configuring an SDM 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 Networks 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 86.

**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 SDM from another computer. Nortel Networks recommends that you execute the command from a computer attached to the SDM 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 Networks recommends that you configure all your SDM nodes within the same DCE cell. SDM client applications using DCE cannot communicate with SDM nodes configured in a different DCE cell.

## Purpose

Perform this procedure when you want to configure or reconfigure the SDM 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 SDM-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 an SDM, you must configure the SDM in the DCE cell to function correctly. This procedure requires that the DCE cell be in operation.

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

- log on as the root user to the SDM 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.

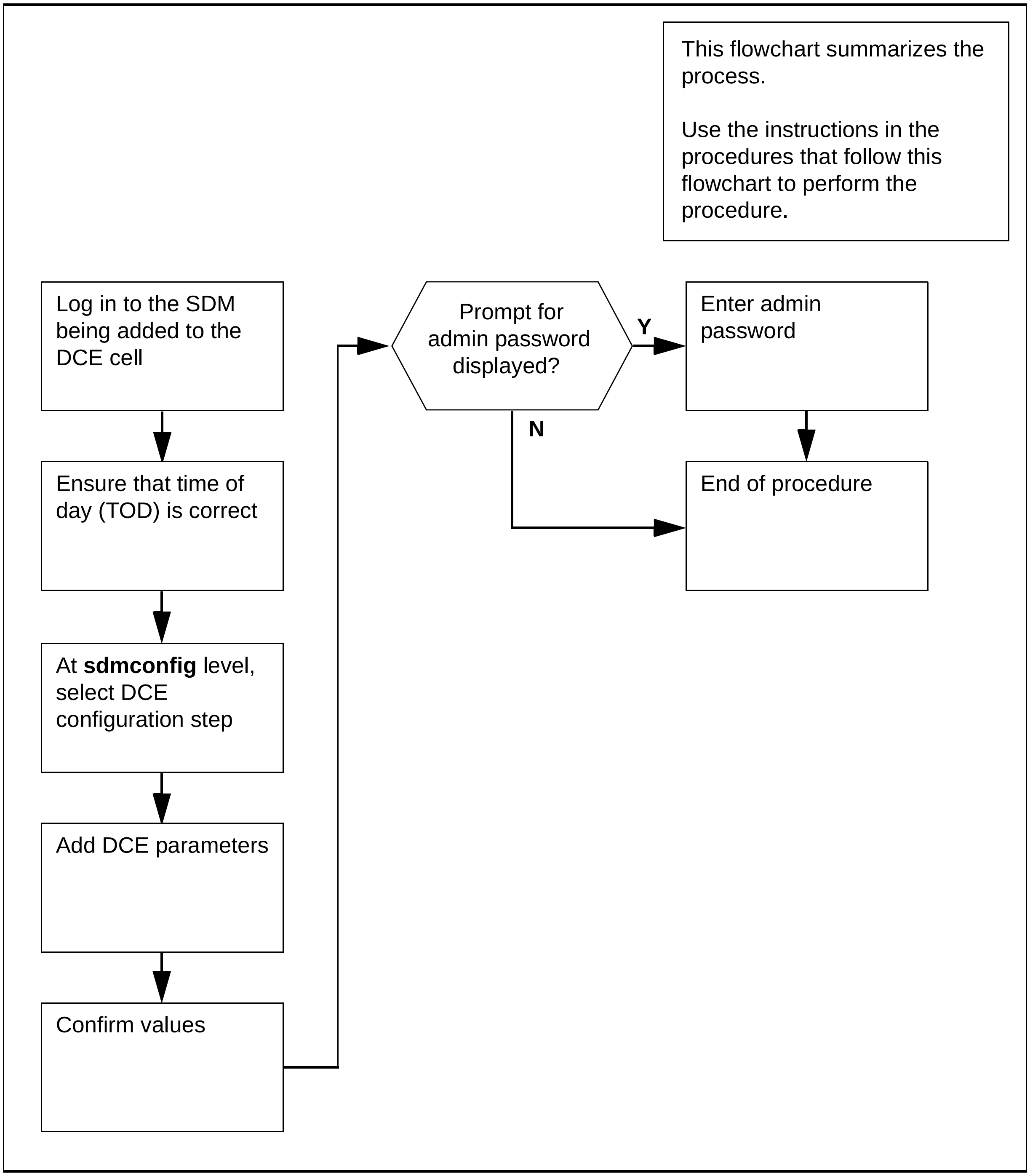
***Note 1:*** You cannot commission DCE until after you have commissioned the LAN. If you try to commission DCE before commissioning the LAN, the system displays an error message. For information about LAN commissioning, refer to the procedure “Commissioning SDM-LAN connectivity”.

***Note 2:*** If you are configuring NTP with DCE on the SDM, 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 an SDM in a DCE cell



# Procedure

### Configuring an SDM in a DCE cell

#### *At the local or remote VT100 console*

**1** Log in as the root user to the SDM you are adding to the DCE cell.

**2** Display the time of day (TOD) of the SDM:

```
# date
```

**3** Compare the TOD displayed in step 2 with the TOD obtained from a reference time signal, adjusted for the SDM 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 SDM 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 SDM | Yes | The name of the DCE LAN profile that supports the part of the cell where the SDM exists. The LAN profile defines the local DTS servers that provide time synchronization for DCE nodes.<br><br>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 SDM.

> **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 SDM: “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).

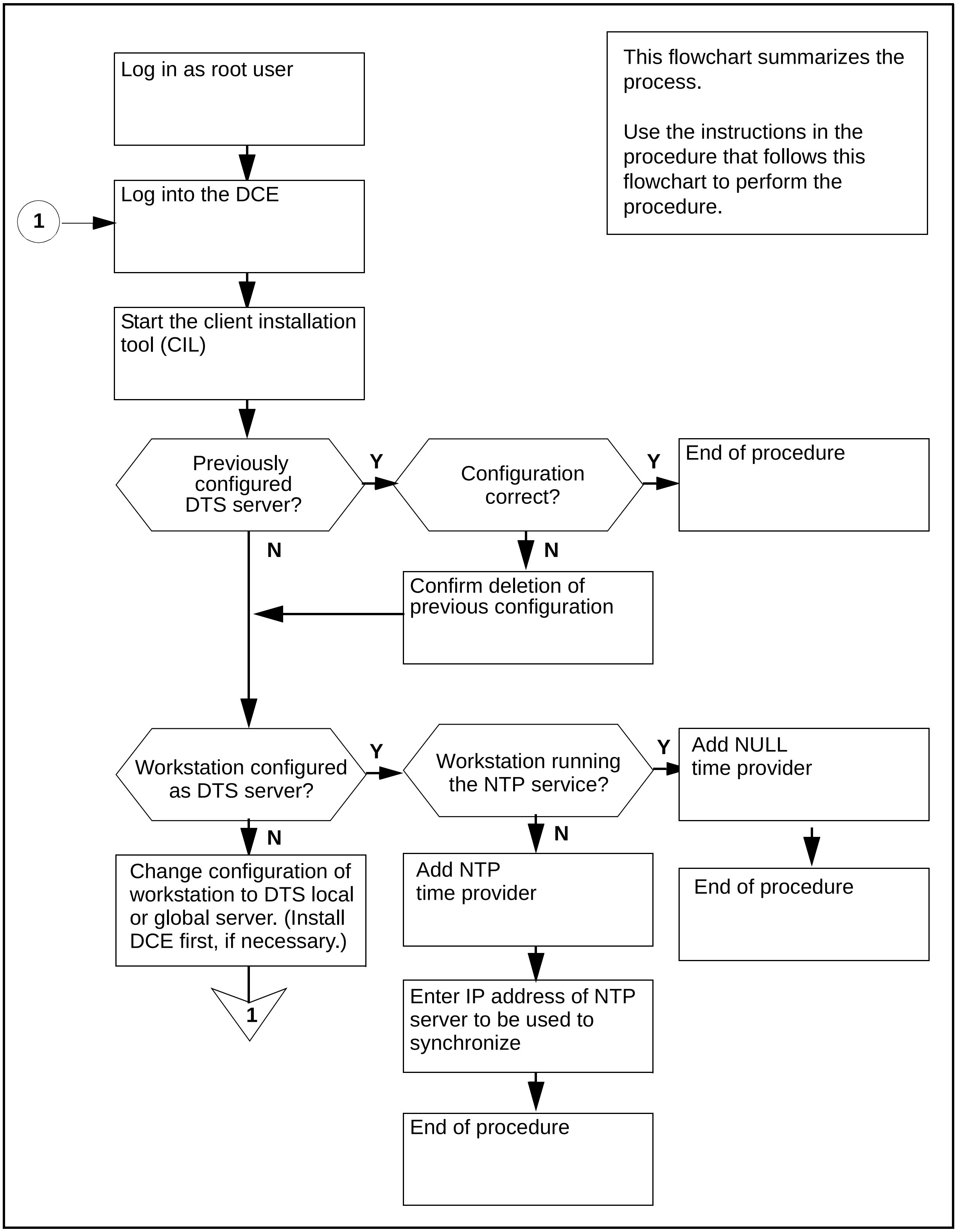
## Prerequisites

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 126.

## 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



### 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 SDM DTS Provider fileset

**5** At the prompt, enter

**> <ip_address>**

*where:*
**<ip_address>** is the address of the SDM where the DTS Provider fileset is installed

*Response:*

The system displays the list of client filesets on the SDM.

**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 SDM 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 an SDM application needs from the master server to the backup server.

