SDM Security and Administration

This document describes the administration and security features and operating procedures for the SuperNode Data Manager (SDM).

Administration and security strategy

The SDM provides security and administration management for the DMS.

Administration and security procedures

Use the SDM to perform the following tasks:

- create an administration account
- create ATA user accounts
- manually create system image backup tapes (S-tapes)
- schedule system image backups
- enable/disable system backup alarm
- start an SCFT client session
- transfer files from Core using SCFT
- transfer files to Core using SCFT
- remove files from Core using SCFT
- display help for SCFT
- create a DCE user
- connect the Core with ATA
- connect the Core with ETA
- connect to the SDM with ATA
- connect to the SDM with ETA
- connect to the SDM with SDMRLOGIN
- connect to another node as a passthru user
- add CM userIDs and passwords for ETA and ATA clients

- add disks and create logical volume in datavg
- add or remove a maintenance user
- add or remove passthru users
- add SDM userIDs and passwords for ETA and ATA clients
- assign the master server for DCE
- remove ERA values for CM userIDs and passwords
- remove DCE port restrictions
- remove the ERA value for the userID
- restrict DCE ports to a predefined range
- restrict DCE ports to a specific range
- set SFT access permissions
- set the time zone, or date and time
- start an FTP client
- transfer files as a passthru user using FTPProxy
- transfer files as a core user using FTPProxy
- transfer and retrieve files using SFT
- change the system time zone and daylight saving time parameters
- use an FTP client
- allow ATA and ETA to operate across a firewall
- change a DCE user password
- change a user password on the SDM
- change a user password on a Sun server
- change a passthru user password
- change CM passwords from ATA client
- change CM passwords from ETA client
- change logical volume thresholds
- change system thresholds
- recover the system when root password is unknown
- recommission date and time zone
- change the system date and time
- transfer files as a passthru user using FTPProxy
- transfer files as a core user using FTPProxy

- start an SFT session
- stop and restart an application
- delete a DCE user
- establish a modem connection
- get ERA values for CM userIDs
- get the ERA value for SDM userID
- increase the size of logical volume
- manage ETA extended registry attributes
- display the CLLI from the command line
- display the CLLI from BILLMTC
- configure secure outbound transfer of OMs

Application

CAUTION
Possible failure when using sdm_admin account
When you have established your new cell, you must always create an sdm_admin account immediately.

For an existing cell, you can create one or more sdm_admin accounts for the client workstations.Tasks can only be performed successfully by a valid sdm_admin account.

ATTENTION
Do not use the sdm_admin account to configure DCE on a DCE client machine.

The sdm_admin account does not have enough privileges to perform that procedure. Use the cell_admin account to configure or un-configure DCE in a normal DCE client machine except SDM.

Use this procedure to create an administration account. The default name is sdm_admin). You can use the sdm_admin account to perform DCE administration activities related to the SDM. The sdm_admin account only has some of the privileges of a cell_admin account.

This procedure allows you to create an sdm_admin account for SDM administration routine tasks:

- separate the SDM administration tasks from the DCE administration tasks
- prevent a general SDM operator from damaging or deleting the DCE system-wide data

The sdm_admin account can perform the following procedures:

- configure an SDM in a DCE cell
- remove an SDM from a DCE cell
- create a DCE user
- delete a DCE user
- configure an SDM application server

- remove an SDM application server
- manage the extended registry attributes (ERA) of an application
- set access permission for secure file transfer (SFT)
- optionally , erpform like a DCE user account
- optionally, move an SDM from a DCE cell previously configured by a different sdm_admin account

The sdm_admin account cannot:

- delete a DCE user previously created by a cell_admin account
- configure a DCE cell
- assign or reassign a new DCE server

The cell_admin account has the same access privileges as the sdm_admin account. Refer to the corresponding sections when using the sdm_admin or cell_admin accounts to perform any procedure.

Note: The cell_admin account cannot start client applications.

The following conditions must be met before you can create an sdm_admin account:

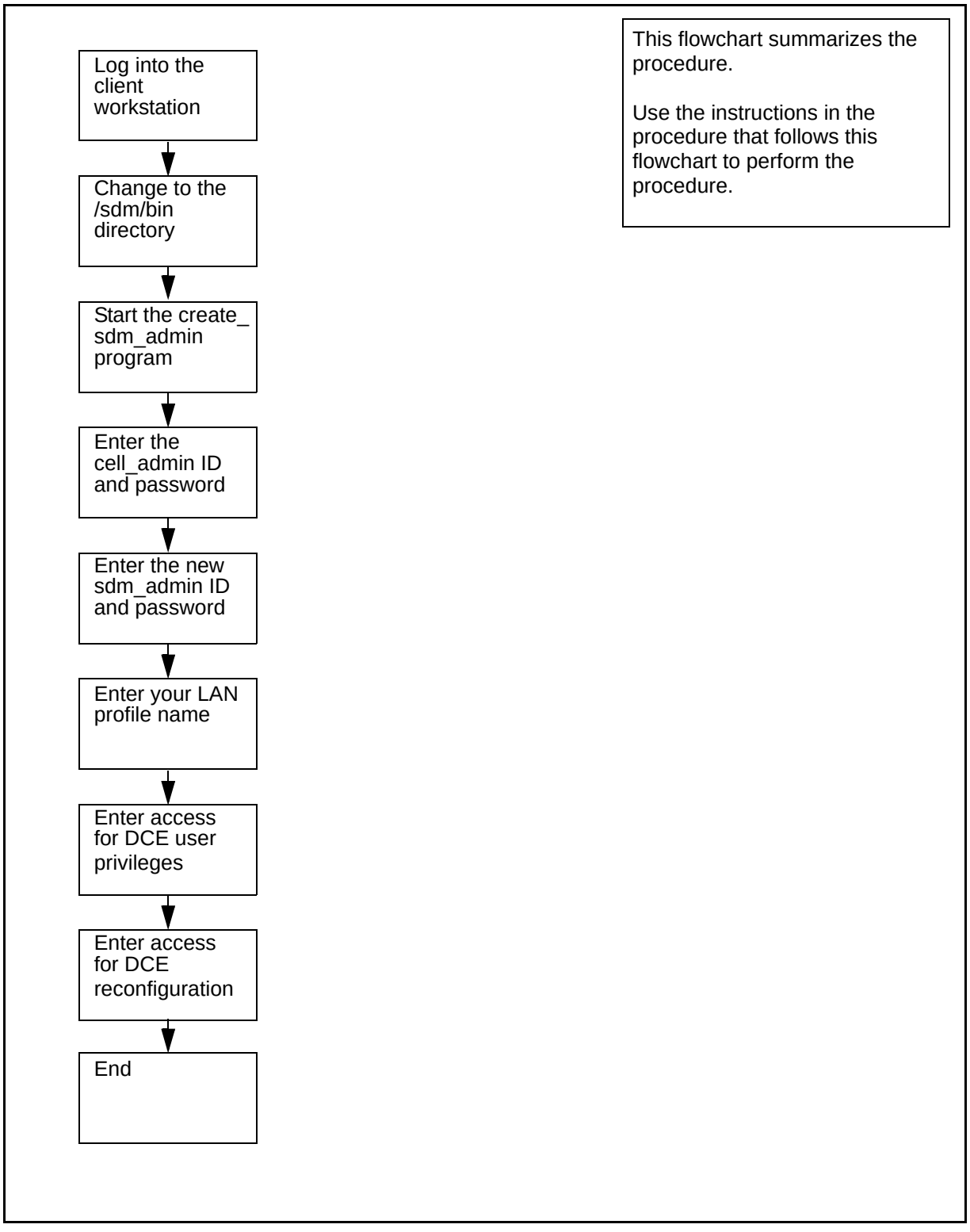
- you must have configured the DCE cell, and at least one remote client machine as the DCE client within the cell
- the DCE cell has cell_admin privileges

Note: You need to perform this procedure once only within your DCE cell.

Action

The following flowchart provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the procedure.

Summary of creating an administration account



Creating an administration account

At the remote client workstation

1 Access the bin directory:

> cd /sdm/bin

2 Create an sdm_admin account:

> ./create_sdm_admin

3 Enter the DCE cell_admin user name, and press the Enter key.

Note: If you do not enter a user ID, the system uses the default value.

4 Enter the DCE cell_admin password, and press the Enter key.

5 Enter the sdm_admin user name that you want to create.

If you do not specify a user name, the system enters sdm_admin as the default name.