## Prerequisites

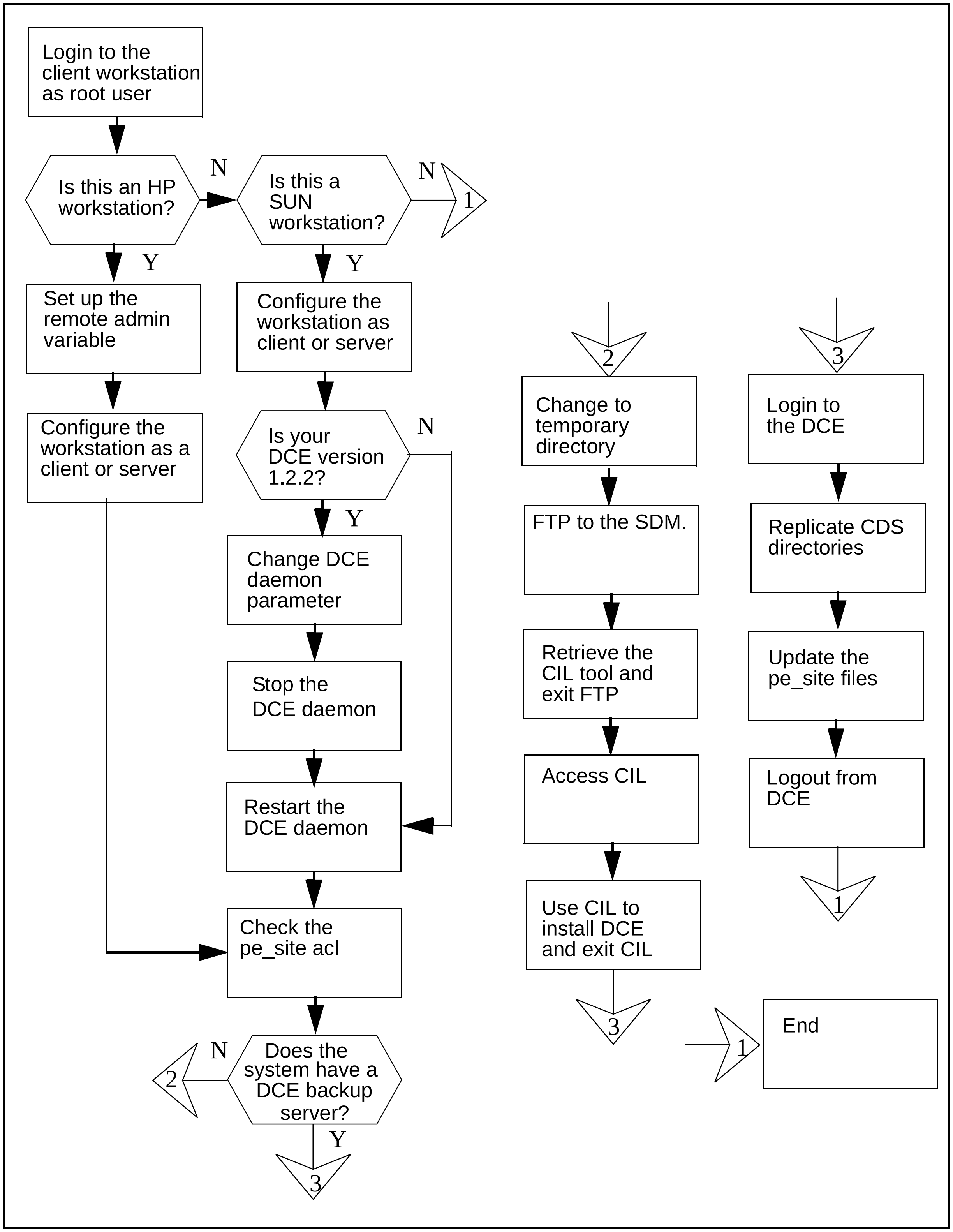
**ATTENTION**
This procedure can only be performed if your operating system is HP-UX or SunOS. If you are using a different operating system, do not attempt to perform this procedure.

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



# 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 an SDM which 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 SDM.

**25** Log in to the SDM 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 SDM:

```
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 SDM:

```
cil> <sdm_name>
```

*where*

***<sdm_name>***
is the IP address or the host name of the SDM.

**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 an SDM hard disk drive.

### Prerequisites

The following procedure applies to an initial installation of the SFT fileset only. You must have root user access to the SDM to perform this procedure.

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

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

**ATTENTION**
If you use the DCE-based SFT application, make sure that the SDM is configured in the DCE cell before performing this procedure. Refer to the procedure Configuring an SDM in a DCE cell on page 78.

**ATTENTION**
Before you can perform an installation, ensure that the FTPProxy 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.

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 SDM 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 Networks recommends that you execute the command from a terminal attached to the SDM console port.

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

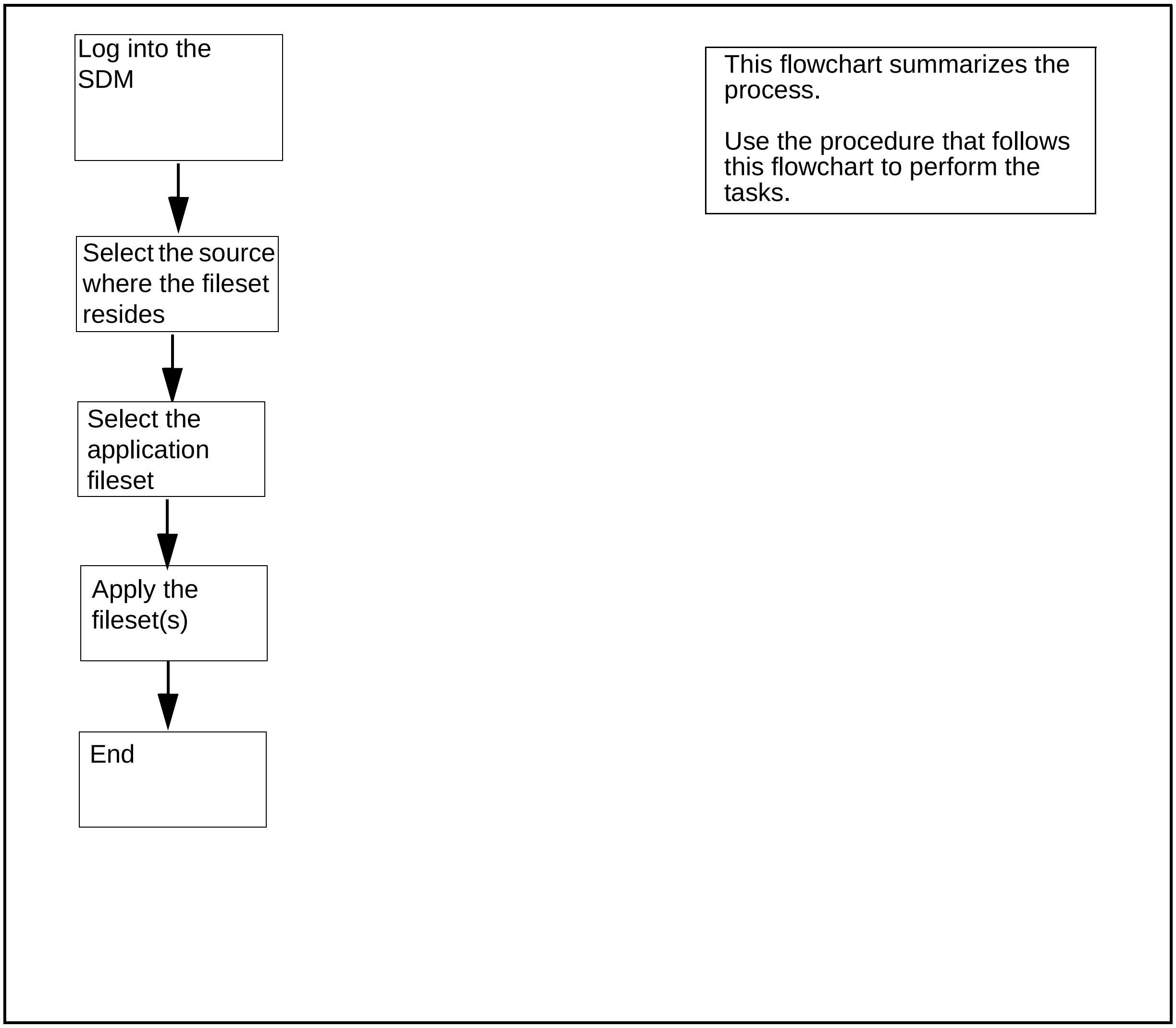
The sub-administrator account requires the following privileges:

- quota to create principals
- add permission for the SDM 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




## Procedure

### Installing the SFT server software

***At the local or remote VT100 console***

**1** Log into the SDM as the root user.

**2** Access the maintenance interface:

```
# sdmmtc
```

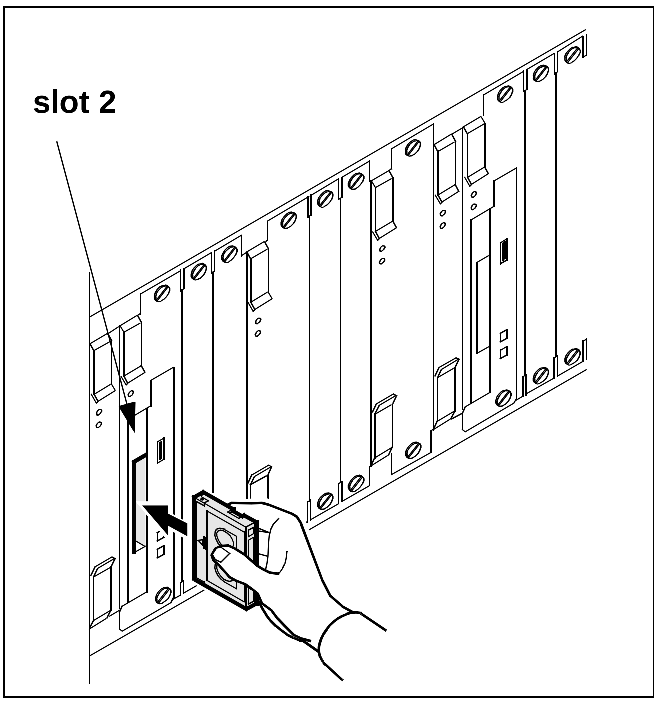
**3** Access the SWIM level:

```
> 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<br>***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 SDM 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 Networks 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.

Nortel Networks recommends that you configure the SFT server application for secure access. Using a non-secure mode can compromise the security of the SDM.

## 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 SDM did not configure the software when you applied the fileset using the procedure Installing the SFT server software on page 103.

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

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

### Anonymous FTP

Anonymous FTP access allows client workstations to access the SDM by logging in as *anonymous*, or *ftp*. The client workstation does not require a root user name and password. The client workstation only has access to the SDM, 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 SDM.

### Normal FTP

Normal FTP access allows client workstations to access the SDM 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 SDM 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<br>Normal<br>Secured | |
| `Anon:Y;Normal:Y;Secured:N` | Anonymous<br>Normal | Secured |
| `Anon:Y;Normal:N;Secured:N` | Anonymous | Secured<br>Normal |
| `Anon:N;Normal:N;Secured:N` | | Secured<br>Anonymous<br>Normal |
| `Anon:N;Normal:N;Secured:Y` | Secured | Anonymous<br>Normal |

**Possible combinations of options for SFT FTP**

| FTP Configuration | Enabled FTP option(s) | Disabled FTP option(s) |
|---|---|---|
| `Anon:N;Normal:Y;Secured:Y` | Normal<br>Secured | Anonymous |
| `Anon:Y;Normal:N;Secured:Y` | Anonymous<br>Secured | Normal |
| `Anon:N;Normal:Y;Secured:N` | Normal | Anonymous<br>Secured |

When you set SFT access on the SDM, you are configuring all FTP type interaction with the SDM. SFT in secure access mode provides a secure operating environment. Anonymous or normal FTP access provides standard FTP access, which is insecure, to the SDM. To avoid sending login, password, and files unsecured over the network, enable *secured* mode and use the SFT client.

## Prerequisites

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 SDM platform maintenance software and the SFT software package. You must have root user access to the SDM.

**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 SDM within the DCE cell.

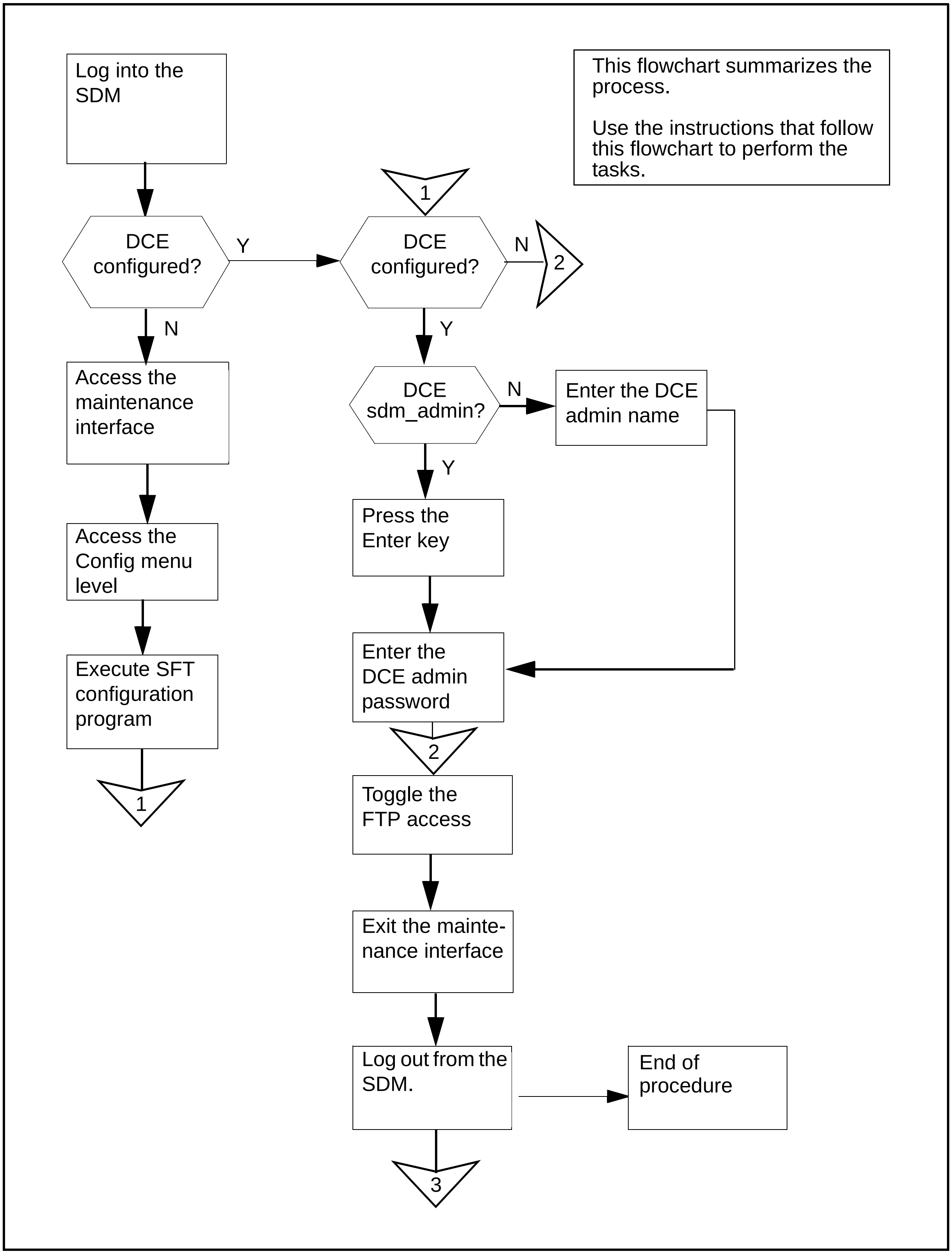
The sub-administrator account requires the following privileges:

- quota to create principals
- the ability to add permission for the SDM 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



## 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 SDM 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 Networks recommends that you execute the command from a terminal attached to the SDM console port.

Log into the SDM as root user.

**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 SDM, 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 SDM 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 SDM:

```
# 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 SDM 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**

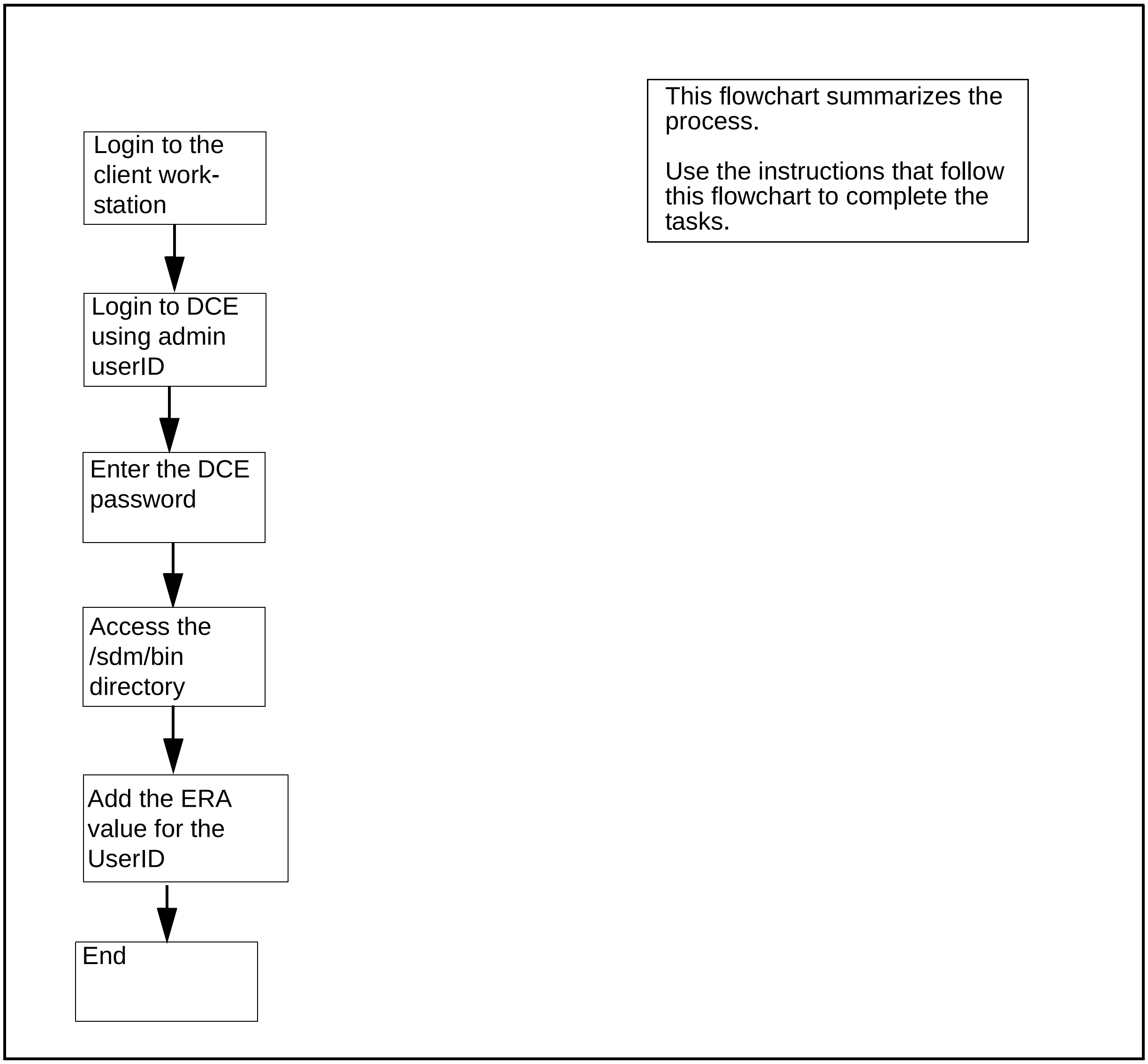
The DCE administrator must create and configure the DCE user accounts before a user can access the SFT servers using the SFT clients. If you are using SFT in FTP (non-DCE) mode, ignore this section.

## Task flow diagrams

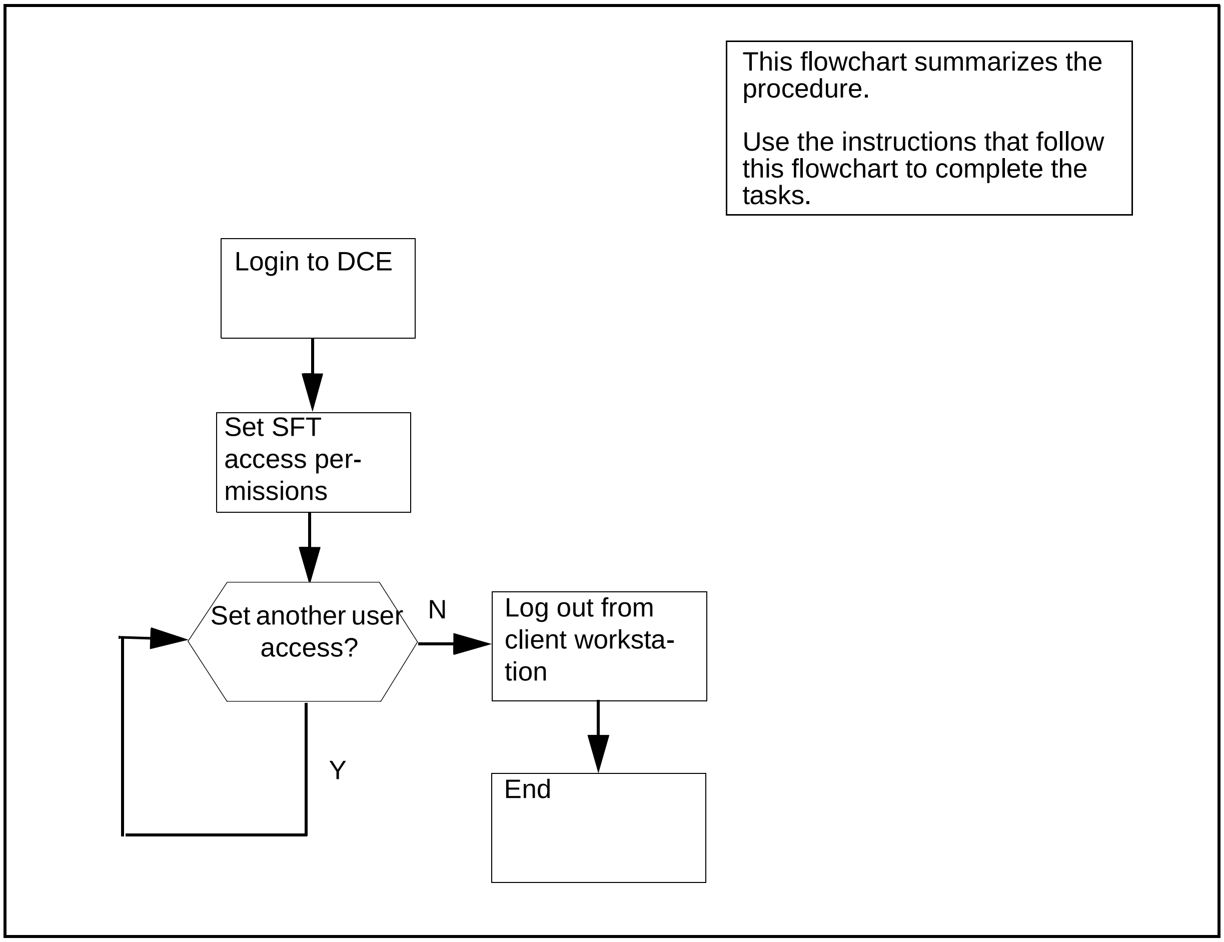
The following task flow diagrams summarize the process. Use the instructions in the procedures that follow the flow charts to complete the tasks.

- setting an ERA value for an SDM userID
- setting the SFT access permissions

## Task flow for Setting an ERA value for the SDM userID



### Task flow for Setting the SFT access permission




# Procedures

## Setting an ERA value

To set an ERA value for the SFT client SDM userID, use the add_sdm_userid command. When an SFT client accesses the SDM, the SFT server obtains the ERA value for that client SDM userID, and uses it to connect the client to the SDM.

### Setting an ERA value for the SDM 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 SDM userID:

```
> ./add_sdm_userid <principal_name>
<sdm_userid>
```

*where*

**<principal_name>**
is the principal name of the DCE user account.

**<sdm_userid>**
is the SDM userID.

***Note:*** The SDM userID must correspond to an existing SDM UNIX account. This account must reside on all of the SDM nodes that you need to access. You cannot use SFT to access the SDM without this SDM UNIX account. You can use either the root or maint account. To use a different account that does not exist, the system administrator with root access privileges must create one.

**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 SDM, or *sdm_cm*, where access is permitted to both the SDM 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

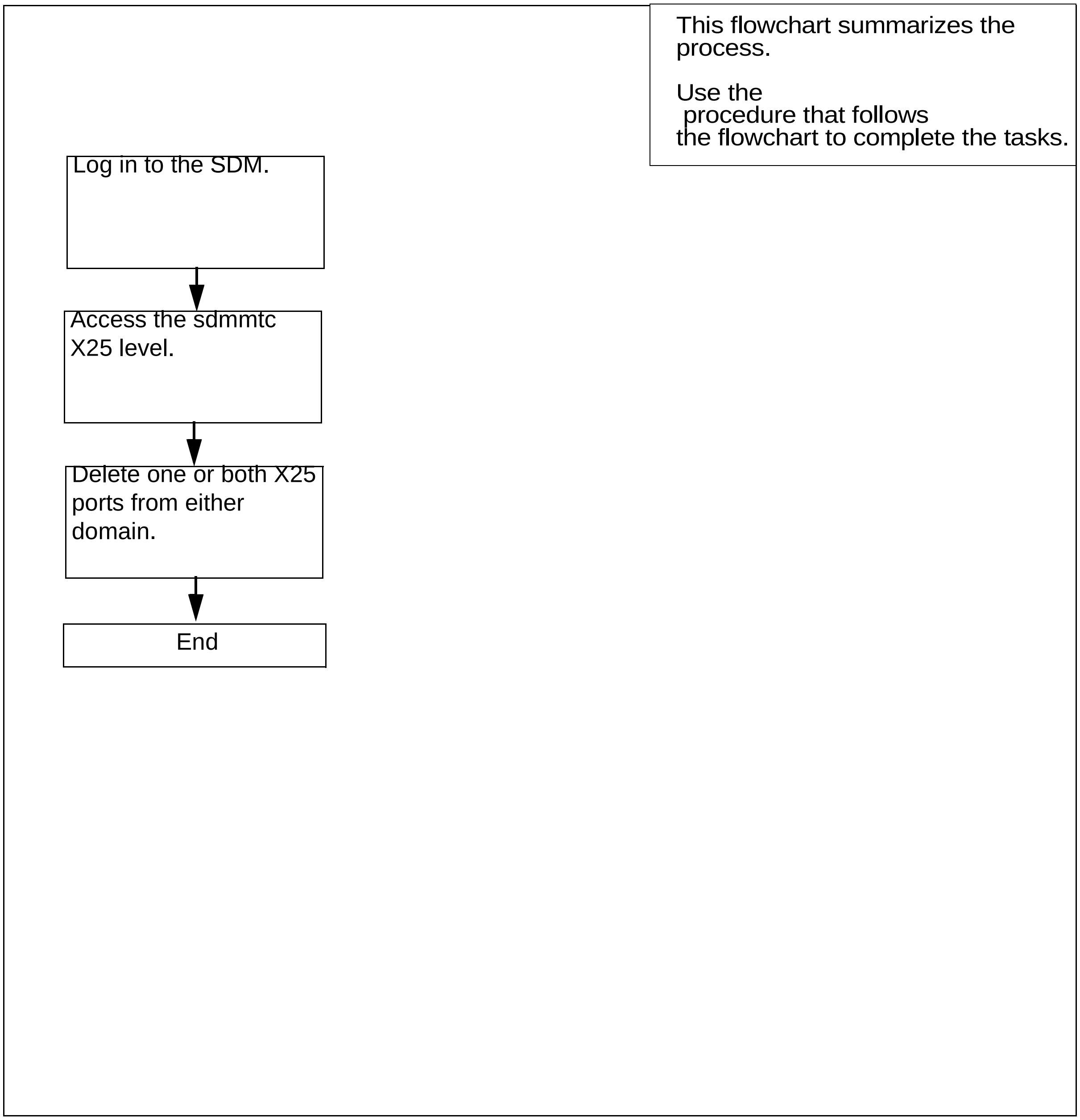
## Purpose

Use this procedure to decommission one or both X.25 ports on an UMFIO/X25 (NTRX50NN) or SYNC X25 (NTRX50FY) module.

## 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




# Procedure

### Decommissioning X.25 ports

***At the local VT100 console***

**1** Log into the SDM as a root user.

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

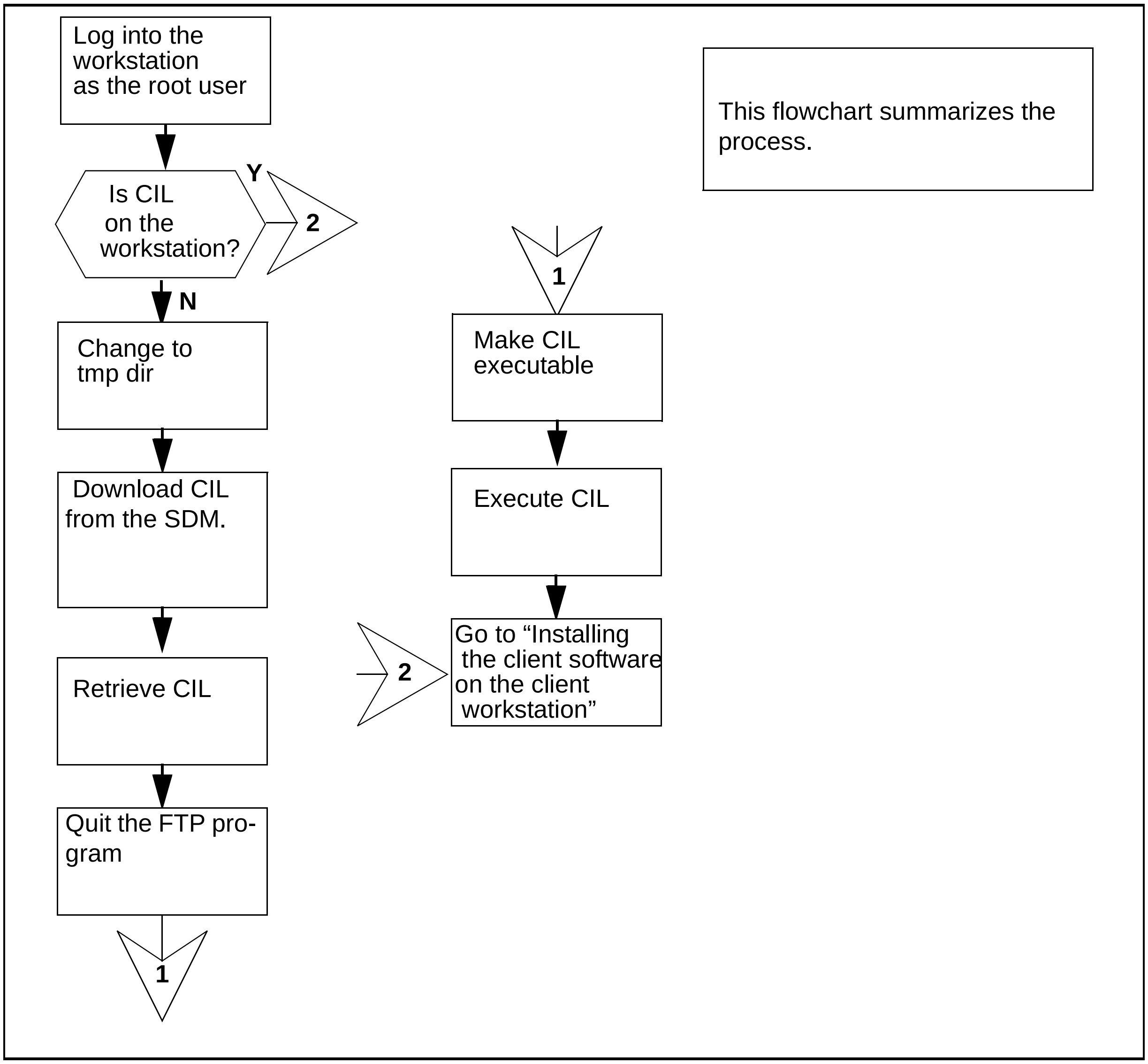
You must have the following information in order to perform this procedure:

- the platform of the client workstations
- the internet protocol (IP) address and root password of the client workstations
- the root user password of the SDM
- the client software fileset names

## 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



## 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 Networks recommends that you execute the commands from a terminal attached to the workstation console port.

Log into the client workstation as the root user.

**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 an SDM:

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

*where*

*<ip-address>*
is the IP address of the SDM.

**4** Log into the SDM 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 SDM:

```
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 133.

# Installing the Base Maintenance Interface software

## Purpose

The following procedure provides instructions on how to install the Base Maintenance Interface software on the SDM.

## Procedure

### Installing the Base Maintenance Interface software

***At the local or remote VT100 console***

**1** Log into the SDM as root user.

**2** Access the maintenance interface level:

**# sdmmtc**

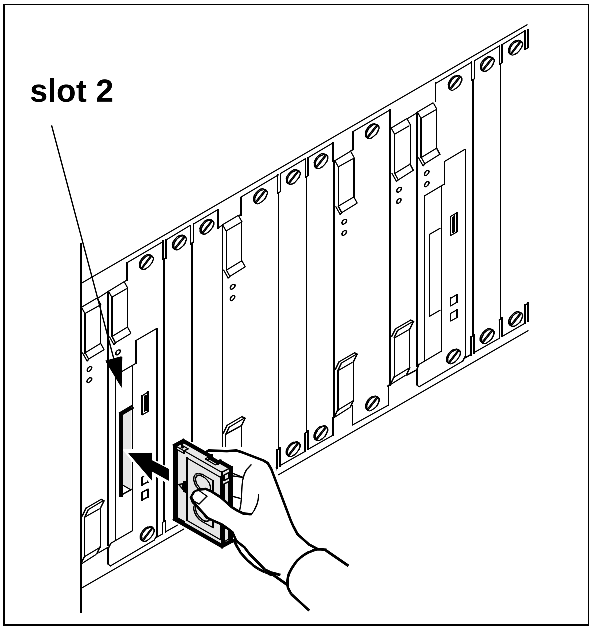
**3** Access the SWIM level:

**> 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<br><br>***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 SDM 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 126.