6 Enter the password for the sdm_admin account you entered in the previous step.

7 Re-enter the password for the sdm_admin account.

8 Enter the name of your LAN profile (the LAN profile you used to create your DCE cell).

Note: Use the same LAN profile name as the one you used to create your DCE cell. If you use a different LAN profile name, the creation of the admin user account fails. If you do not specify a LAN profile, the system enters lan_profile as the default value

Example response:

```
Do you wish to provide sdm_admin with
“sdm-users” group privileges. (y/n):
```

If you	Do
want the sdm_admin user to have DCE user privileges	enter **y**, press the Enter key, and continue
do not want the sdm_admin user to have DCE user privileges	enter **n**, press the Enter key, and go to step 9

Example response:

```
Do you wish to provide sdm_admin with “config”
group privileges. (y/n):
```

If you	Do
want the sdm_admin user to be able to reconfigure the SDM that is configured by another sdm_admin user	enter **y**, press the Enter key
do not want the sdm_admin user to be able to reconfigure the SDM that is configured by another sdm_admin user	enter **n**, press the Enter key

Example response:

```
Creating principal “sdm_admin”...

Adding “sdm_admin” as a member of the
“sdm-admin” organization...

Adding “sdm_admin” as a member of the
“sdm-admin” group...

Creating account for “sdm_admin”...

Adding “sdm_admin” as a member of the
“sdm-users” organization...

Adding “sdm_admin” as a member of the
“sdm-users” group...

Setting “sdm-admin” ACLs for AIX mkdce and rmdce
routine...

Setting “sdm-admin” ACLs for add_sdm_server
script...

Setting “sdm-admin” ACLs for pre-existing SDM
server principals...

Setting “sdm-admin” ACLs for all other DCE
script objects...

Setting “sdm-admin” ACL for SDM servers that use
ERA...

Setting “sdm-admin” ACL for the SDM ETA
server...

Adding “sdm_admin” as a member of the “config”
security group...

The SDM administrator user ID “sdm_admin” has
been created.
```

9 You have completed this procedure.

Creating ATA user accounts

To install the ATA client application, you must first create the generic ATA user account. Use the following table to determine which procedure to use to create the ATA user account based upon the workstation platform.

Procedures for creating an ATA user account

Platform	Procedure
Hewlett-Packard 700/800 series workstations running the HP-UX 10.20 operating system or higher	Creating the ATA user account with SAM on HP-UX 10.20 on page 11
Sun SPARC workstations running the Solaris 2.6 operating system or higher	Creating the ATA user account with Admintool on Solaris 2.7, 2.8, 2.9 and higher on page 12
IBM RS6000 (AIX 4.3.3) workstations running the AIX 4.1 operating system or higher	Creating the ATA user account with the System Maintenance Interface on the IBM RS6000 on page 13

Creating the ATA user account with SAM on HP-UX 10.20

At the client workstation

1 Log into the client workstation as the root user.

2 Start the System Administration Manager (SAM):

> sam &

The SAM window appears.

3 Double click the Accounts for Users and Groups icon.

The Accounts for Users and Groups window appears.

4 Double click the Local Users icon.

A list of user accounts appears in the list box of the window.

5 From the Actions menu in the Accounts for Users and Groups window, select the Add... menu item.

The Add a user account window appears.

6 In the Login name text box, enter

> ata

7 Change the startup program to read:

`/sdm/bin/ata`

8 Click the Set Password Options button.

A window for setting password options appears.

9 Select the No restrictions (Normal Behavior) item, and click OK.

10 Click the OK button in the Add a user account window.

The Set user password window appears prompting for a password.

11 Click the OK button without setting a password.

A confirmation window appears.

12 Click the Yes button and the user ata is added to the system.

13 You have completed the procedure. You must proceed to the section "Managing ETA extended registry attributes on page 257 after setting up your workstations.

Creating the ATA user account with Admintool on Solaris 2.7, 2.8, 2.9 and higher

At the client workstation

1 Log into the client workstation as the root user.

2 Start the Admintool:

> admintool

The Admintool: Users window appears.

3 Select Add. from the edit menu.

The Admintool: Add User window appears.

4 In the User Name box, enter

ata

5 Select Other from the login shell pop-up menu.

6 In the default login shell text box that appears to the right of the login shell pop-up menu, enter

/sdm/bin/ata

7 Select the No password -- setuid only for password option.

8 Select the Create home dir radio button.

9 In the Path text box, enter

/users/ata

10 Click the Apply button to add the new user to the system.

11 Click theOK button to close the Admintool:Add User window.

12 Exit the Admintool application.

13 Add an entry to the.rhosts file in the ata directory:

cat >> .rhosts

14 Enter a hostname and a user name, separated by a space.

15 Press Ctrl-D to close the file.

16 Change permissions of the.rhosts file to be readable only:

> chmod 644 rhosts

17 You have completed the procedure. You must proceed to the section Managing ETA extended registry attributes on page 257 after setting up your workstations.

Creating the ATA user account with the System Maintenance Interface on the IBM RS6000

At the client workstation

1 Log into the client workstation as the root user.

2 Start the administration tool:

smit mkuser

The Add User window appears.

3 Select Add. from the edit menu.

The Admintool: Add User window appears.

4 In the User Name field, enter

ata

5 In the HOME Directory field, enter

/users/ata

6 In the Initial PROGRAM field, enter

/sdm/bin/ata

7 Exit smit by pressing Esc-0, or the F10 key.

8 Access the ata user’s home directory:

cd /users/ata

9 Create a .rhosts file:

cat > .rhosts

10 Enter a host name and user name separated by a space.

11 Press Ctrl-D to close the .rhosts file.

12 Change the permissions of the .rhosts file:

chmod 644 .rhosts

13 Access the smit password screen:
smit passwd

14 In the user name field, enter

ata

15 Leave the password field blank, and press the Enter key to confirm the ata new blank password.

16 Press the Enter key again to confirm a blank password for the ata account.

17 Exit smit by pressing Esc-0, or the F10 key.

18 Log in to the client machine as the ATA user (leave the password box empty and press the Enter key when prompted)

19 Confirm the blank password when prompted by pressing the Enter key.

20 You have completed this procedure.

Creating system image backup tapes (S-tapes) manually

Purpose

Use this procedure to create a system backup image manually.

Application

Use this procedure to create a system image backup tape (S-tape) manually.

Note: If you want to schedule automatic system image backups, refer to SDM Security and Administration document.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- SDM software

ATTENTION
This procedure must be performed ONLY from a local console by a trained AIX system administrator with root user privileges.

ATTENTION
All volume groups on the SDM must be fully mirrored (Mirrored) before performing this procedure. If not, an error message is displayed.

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

ATTENTION
The files under the /data file system are temporary files only, and are excluded from system image backup.

Perform a system image backup after the following events:

- initial installation and commissioning of the SDM
- changes to the configuration of disks or logical volumes
- installation of a new version of SDM platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 minutes to complete, depending on the size of your file systems.

Recommended tapes

To complete this procedure, use one of the digital audio tape (DAT) drive tapes approved by Nortel Networks.

The brands approved by Nortel Networks are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

The tape lengths approved by Nortel Networks are:

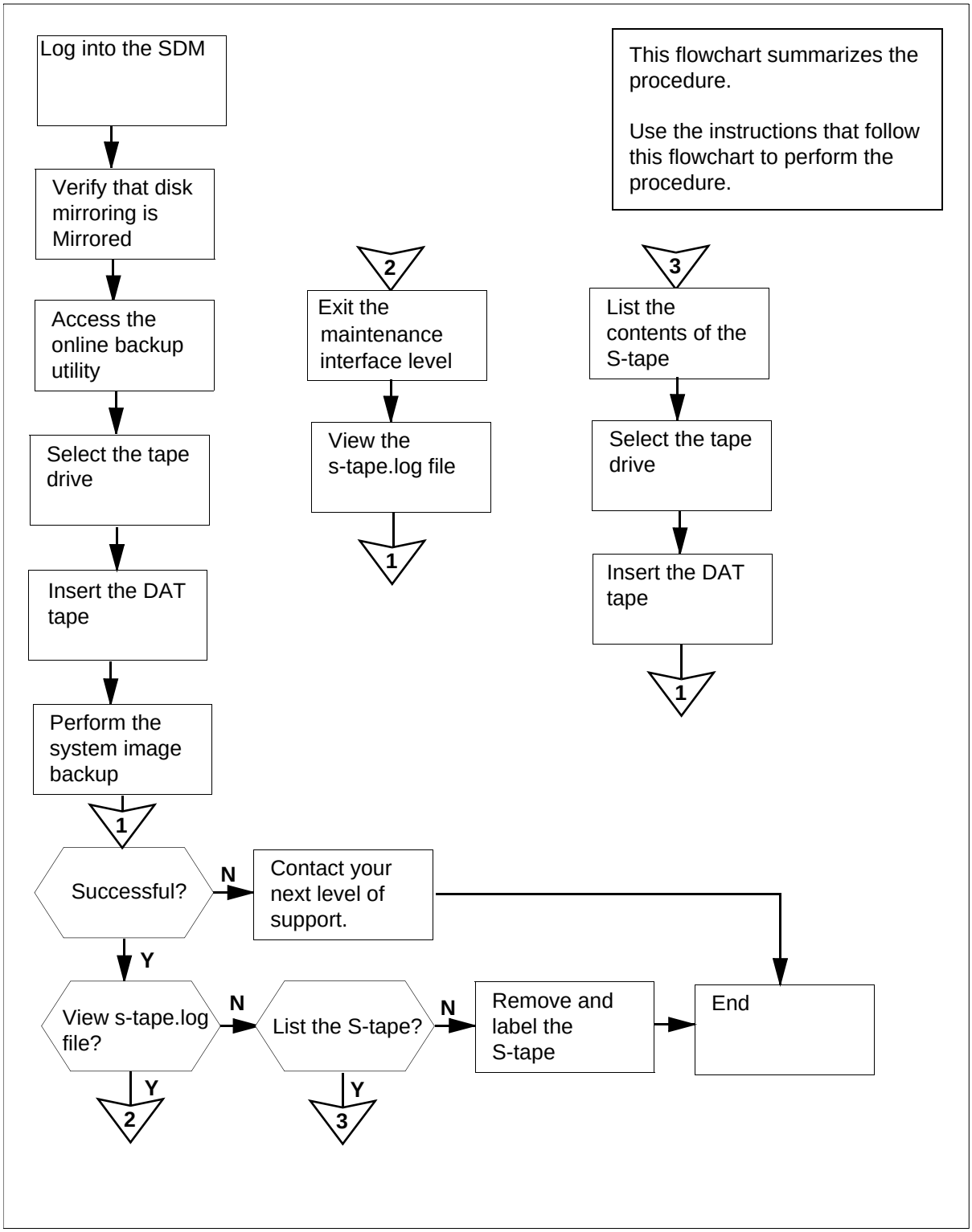
- 90-meter (90M)
- 125-meter (125M)
- 120-meter (120M)

The 125M tape is approved for UMFIOs only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

Action

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

Summary of creating system image backup tapes (S-tapes)



Creating system image backup tapes (S-tapes)

At the local VT100 console

1 Log into the SDM as the root user.

2 Access the maintenance interface:

 # sdmmtc

CAUTION
System mirroring must be MIRRORED
You cannot perform this procedure until disk mirroring of all volume groups is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

Access the storage menu level:

> storage

Example response:

```
Volume Group                Status
Free(MB)
rootvg                    Mirrored            608


Logical Volume   Location     Size(MB)
%full/threshold 1 /          rootvg    20
25/ 80
2 /usr           rootvg      192             85/ 90
3 /var           rootvg      64              11/ 80
4 /tmp           rootvg      24               6/ 90
5 /home          rootvg      300              4/ 70
6 /sdm           rootvg      300             44/ 90
Logical volumes showing: 1 to 6 of 6
```

If the disks	Do
are “Mirrored”	step 3
are not “Mirrored”	contact next level of support

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

> admin

4 Access the System Image Backup and Restore Menu:

> backup

Example response:

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

Note: If another operator attempts to use the Backup and Restore utility when it is in use, an error message is displayed.

5 From the System Image Backup and Restore Menu, select Create a System Image on Tape (S-tape):

> 2

After you select option 2, you are prompted to select the tape drive.

Example response:

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

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

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

6 Select the tape drive to use:

> <n>

where

<n>
is the option (1 or 2) for the tape drive you wish to use

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

Response:

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

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

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

If you	Do
wish to continue using DAT1	enter **y** press the Enter key
do not wish to use DAT1	enter **n** press the Enter key

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

After you select the tape drive, you are prompted to insert a tape in the drive you have selected.

Example response:

```
Please insert a 4mm DAT tape into the tape drive
DAT0.

Caution:
This action will overwrite the content on the
inserted tape.Do you want to proceed? ( y | n )
==>
```

At the SDM

7

CAUTION
System image backup tape
Creating a system image overwrites the contents of the inserted tape. Ensure that you are using the correct tape before starting the system image backup. If your system includes SBA and you are using DAT1, ensure that the tape drive does not contain an SBA tape.

Ensure that the appropriate SDM tape drive contains a 4-mm digital audio tape (DAT) either 90 m or 120 m long. This tape will be designated as the system image backup tape (S-tape).

Note: For the complete list of approved tapes, refer to the Recommended tapes on page 16 section.

At the local console

8 When you are certain you are using the correct tape, enter:

> y

9 Read the system message to determine if there is enough room on the temporary directory for the system image backup to proceed.

Example response:

```
Rewinding the tape...

    The /tmp directory is not big enough.
    Trying to expand /tmp by 6600KB...

Failed to expand the /tmp directory because
there isn't enough free disk space left on the
rootvg.

Please erase some files under /tmp directory to
create at least 6600KB for the full system image
backup.
```

```
Enter any key and return to exit ==>
```

If there is	Do
enough disk space	step 13
not enough disk space	step 10

Note: If there is not enough room on the temporary directory, an error message appears.

10 Erase enough files from the temporary directory to create the required amount of disk space specified in the error message:

> rm -rf /tmp/<filenames>

Note: If you have trouble erasing files from the temporary directory to free up disk space, contact the personnel responsible for your next level of support.

11 Execute the system image backup again.

The system image backup begins.

Example response:

```
Rewinding the tape...

Starting the system image backup on bnode73.

The backup takes a minimum of 10 minutes,
depending on the size of your file systems.

When the backup is complete, you will be asked
to remove the tape from the tape drive.

System image backup is in progress ...
```

Note: This backup process takes approximately 10 minutes to complete, depending on the amount of data stored on the disk.

12 Read the system message.

If the backup	Do
is successfully completed	step 13
fails	contact your next level of support

13 The system informs you if the backup is successful. When the backup is complete, the system prompts you to remove the tape and label it as an S-tape.

Example response:

```
The tape backup started on Wed Oct 16 08:21:15
EDT 1997
completed successfully on Wed Oct 16 08:37:37
EDT 1997.
A log file /tmp/s-tape.log has been created.

Please remove the backup tape from the tape
drive.
Label the tape as shown below and store it in a
safe place.
       System Image Tape (S-tape)
       The Machine Node Id: bnode73
       Date: Wed Oct 16 08:37:37 EDT 1997

Eject the S-tape from the tape drive? ( y | n )
==>
```

14 Determine if you wish to eject the S-tape. Enter

- **y** to eject the tape, or
- **n** if you do not wish to eject the tape, and wish to list its contents.

If you	Do
you wish to list the S-tape	step 27
protect and label the tape	step 15

If you eject the tape, the screen displays “Tape ejected.” below the information displayed in step 13. You are then prompted to return to the System Image Backup and Restore Main Menu.

Response:

```
Tape ejected.

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

15 Place the write-protected tab of the S-tape in the open position, to prevent accidental erasure.

16 When you are ready for the system to return to the System Image Backup and Restore Main Menu, enter

> y

17 Determine if the backup is successful.

The system informs you if the system image backup is successful, as shown in the response in step 13. You may also wish to view the s-tape.log file or list the files on the S-tape.

If	Do
you wish to view the s-tape.log file	step 18
you wish to list the S-tape	step 27
the backup is successful	step 35
the backup fails	contact your next level of support

18 Exit the System Image Backup and Restore Main Menu:

> 0

19 Exit the RMI:

> quit all

20 Access the s-tape.log file:

 # cd /tmp

21 Scroll through the file:

 # more s-tape.log

This screen informs you that the system image backup was completed successfully.

Example response:

```
bosboot:  Boot image is 5881 512 byte blocks.
0+1 records in.
1+0 records out.

Backing up the system...
.....................................................
............
0512 038 mksysb: Backup Completed Successfully.