> **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.

**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 SDM:

**SDM's Address: <*sdm*_name>**

*where*

***<sdm_name>***
is the IP address or the host name of the SDM

*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

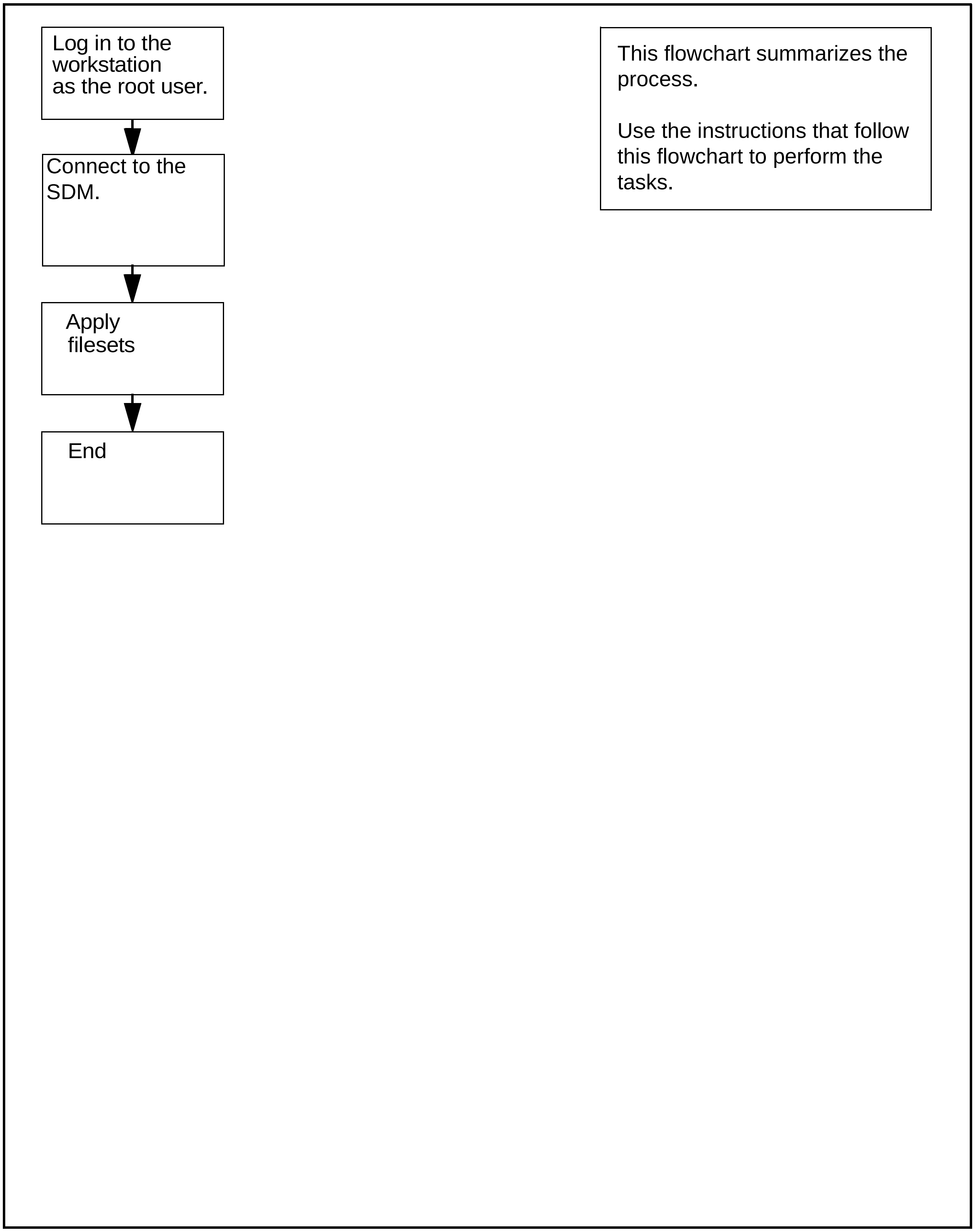
## Purpose

Use this procedure to install the logreceiver tool on a client workstation. The procedure accesses the logreceiver software stored on the SDM 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



## 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 Networks 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 SDM:

**SDM's Address: <*sdm*_name>**

*where*

***<sdm_name>***
is the IP address or the host name of the SDM.

*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 SDM 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 SDM before executing this procedure.

Use the following procedure to install or upgrade the OMD application.

**Installing and configuring OM Delivery software**

***At the local or remote VT100 console***

**1** Log into the SDM as root user.

**2** Access the maintenance interface by typing

```
# sdmmtc
```

and pressing the Enter key.

**3** Access the SWIM level by typing

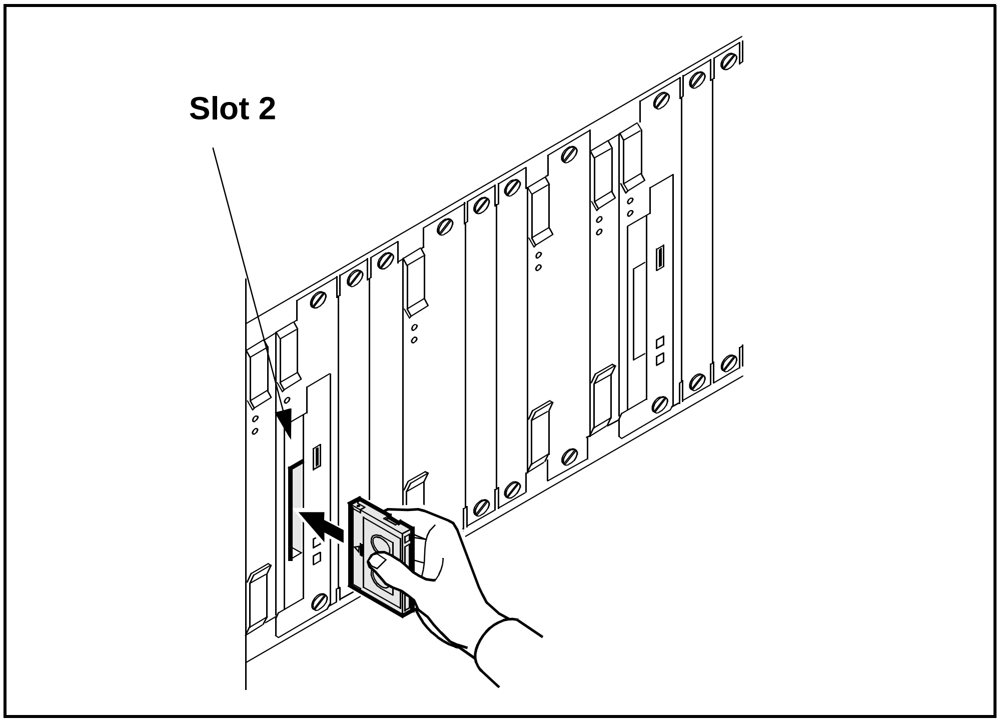
```
> swim
```

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<br>***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** Exit the maintenance interface by typing

**> quit all**

and pressing the Enter key.

**15** You have completed this procedure.

# Installing the CMFT on a client workstation

## Purpose

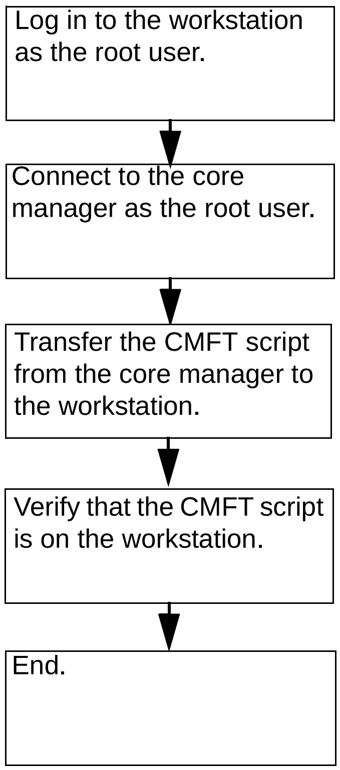
Use this procedure to install the Command Module File Transfer script (CMFT) on a client workstation. This procedure copies the CMFT from the Command Module (CM) to a specified directory location on the client workstation. The CMFT script allows you to use SCFT (SSH Core File Transfer) to transfer files to and from the CM. SCFT is discussed in NN10362-611, Administration and Security.

***Note:*** SCP must be installed before you can install CMFT.

## 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




This flowchart summarizes the process.

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

## Procedure

### Installing the CMFT on a client workstation

### At the local or remote VT100 console

**1** Log in to the client workstation as the root user.

**2** Log in to the core manager as a root user

**3** Get the CMFT script from the core manager:

```
> scp
root@<coremanager_ip_address>:/sdm/scft/cmft .
```

where

**<coremanager>**
is the core manager node name or ip address

**4** Verify that you have successfully transferred the CMFT script

```
> ls -l cmft
```

Response

The client workstation displays the CMFT script.