The S-tape backup started on Wed Oct 16 09:24:07
EDT 1997
```

```
completed successfully on Wed Oct 16 09:36:03
EDT 1997
```

22 Determine if you wish to list the S-tape.

If you	Do
wish to list the S-tape	step 23
do not wish to list the S-tape	step 39

23 Return to the login directory:

 # cd

24 Access the RMI:

 # sdmmtc

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

> admin

26 Access the System Image Backup and Restore Menu:

> backup

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

> 3

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

Example response:

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

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

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

29 Select the tape drive:

> n

where

<n>
is the l (1 or 2) for the tape drive you wish to use

Example response:

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

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

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

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

If you wish to	Enter
continue using DAT1	**y**
not continue	**n**

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

30 After you select the tape drive, you are prompted to insert the S-tape into the tape drive that you selected in step 29.

Example response:

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

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

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

At the SDM

31 Insert the S-tape into the tape drive.

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

At the local VT100 terminal

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

> y

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

Example response:

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

34 Return to the System Image Backup and Restore Menu:

> y

At the SDM

35 If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive.

36 Label the tape according to your office procedures, and store it in a safe location.

37 If you ejected an SBA tape, reinsert the tape.

At the local VT100 terminal

38 Exit the System Image Backup and Restore Menu,:

> 0

Note: If you wish to exit the RMI, enter QUIT ALL.

39 You have completed this procedure.

Scheduling system image backups

Application

ATTENTION
This procedure must be performed ONLY from a local console by a trained AIX system administrator with root user privileges to access the SDM.

ATTENTION
All volume groups on the SDM must be fully mirrored (Mirrored) before performing the backup. If you attempt to perform the backup when disk mirroring is not Mirrored, an error message will be displayed.

ATTENTION
If your system includes the SuperNode Billing Application (SBA), Nortel Networks recommends that you use tape drive DAT0 to perform the backup.

ATTENTION
The files under the /data file system are excluded from system image backup. The files under the /data file system are temporary files that do not require backing up.

ATTENTION
You must also schedule regular cleaning of the digital audio tape (DAT) drive in an NTRX50FQ I/O controller module. Nortel Networks recommends that you clean the tape drive heads after each 25th system backup. For cleaning instructions refer to the “Cleaning the DAT drive” procedure in the Fault Management section.

Use this procedure to schedule automatic system image backups.

Note 1: If you want to create a system image backup tape (S-tape) manually, refer to procedure “Creating system image backup tapes (S-tapes) manually” in the Administration and Security section.

Note 2: If a Backup Failed alarm exist, the next scheduled backup will not start. You must clear the alarm using procedure “Clearing a system image backup Required or Failed alarm” in the Fault Management section.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- SDM software

Nortel Networks recommends that you perform a system image backup after the following:

- initial installation and commissioning of the SDM
- changes to the configuration of disks or logical volumes
- installation of a new version of SDM platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 min. to complete, depending on the size of your file systems.

When scheduling the backup, the tool will prompt for five different parameter values:

1)minute
2)hour
3)day of the month
4)month of the year
5)day of the week

The "day of the month" and "day of the week" fields are distinct.

The specification of days may be made by two fields (day of the month and day of the week). If you specify both as a list of elements, both are adhered to. For example, the following entry:

0 0 1,15 * 1 command would run the backup on the first and fifteenth days of each month, as well as every Monday. To specify days by only one field, the other field should contain a * .

Recommended tapes

Use one of the digital audio tape (DAT) drive tapes approved by Nortel Networks.

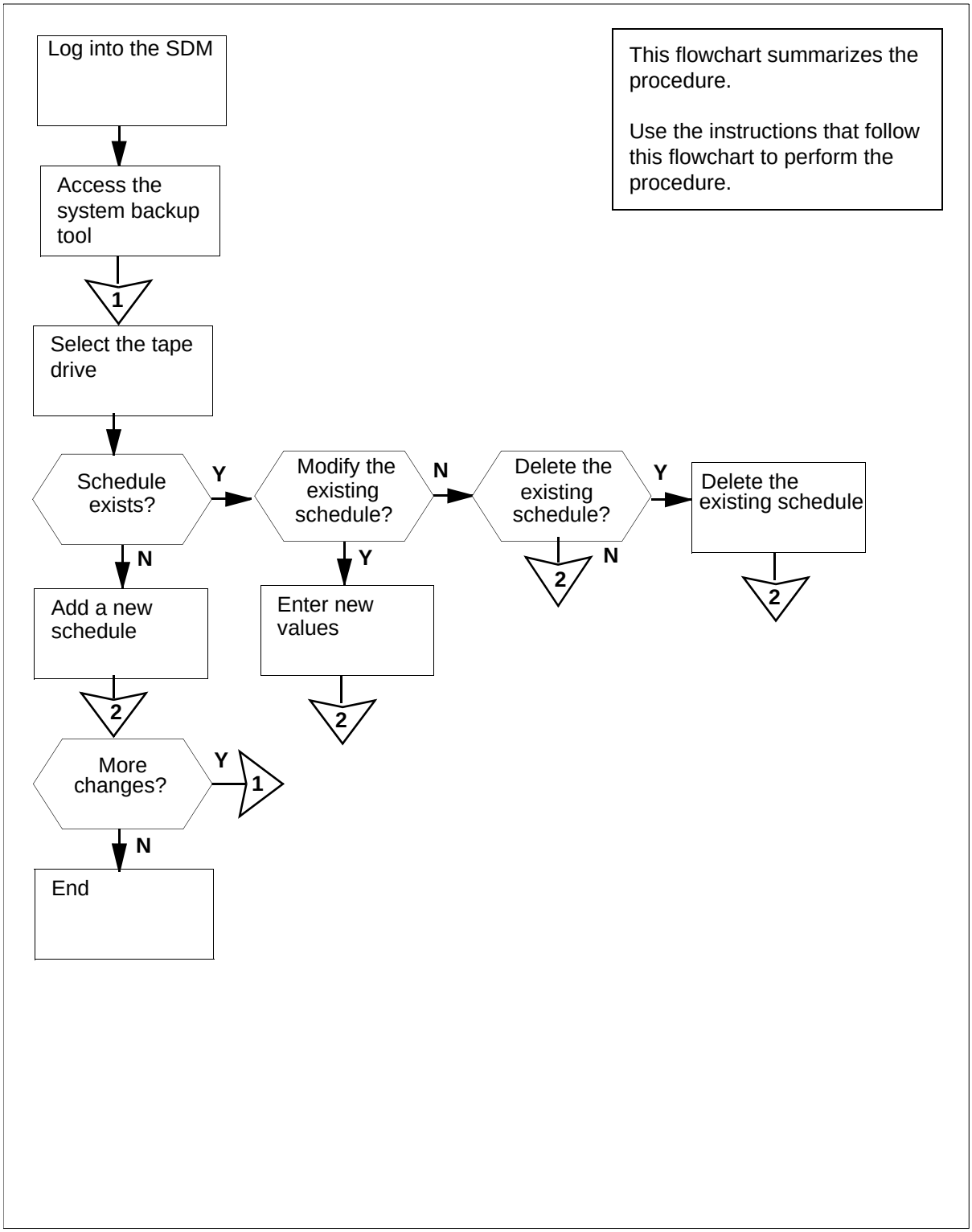
The brands approved by Nortel Networks are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

The tape lengths approved by Nortel Networks are: 90-meter (90M), 120-meter (120M), or 125-meter (125M). The 125M tape is approved for UMFIOs only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

Action

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

Summary of scheduling system image backups



Scheduling system image backups

At the local VT100 console

1 Log into the SDM as the root user.

2 Access the system backup tool:

```
# sysbkup
```

and pressing the Enter key.

Example response:

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


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

3 Access the System Image Backup and Restore Menu by typing

```
> 2
```

and pressing the Enter key.

Response:

```
0. Exit
1. Previous Menu
2. Create a System Image on Tape (S-tape)
3. List Contents of the System Image Tape
(S-tape)
4. Restore Files from the System Image Tape
(S-tape)
5. Schedule Backup

Please enter your selection (0 to 5) ? ==>
```

4 Access the Schedule Backup Configure Menu by typing

> 5

and pressing the Enter key.

Response:

```
0. Exit
1. Previous Menu
2. Schedule Dat 0
3. Schedule Dat 1
4. List Backup Schedules

Please enter your selection (0 to 4) ? ==>
```

5 Use the following table to determine your next step.

If you wish to	Do
view the current schedules	step 6
add, delete, or modify a schedule	step 7

6 Select the List Backup Schedules option by typing

> 4

and pressing the Enter key.

Example response:

```
DAT0
----
         Min    : *
         Hrs    : *
         Date   : *
         Month  : *
         Day    : *
DAT1
----
         Min    : *
         Hrs    : *
         Date   : *
         Month  : *
         Day    : *
```

Note 1: Overlapping backup schedules can be created when fields are set to overlap; for example if the date of the month and the day of the week are both assigned scheduled backup events.

Note 2: If there are no scheduled backups configured, the system displays the following message:

```
There is no Scheduled backup entry
Press Enter to continue...
```

Press the Enter key. The system returns to the Schedule Backup Configure Menu.

7 Select the tape drive that you want to use for the scheduled backup by typing

> x

and pressing the Enter key.

where

x
is the option (2 or 3) for the tape drive you wish to use

Note: If your system includes SBA, Nortel Networks recommends that you use tape drive DAT0 (option 2).

8 Use the following table to determine your next step.

If the response is:	Do
`There is no schedule for DAT<#>, Add new schedule [y/n] ==>`	step 9
`The existing schedule for DAT<#> is ..... Please Enter Your Selection: Modify [1] Disable [2] Exit [0] -->`	step 12

9 To add a new schedule, type **y** and press the Enter key.

If the selected tape drive is	Do
Dat 1 (option 3)	step 10
Dat 0 (option 2)	step 11

10 The system displays the following message:

```
You have selected DAT1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.

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

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

If you wish to continue scheduling for DAT1, type **y**, press the Enter key, and continue with step 11.

If you do not wish to use DAT1, type **n** and press the Enter key. The system returns to the Schedule Backup Configure Menu. Go back to step 7 to continue the procedure.

11 The system displays the following Scheduling Backup screen and prompts you to enter the value for the first parameter (Minute).

```
                    Scheduling Backup

minute (0-59 or '*')
hour (0-23 or '*')
day of the month (1-31 or '*')
month of the year (1-12 or '*')
day of the week (0-6 with 0=Sunday or '*')

Note:
Each pattern can be either an asterisk '*',
meaning all legal values, or a list of elements
separated by commas. An element is either a
number in the ranges, or two numbers in the
range separated by a hyphen (meaning all
inclusive range).

Minute [ 0-59 | * | abort ] :
```

Enter a value (from the range displayed) for each parameter, and press the Enter key after each entered value.

After you enter the last value (day of the week), the system returns to the Schedule Backup Configure Menu.

Go to step 13 to continue the procedure.

12 Use the following table to determine your next step.

If you want to	Do
modify the existing schedule	substep a
delete the existing schedule	substep b

a Type **1**, press the Enter key, and go back to step 11.

b Type **2** and press the Enter key.

Response:

```
Continue with deleting Schedule for DAT<#>
[y/n] ==>
```

c Confirm the command by typing **y** and pressing the Enter key.

Response:

```
Deleted successfully
Press Enter to Continue...
```

Press the Enter key again.

Note: If you want to cancel your delete operation, type **n** and press the Enter key. When prompted, press the Enter key again.

13 If you want to make more changes to your schedules, go back to step 5. Otherwise, continue with step 14.

14 Exit the system backup tool by typing

`> 0`

and pressing the Enter key.

15 You have completed the procedure.

Disabling or enabling a backup Required alarm

Purpose

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

Application

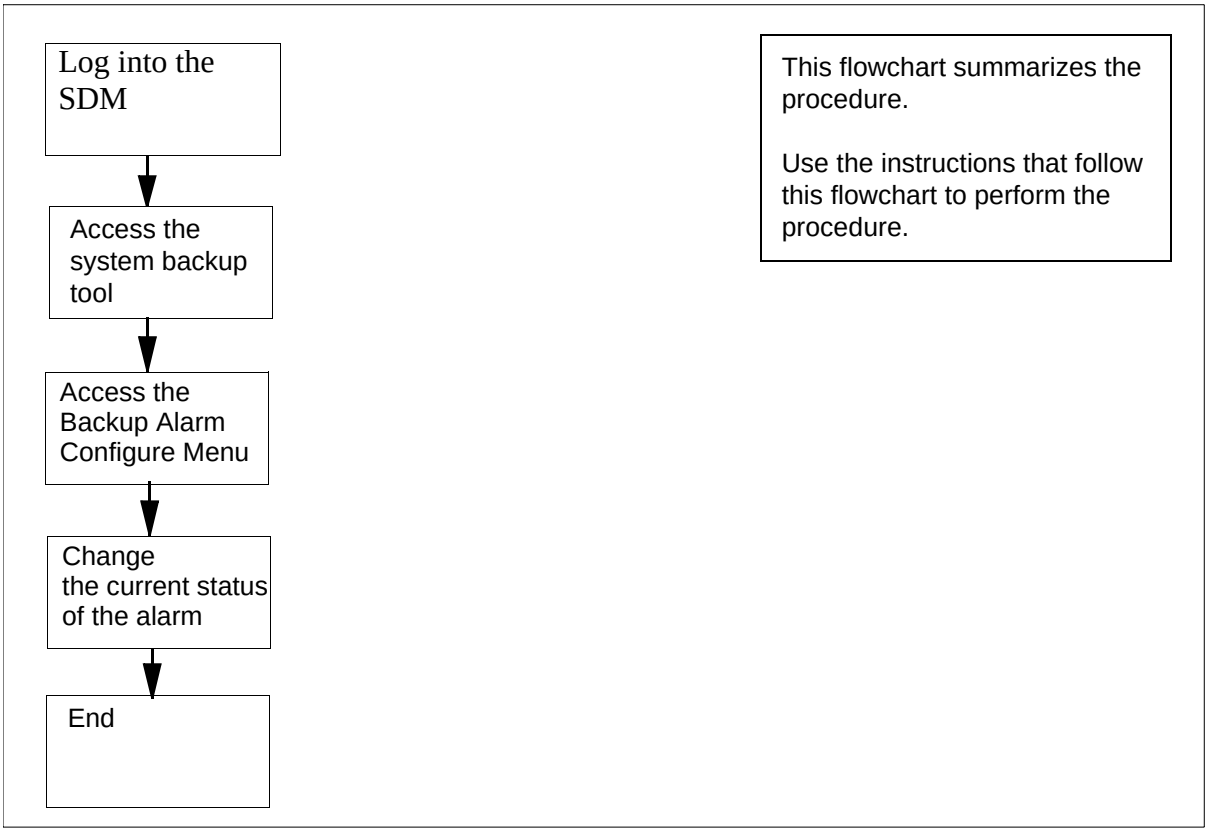
The system generates a backup Required alarm whenever any change occurs to the SDM environment (for example, a patch is applied or logical volume changes). If you do not wish to manually clear the alarm or to initiate a system backup every time a change occurs, you can disable the backup Required alarm.

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

Action

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

Summary of disabling or enabling a backup Required alarm



Disabling or enabling a backup Required alarm

At the VT100 console

1 Log into the SDM as the root user.

2 Access the system backup tool:

```
# sysbkup
```

and pressing the Enter key.

Example response:

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


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

3 Access the Backup Alarm Configure Menu:

```
> 3
```

Example response

```
The Current Alarm Status is: Enabled

You want to Disable it?

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

4 Change the current status of the alarm:

```
> y
```

Note: If you do not want to change the current status of the alarm, type n and press the Enter key. Continue with step 6.

Example response

```
The Current Alarm Status is: Enabled

You want to Disable it? y
Confirm ?...[y/n] ==>

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

5 Confirm your command:

```
> y
```

Note: If you want to abort your command, type n and press the Enter key.

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

If you want to make more changes, go back to step 3. Otherwise, continue the procedure.

7 Exit the system backup tool:

```
> 0
```

8 You have completed the procedure.

Creating a DCE user

Purpose

Use this procedure to create a DCE user account.

Application

Use his procedure to create a DCE user account for a user who runs SDM graphical user interface (GUI) client programs.

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

ATTENTION
Use either the master administration account (cell_admin) or a DCE sub administrator account (sdm_admin) to perform this procedure.

You cannot use the sdm_admin account to delete a DCE user created by a cell_admin account. The cell_admin account can delete any DCE users created by either a cell_admin or an sdm_admin account.

The create_dce_user command creates a new DCE user and makes the user a member of a specified group.

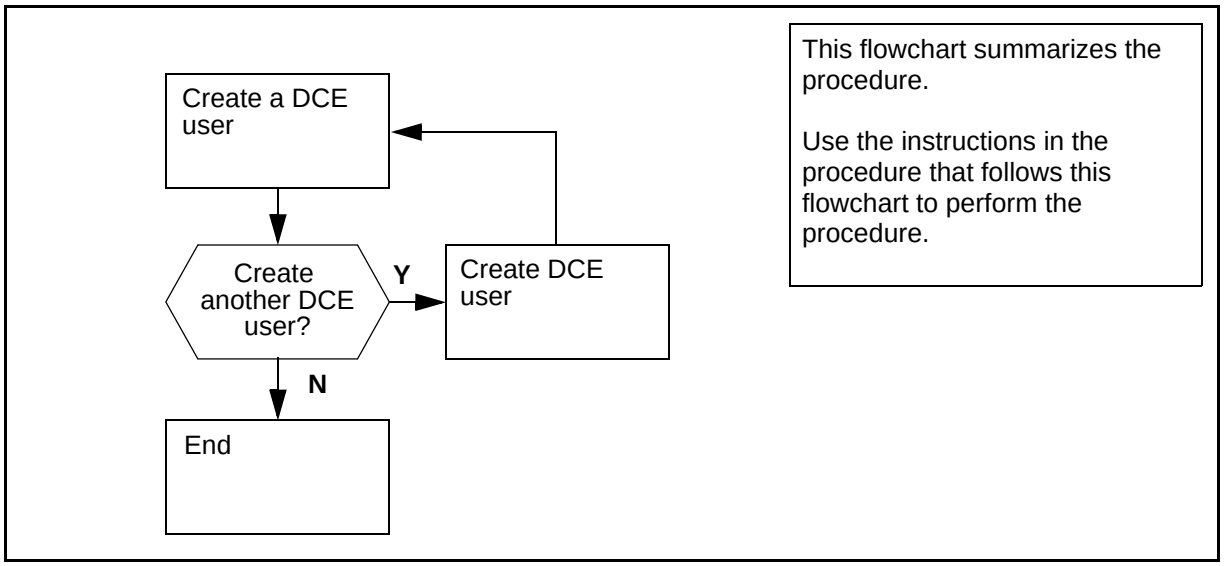
Note: You must use the cell_admin account to create groups.

You can use these groups for access control purposes to categorize users with similar job functions.You only need a DCE account to run an SDM GUI program. There can be some exceptions for specific SDM applications. For any exceptions, refer to the OSF DCE Command Reference document that is provided with the application.

Action

The following flowchart provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the procedure.

Summary of creating a DCE user account



Creating a DCE user

At the client workstation

1 Create a DCE user:

> /sdm/bin/create_dce_user

Note: When running the create_dce_user script, place the new dce user ONLY into the sdm-users group.

2 Enter the DCE administrator user ID.

Note: If you do not enter a user name, the system enters sdm_admin as the default value.

3 Enter the DCE administrator password.

4 Enter the new DCE user ID.

5 Enter a password for the new DCE user ID.

6 Re-enter the password.

Example response:

```
Full name of the person associated with “ops_1”
```

7 Enter the full name of the person associated with the new user ID.

8 Enter the user group for the new DCE user.

Note: If you do not enter a user group, the system enters sdm-users as the default value.

Example response:

```
Creating principal “ops_1”...

Adding “ops_1” as a member of the “sdm-users”
organization...

Adding “ops_1” as a member of the “sdm-users”
group...

Creating account for “joe”...

Setting “ops_1” ACL for SDM server to use
ERAs...

Setting “ops_1” ACL for the SDM ETA server...

The DCE user ID “ops_1” has been created.
```

9 You have completed this procedure.

Starting an SCFT client session

Application

Use this procedure to start an SSH Core File transfer (SCFT) session.

You must perform this procedure from the client workstation running UNIX or Linux with the SSH and the CMFT script installed.