**5** You have completed this procedure.

# Installing SCFT

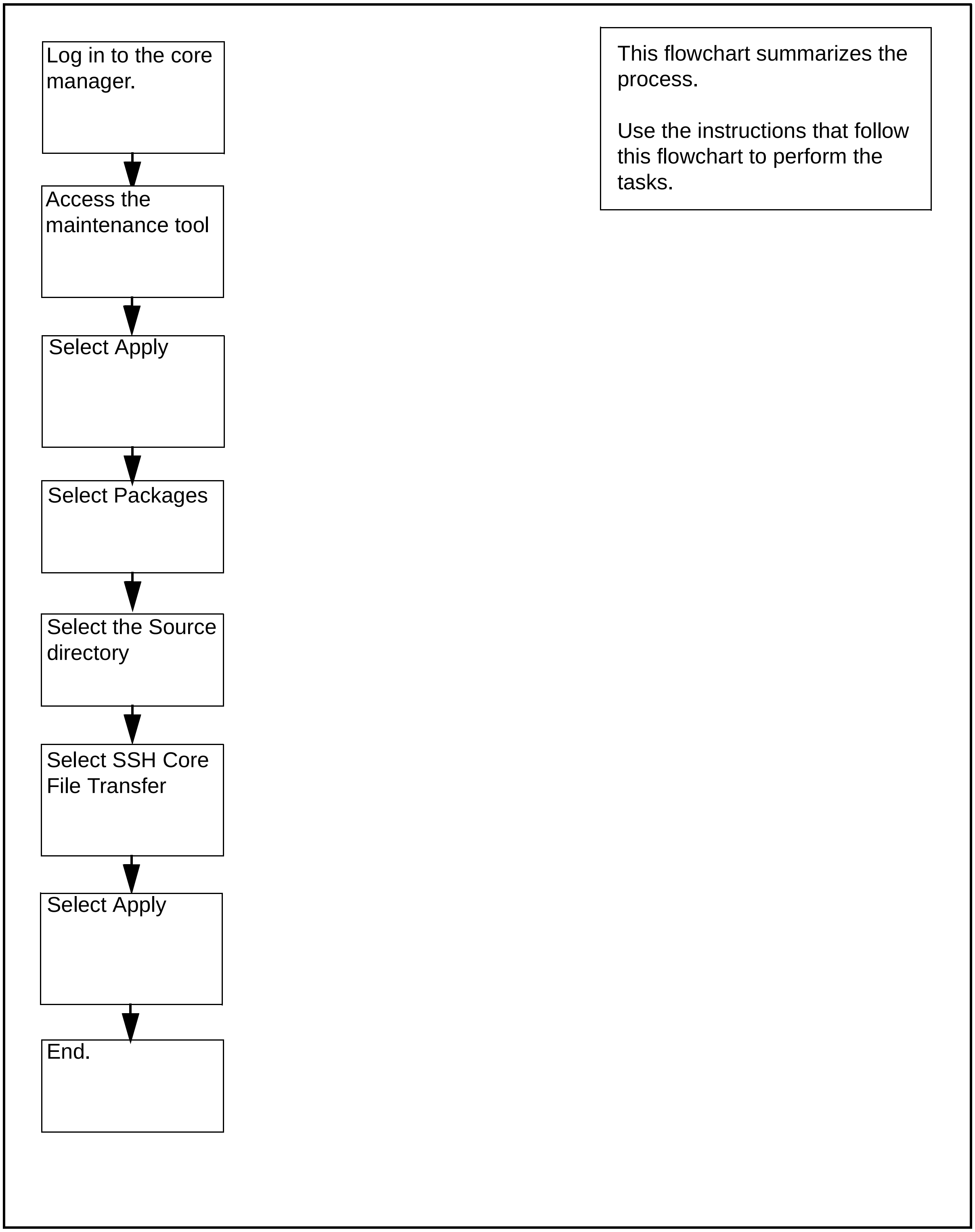
## Purpose

Use this procedure to install SCFT (SSH Core File Transfer). SCFT allows you to use secure FTP to access the Core. SCFT usage is discussed in NN10362-611, Security and Administration.

## 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 SCFT



# Procedure

### Installing SCFT

### At the local or remote VT100 console

**1** Log in to the core manager. Use the maint user ID and password, then

switch user (**su** ) to root using the root ID and password.

**2** Access the cbmmtc interface:

**# sdmmtc**

**3** Go to the apply level of the cbmmtc interface:

**# apply**

**4** Select **<n>**

where

**<n>**
is the number next to the SSH Core File Transfer selection

**5** Select the default source for the directory path on the core: /data/swd/sdm

**6** Apply this selection:

**# apply**

**7** A dialog will prompt you to confirm your selection:

Do you wish to proceed?

Please confirm ("YES", "Y", "NO", or "N")

Type **Y** to confirm your selection.

The system will execute your request. A dialog will then confirm the successfull execution of your selection.

**8** You have completed this procedure.

# Removing SCFT

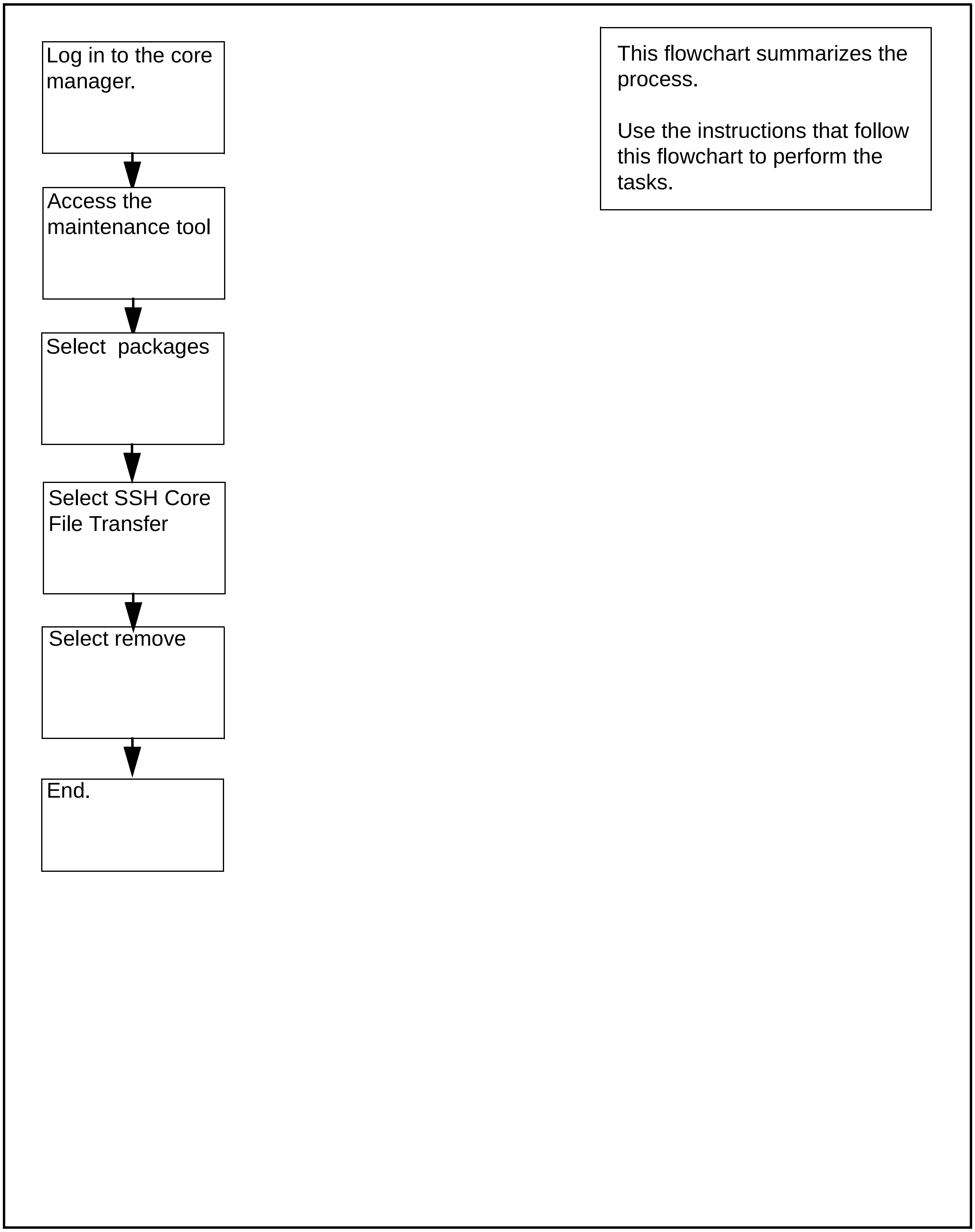
## Purpose

Use this procedure to remove SCFT (SSH Core File Transfer). SCFT allows you to use secure FTP to access the Core. SCFT usage is discussed in NN10362-611, Administration and Security.

## 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 removing SCFT



## Procedure

### Removing SCFT

### At the local or remote VT100 console

1 Log in to the core manager. Use the maint user ID and password, then

switch user (**su** ) to root using the root ID and password.

2 Access the cbmmtc interface:

**# sdmmtc**

3 Go to the apply level of the cbmmtc interface:

**# apply**

4 Select **<n>**

where

**<n>**
is the number next to the SSH Core File Transfer selection

5 Remove the selection:

**# remove**

6 A dialog will prompt you to confirm your selection:

Do you wish to proceed?

Please confirm ("YES", "Y", "NO", or "N")

Type **Y** to confirm your selection.

The system will execute your request. A dialog will then confirm the successfull execution of your selection.

7 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 SDM, 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 SDM 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 Networks recommends that you execute the commands from a terminal physically attached to the SDM 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 SDM on page 71.

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 SDM 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 SDM

## Prerequisites

To perform this procedure, you must have a DCE account with administrative privileges and root user access to the SDM.

## Procedures

### Removing an ETA server from a DCE cell

***At the local or remote VT100 console***

**1** Log into the SDM 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 SDM:

**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 |

| If the list | Do |
|---|---|
| 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 SDM resides.

***clli***
is the Common Language Location Identifier (CLLI) of the switch to which the SDM 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 SDM resides

***clli***
is the Common Language Location Identifier (CLLI) of the switch to which the SDM is connected.

11 Delete the key table:

**dcecp> key delete eta**

12 Remove the principal for the SDM application server:

**dcecp> principal delete sdm/<*clli*>/eta-server**

*where*

***clli***
is the CLLI of the switch to which the SDM 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 SDM, use the procedure Removing an ETA server from a SDM.

**Removing an ETA server from a** SDM

***At the local or remote VT100 console***

**1** Ensure that you are logged into the SDM as the root user.

**2** Access the maintenance interface:

**# sdmmtc**

**3** Access the SWIM level:

**> swim**

**4** 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.

**5** Delete the filesets:

**> 8 or remove**

**6** 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.

**7** Exit the maintenance interface:

**> quit all**

**8** Log out from the SDM:

**> exit**

**9** You have completed this procedure.

# Removing an SDM 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 SDM from another computer. Nortel Networks recommends that you execute the command from a computer attached to the SDM console port to maintain password security.

If you are taking the SDM out of service permanently, you must remove the SDM from the DCE cell. You can remove the SDM 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.