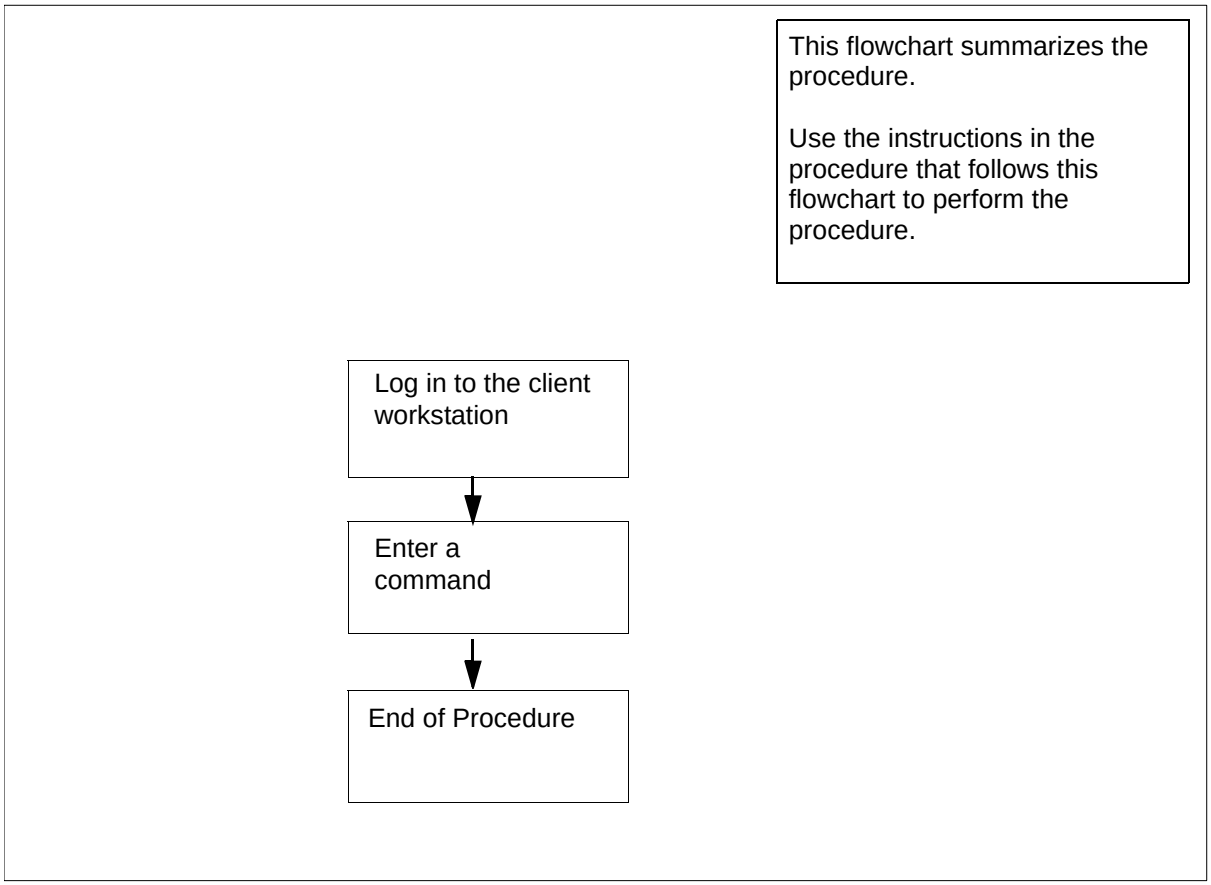
Nortel Networks recommends that all component level security management connections to the core be made using SCFT.

You must have root user privileges on the core module to perform this procedure.

Action

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

Summary of starting an SCFT client session



Starting an SCFT client session

At the client workstation

1 Enter a command. Refer to the following procedures in this document:

- Displaying help for SCFT on page 61
- Listing volumes on Core using SCFT on page 65
- Removing a file from Core using SCFT on page 57
- Transferring files from Core using SCFT on page 49
- Transferring files to Core using SCFT on page 53

2 You have completed this procedure.

Transferring files from Core using SCFT

Application

Use this procedure to transfer files from the Core using SSH Core File transfer (SCFT).

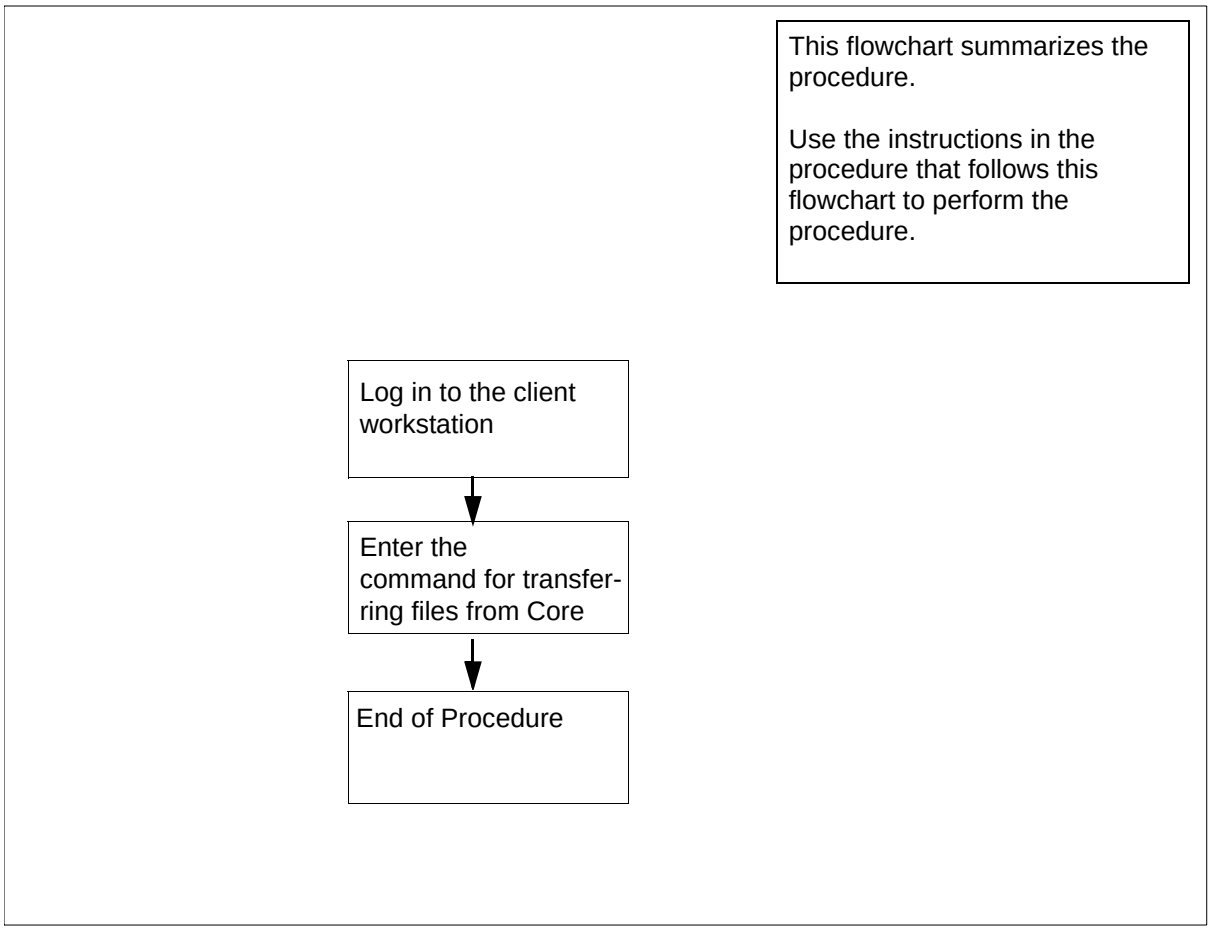
You must perform this procedure from the client workstation running UNIX or Linux with the SSH and the CMFT script installed.

You must have root user privileges on the core module to perform this procedure.

Action

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

Summary of transferring files from core using SCFT



Transferring files from core using SCFT

At the client workstation

1 Go to the next step depending on the command type you use.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Transfer files from a specific volume on the core by typing

```
> ssh <user>@<host> "scft <-b|-a> < -s reclen>
-g /<volume>/<SDMfile>" > <localfile>
```

and pressing the Enter key.

where

user
is the user name you are using to log on to the SDM

host
is the name or IP address of the SDM

b
is used with get or put to specify binary format

a
is used with a file transfer to specify ASCII format

reclen
is the length of the records in the file being transferred

volume
is the name of the SDMvolume on the core from which the file to be downloaded is located.

SDM*file*
is the full name (including the directory path) of the SDM file on the Core from which the copy originates.

localfile
is the name of the local file the copy is going to including the directory path

Example entry:

```
ssh root@host1 "scft -b -s 1024 -g /sfdev/file1"
> /localdir/localfile
```

Example response:

```
Opened Connection to Core


Command complete
```

3 You have completed this procedure.

4 Transfer files from a specific volume on the core by typing

> cmft <-b|-a> < -s reclen> <user>@<host>:

/<volume>/<SDMfile> <localfile>

and pressing the Enter key.

where

user
is the user name you are using to log on to the SDM

host
is the name or IP address of the workstation

b
is used with get or put to specify binary format

a
is used with a file transfer to specify ASCII format

reclen
is the length of the records in the file being transferred

volume
is the name of the volume on the core

SDM*file*
is the name of the SDM Core file the copy is coming from including the directory path

localfile
is the name of the local file the copy is going to including the directory path

Example entry:

```
cmft root@host1:/sfdev/file1/localdir
/localfile
```

Example response:

```
Opened Connection to Core

Command complete
```

5 You have completed this procedure.

Transferring files to Core using SCFT

Application

Use this procedure to transfer files to the Core using SSH Core File transfer (SCFT).

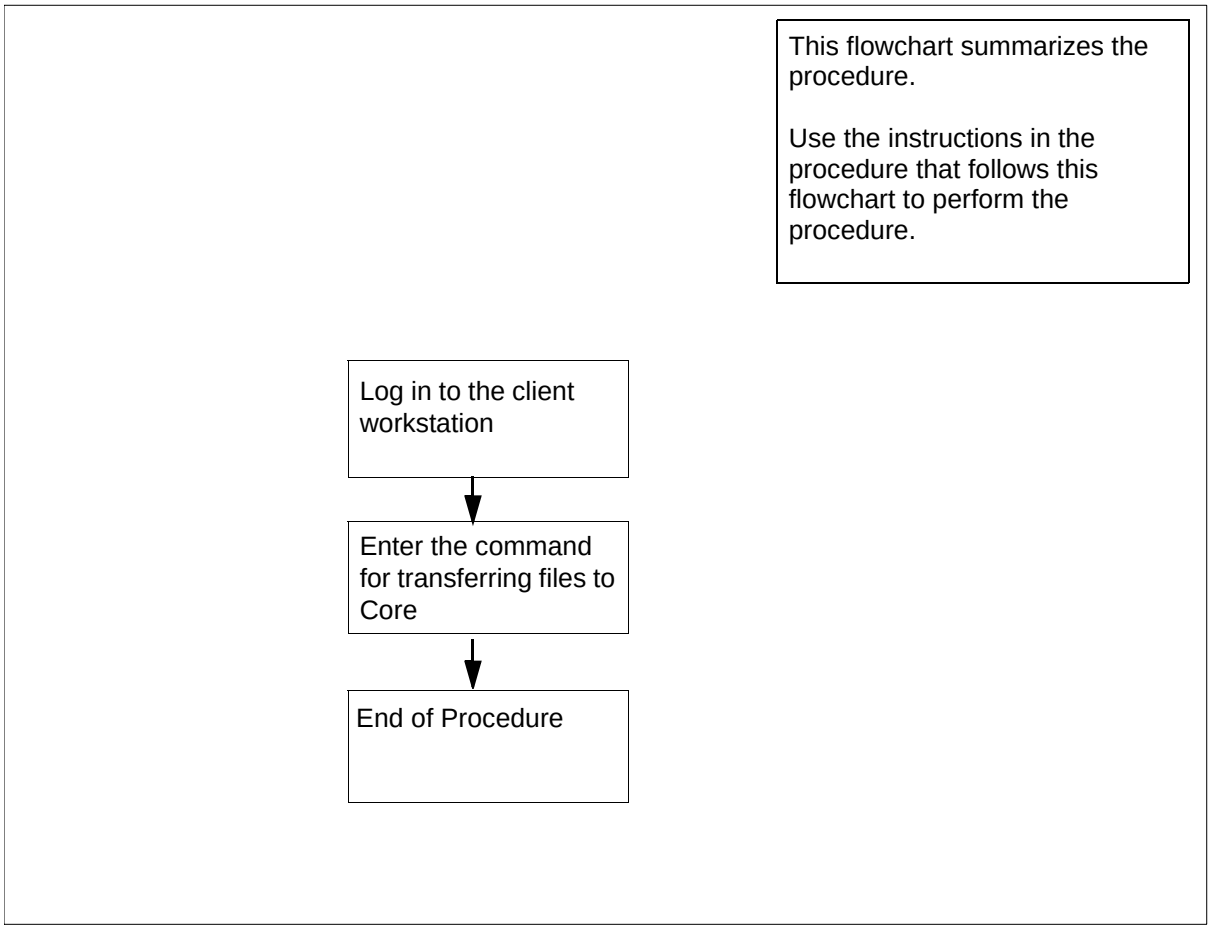
You must perform this procedure from the client workstation running UNIX or Linux with the SSH and the CMFT script installed.

You must have root user privileges to perform this procedure.

Action

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

Summary of transferring files to core using SCFT



Transferring files to core using SCFT

At the client workstation

1 Go to the next step depending on the command type you use.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Transfer files to a specific volume on the core by typing

```
> ssh <user>@<host> "scft <-b|-a> < -s reclen>
-p /<volume>/<SDMfile>" < <localfile>
```

and pressing the Enter key.

where

user
is the user name you are using to log on to the SDM

host
is the name or IP address of the SDM

b
is used with get or put to specify binary format

a
is used with a file transfer to specify ASCII format

reclen
is the length of the records in the file being transferred

volume
is the name of the volume on the SDM

SDM*file*
is the name of the SDM Core file the copy is going to including the directory path

localfile
is the name of the local file the copy is coming from including the directory path

Example entry:

```
ssh root@host1 "scft -b -s 1024 -p /sfdev/file1"
< /localdir/localfile
```

Example response:

```
Opened Connection to Core


Command complete
```

3 You have completed this procedure.

4 Transfer files to a specific volume on the core by typing

> cmft <-b|-a> < -s reclen> <localfile> <user>@<host>:/<volume>/<SDMfile>

and pressing the Enter key.

where

b
is used with get or put to specify binary format

a
is used with a file transfer to specify ASCII format

reclen
is the length of the records in the file being transferred

localfile
is the name of the local file the copy is coming from including the directory path

user
the user name you are using to log on to the SDM

host
the name or IP address of the SDM

volume
is the name of the volume on the workstation

SDM*file*
is the name of the SDM Core file the copy is going to including the directory path

Example entry:

cmft /localdir/localfile root@host1:/sfdev /file1

Example response:

```
Opened Connection to Core


Command complete
```

5 You have completed this procedure.

Removing a file from Core using SCFT

Application

Use this procedure to remove a file from the Core using SSH Core File transfer (SCFT).

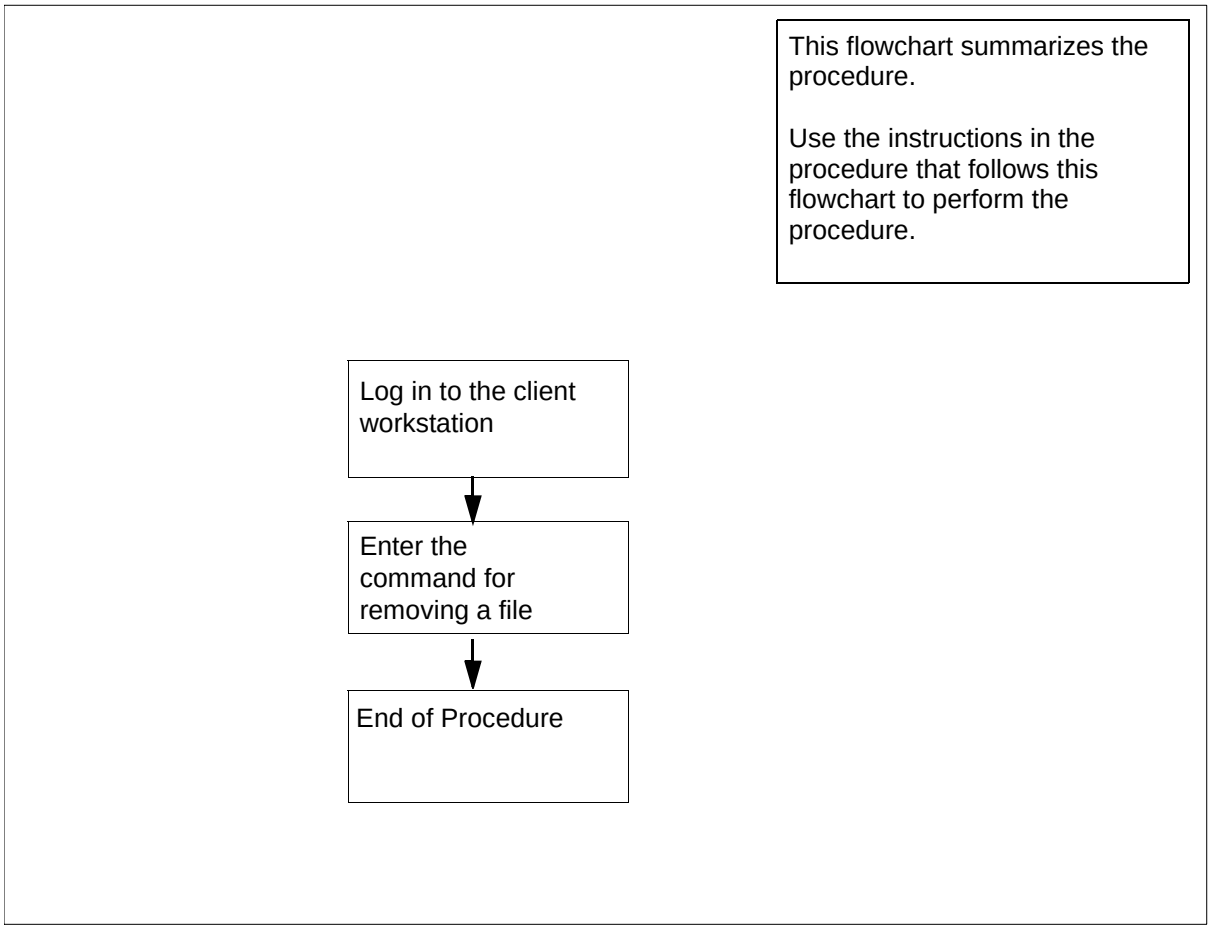
You must perform this procedure from the client workstation running UNIX or Linux with the SSH and the CMFT script installed.