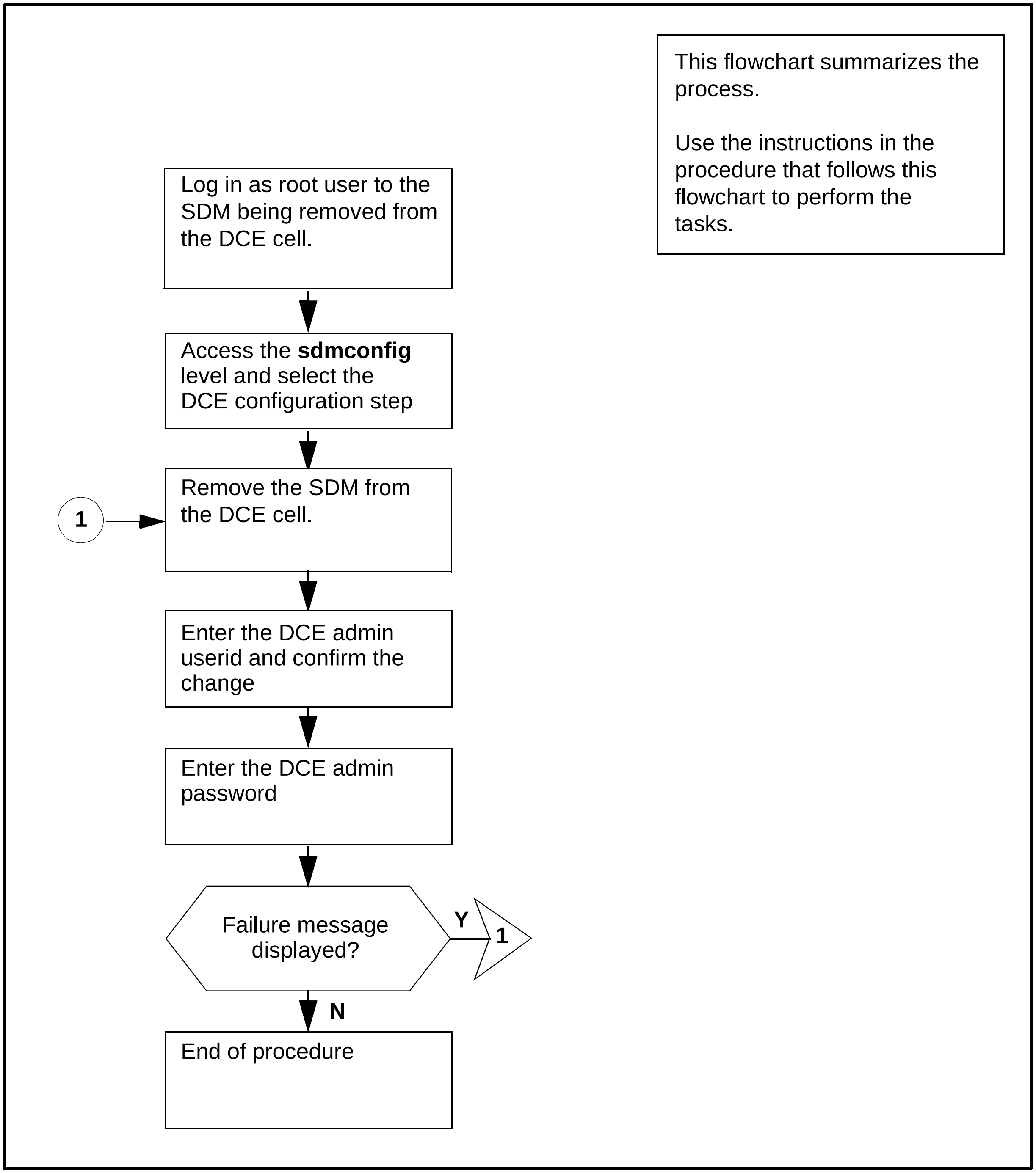
The cell_admin principal can also create a sub administrator account (default is sdm_admin) with limited privileges for the purpose of maintaining SDMs in the DCE cell. If you decide to create a sub administrator account, refer to the DCE procedure “Creating SDM administration account”.

**CAUTION**
**Possible failure to remove DCE**
You cannot use the sdm_admin account to remove DCE from an SDM 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 an SDM from a DCE cell



## Procedure

### Removing an SDM from a DCE cell

***At the local or remote VT100 console***

**1** Log in as root user to the SDM 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 SDM, 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 SDM.

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 103.

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 SDM 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 SDM 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 Networks recommends that you execute the commands from a terminal physically attached to the SDM console port.

## Prerequisites

To perform this procedure, you must have a DCE account with administrative privileges and root user access to the SDM.

### Removing an SFT server

#### *At the local or remote VT100 console*

**1** Log into the SDM 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 SDM:

**`dcecp> key catalog -simplename`**

**6** Determine whether the key table list contains a key table called eta.

| If the list | Do |
|---|---|
| contains the sft key table | step 7 |
| does not contains the sft key table | step 12 |

**7** List the principals that are supported by the key table:

```
dcecp>key list sft
```

**8** The list from the command executed in step 7 must contain entries that follow the format: /.../cell name/sdm/clli/principal name.

*where*

***cell name***
is the cell in which the SDM resides.

***clli***
is the Common Language Location Identifier (CLLI) of the switch to which the SDM 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 SDM resides

***clli***
is the Common Language Location Identifier (CLLI) of the switch to which the SDM is connected.

**11** Delete the key table:

```
dcecp> key delete sft
```

**12** Remove the principal for the SDM application server:

```
dcecp> principal delete sdm/<clli>/sft-server
```

*where*

***clli***
is the CLLI of the switch to which the SDM 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 SDM:

**> exit**

**22** You have completed this procedure.

# Restricting the SFT port range

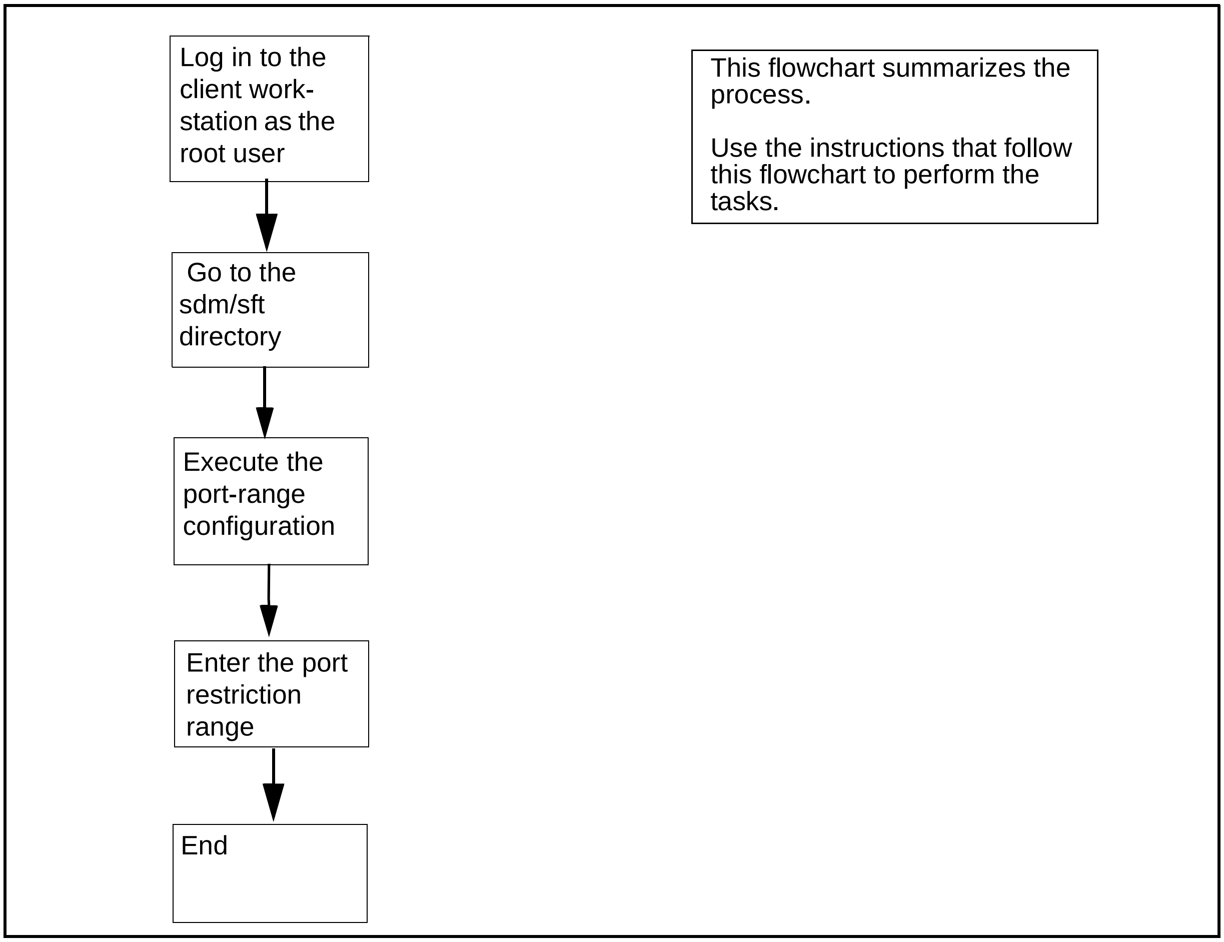
## Purpose

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



## 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 Networks recommends a range of at least 20 ports (b-a >= 20).

**5** Exit the program:

**`> exit`**

**6** You have completed this procedure.

# Configuring the SDM to communicate with a call agent

## Purpose

This procedure describes how to add or change the Ethernet and LANCOMM IP addresses on the SDM to communicate with a call agent. It assumes that the latest software release is already installed on the SDM.

## Prerequisites

The prerequisites for successful configuration are:

- you must have root access to the SDM
- table IPNETWRK must contain the LANCOMM stack IP address

## Procedure

**Configuring the SDM to communicate with a call agent**

***At the SDM***

**1** Login to the SDM as the root user.

**2** Access the Maintenance level of the maintenance interface:

```
# sdmmtc mtc
```

**3** Verify the state of the SDM under SDM in the top banner.

| If the SDM is | Do |
|---|---|
| Offl or ManB | step 6 |
| InSv or ISTb | step 4 |
| SysB | contact your next level of support |

**4** Busy the SDM:

```
> 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 SDM for the first time | step 9 |
| reconfiguring the SDM | 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 SDM to service | step 14 |
| you need to perform other tasks on the SDM | step 17 |

**14** Access the maintenance level:

`> mtc`

**15** Return the SDM 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 an SDM

## Purpose

Use this procedure if you want to delete a file system that you previously defined on the SuperNode Data Manager (SDM).

## Procedure

**Deleting a file system on an SDM**

***At the local VT100 console***

**1** Log on to the SDM 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 can result in the SDM rebooting if devices are connected, and they take a power spike.

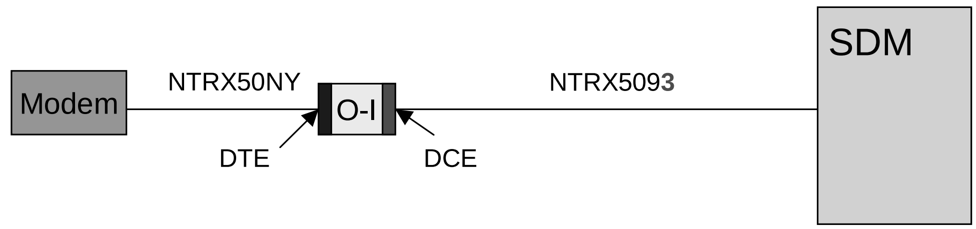
Refer to the following table to determine which procedure you should use to change console connections with O-I.

| 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 173 |
| 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 175 |

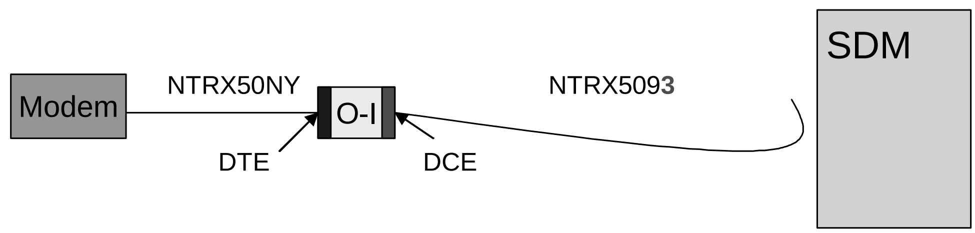
### Changing from a remote to a local console connection with O-I

***At the SDM***

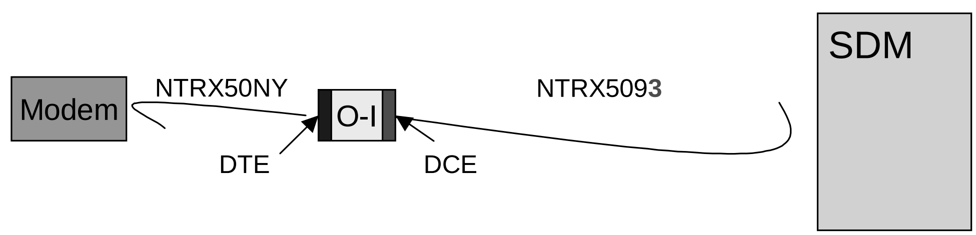
**1** The following figure shows an existing remote console connection. Be sure that you are familiar with the configuration, then go to step 2.



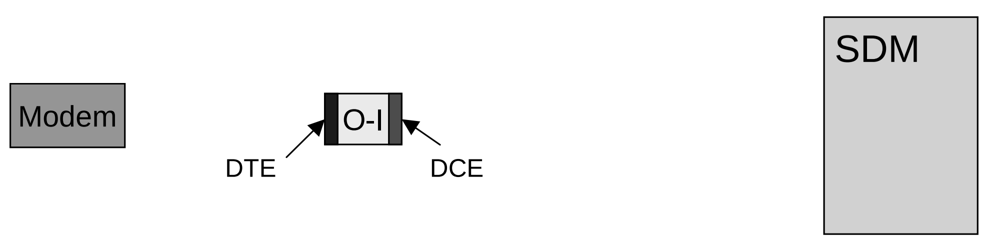

**2** Disconnect the NTRX5093 from SP0.



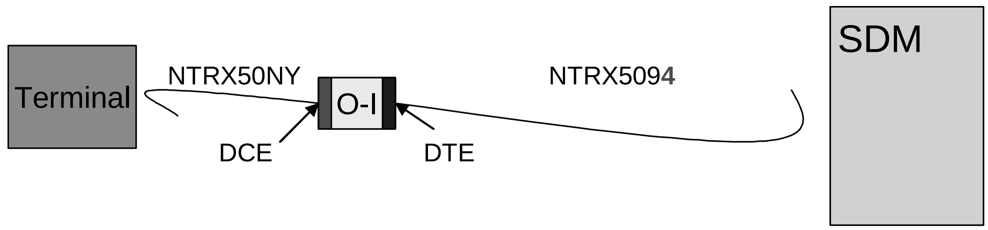

**3** Disconnect the NTRX50NY from the modem.



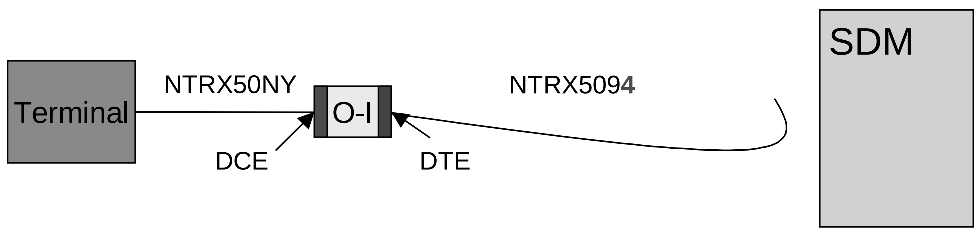

**4** Disconnect NTRX50NY from the DTE side of the O-I, and NTRX5093 from the DCE side of the O-I.



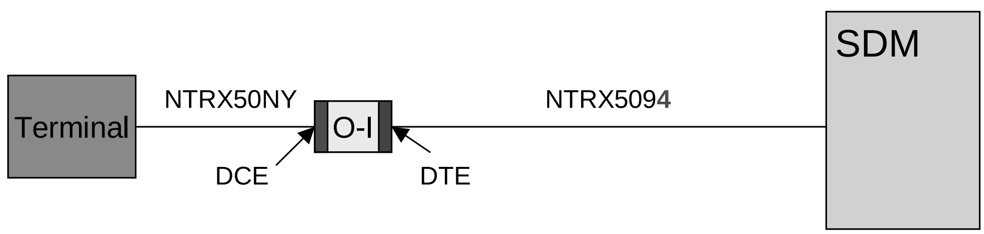

**5** Connect the NTRX50NY to the DCE side of the O-I. Connect the NTRX5094 to the DTE side of the O-I.




**6** Connect the NTRX50NY to the terminal.




**7** Connect the NTRX5094 to SP0.

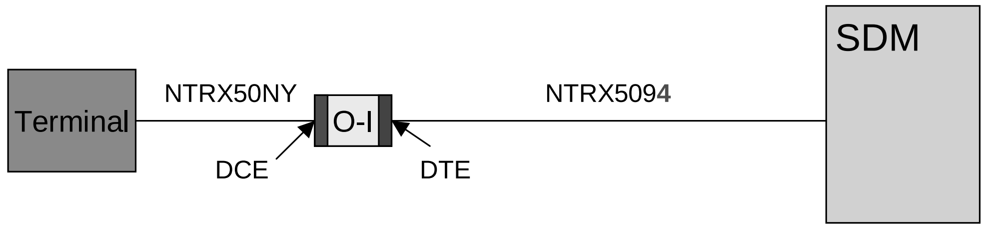



**8** You have completed this procedure.

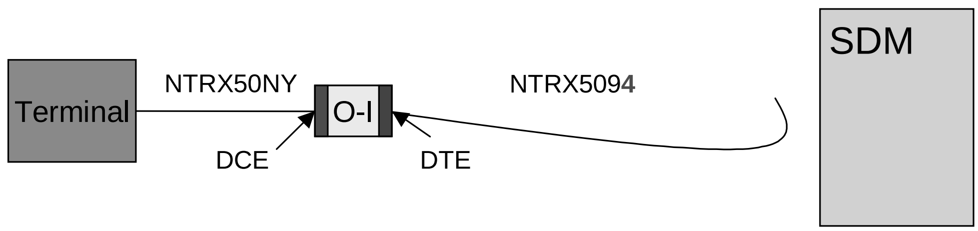
### Changing from a local to a remote console connection with O-I

#### *At the SDM*

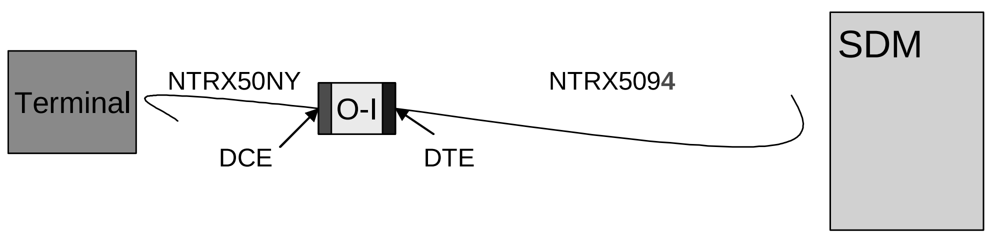
**1** The following figure shows an existing local console connection. Be sure that you are familiar with the configuration, then go to step 2.



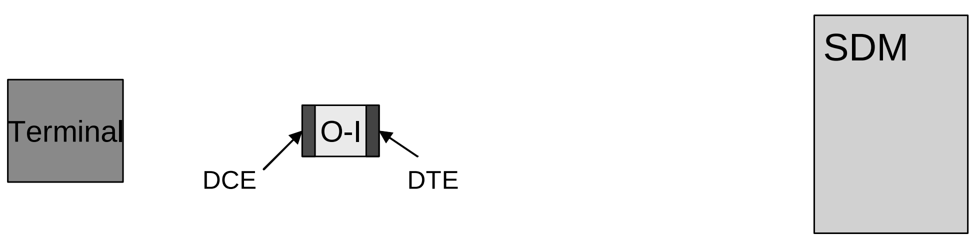

**2** Disconnect the NTRX5094 from the SP0.



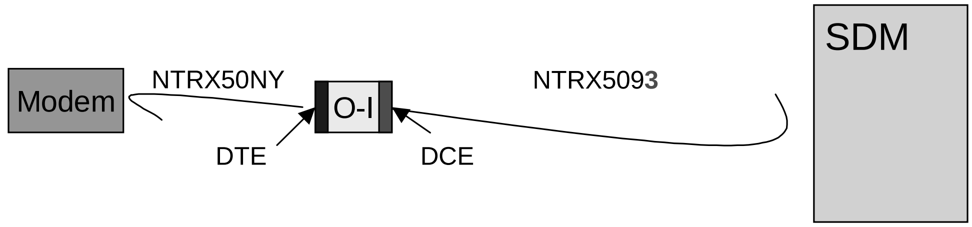

**3** Disconnect the NTRX50NY from the terminal.



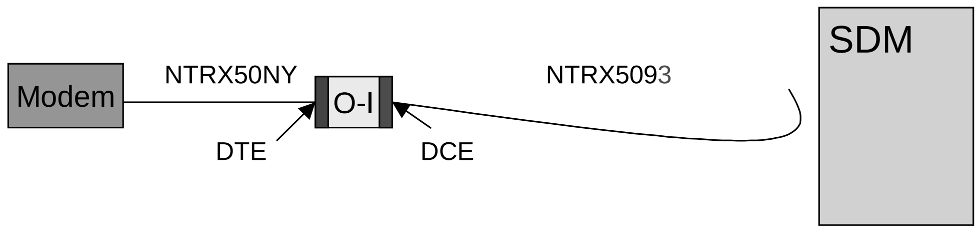

**4** Disconnect NTRX50NY from the DCE side of the O-I and NTRX5094 from the DTE side of the O-I.



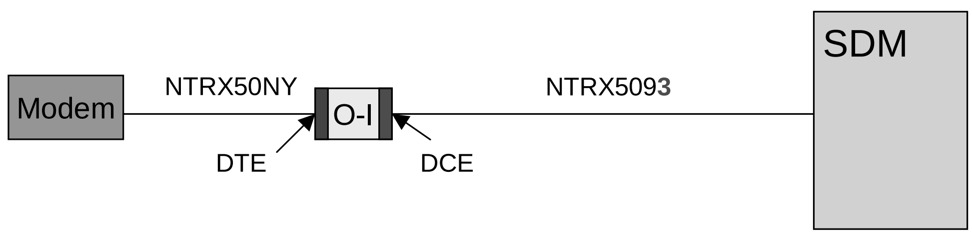

**5** Connect the NTRX50NY to the DTE side of the O-I. Connect the NTRX5093 (SDM modem cable) to the DCE side of the O-I.




**6** Connect the NTRX50NY to the modem.




**7** Connect the NTRX5093 to SP0.




**8** You have completed this procedure.