You must have root user privileges to perform this procedure.

Action

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

Summary of removing a file from core using SCFT



Removing a file from core using SCFT

At the client workstation

1 Go to the next step depending on the command type you use.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Remove a file in a specific volume on the core by typing

`> ssh <user>@<host>"scft -r /<volume>/ <filename>"`

and pressing the Enter key.

where

user
is the user name you are using to log on to the SDM

host
is the name or IP address of the SDM

volume
is the name of the volume on the SDM

filename
is the name of the SDM Core file being removed including the directory path

Example response:

```
Opened Connection to Core


Command complete
```

3 You have completed this procedure.

4 Remove a file in a specific volume on the core by typing

`> cmft -r <user>@<host>:/<volume>/<filename>`

and pressing the Enter key.

where

user
is the user name you are using to log on to the SDM

host
is the name or IP address of the SDM

volume
is the name of the volume on the SDM

filename
is the name of the SDM Core file being removed including the directory path

Example response:

```
Opened Connection to Core


Command complete
```

5 You have completed this procedure.

Displaying help for SCFT

Application

Use this procedure to display help during an SSH Core File transfer (SCFT) session.

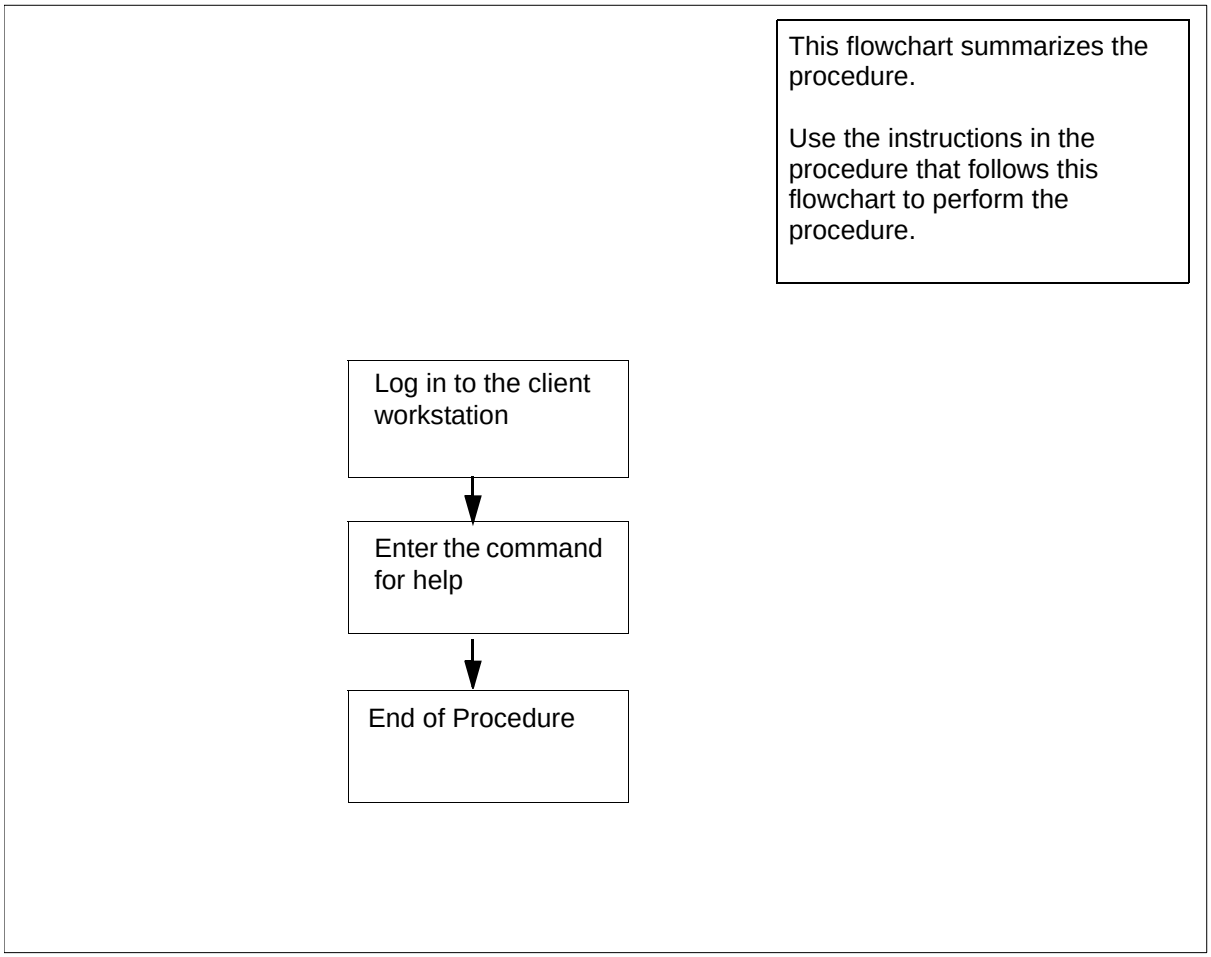
You must perform this procedure from the client workstation running UNIX or Linux with the SSH and the CMFT script installed.

You must have root user privileges to perform this procedure.

Action

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

Summary of displaying help for SCFT



Displaying help for SCFT

At the client workstation

1 Go to the next step depending on the command type you use.

If you use	Do
ssh commands	step 2
cmft commands	step 4

2 Display help text by typing.

`> ssh <user>@<host> "scft -h"`

and pressing the Enter key.

where

user
the user name you are using to log on to the SDM

host
the name or IP address of the SDM

Response:

```
Command complete


SCFT Help:

<-n hostname><-a><-b><-s record length>
<-p filename><-h><-l volume><-g filename>
<-r filename>

-n: Hostname of Core
-b: Binary Transfer
-a: Ascii Transfer
-s: Specify the record length to be used for the
file being transferred
-p: Put a file on the Core
-h: Help
-l: List the directory on the Core
-g: Get a file from the Core
-r: Remove a file on the Core
```

3 You have completed this procedure.

4 Display help text by typing.

> cmft - h

and pressing the Enter key.

Response:

```
 To transfer a file
cmft  [-b|-a][-s <int>] [[[user@host:]vol]file1
[[[user@]host:]vol]file2

 To list a volume on the Core
cmft  -l [user@]host:<vol>

 To remove a file from the CBM
cmft  -r [[[user@]host:]vol]file1

 For this help information
cmft -h
  -l  -- To list a volume on the Core
  -r  -- To remove a file from the Core
  -h  -- To get this help information
  -s  -- To set the record length for the file
being transferred
  -b  -- Use with a get or put to specify binary
format
  -a  -- Use with a file transfer to speciy ASCII
format
       NOTE:  one or the other can be used not
both.  Default is binary

 int  -- An integer representing the record
size.
 user -- the user name you wish to log on to the
CBM with.
     This is optional. If not entered the userid
you are executing this script with will be used.
          eg.   root

 host --  the name or ip address of the cbm you
wish to log on to.
          eg.   ##.###.###.## or HOSTNAME
```

```
 file1 -- name of the file the copy is coming
from including directory path
 file2 -- name of the file the copy is going to
including directory path
      NOTE: Only one of the files can have the
host name present.
            This would be the file that is or
will be on the CBM.
       NOTE: the local files can also have an
extension
           Allowable extensions are .bin[##],
.txt[##], $df and $patch
          .txt is Ascii with a specified record
length
            .bin is Binary with a specified
record length
          $df and $patch are Binary with record
length of 128

 vol  -- the name of the volume on the SDM, you
wish to list or
        '/' to list all volume

 examples:
   To put a binary file with record length 1024
from local file /bin/data1 to core file
/volume/data:
          cmft -b -s 1024 /bin/data1
root@HOSTNAME:/volume/data1

   To get a file from the core file /volume/data
to a local file data:
          cmft root@HOSTNAME:/volume/data1
/bin/data1

    To list the volume names on the core:
          cmft -l root@HOSTNAME:/

    To list the files in the sfdev volume:
          cmft -l root@HOSTNAME:/sfdev
```

5 You have completed this procedure.

Listing volumes on Core using SCFT

Application

Use this procedure to list volumes on the Core during SSH Core File transfer (SCFT) session.

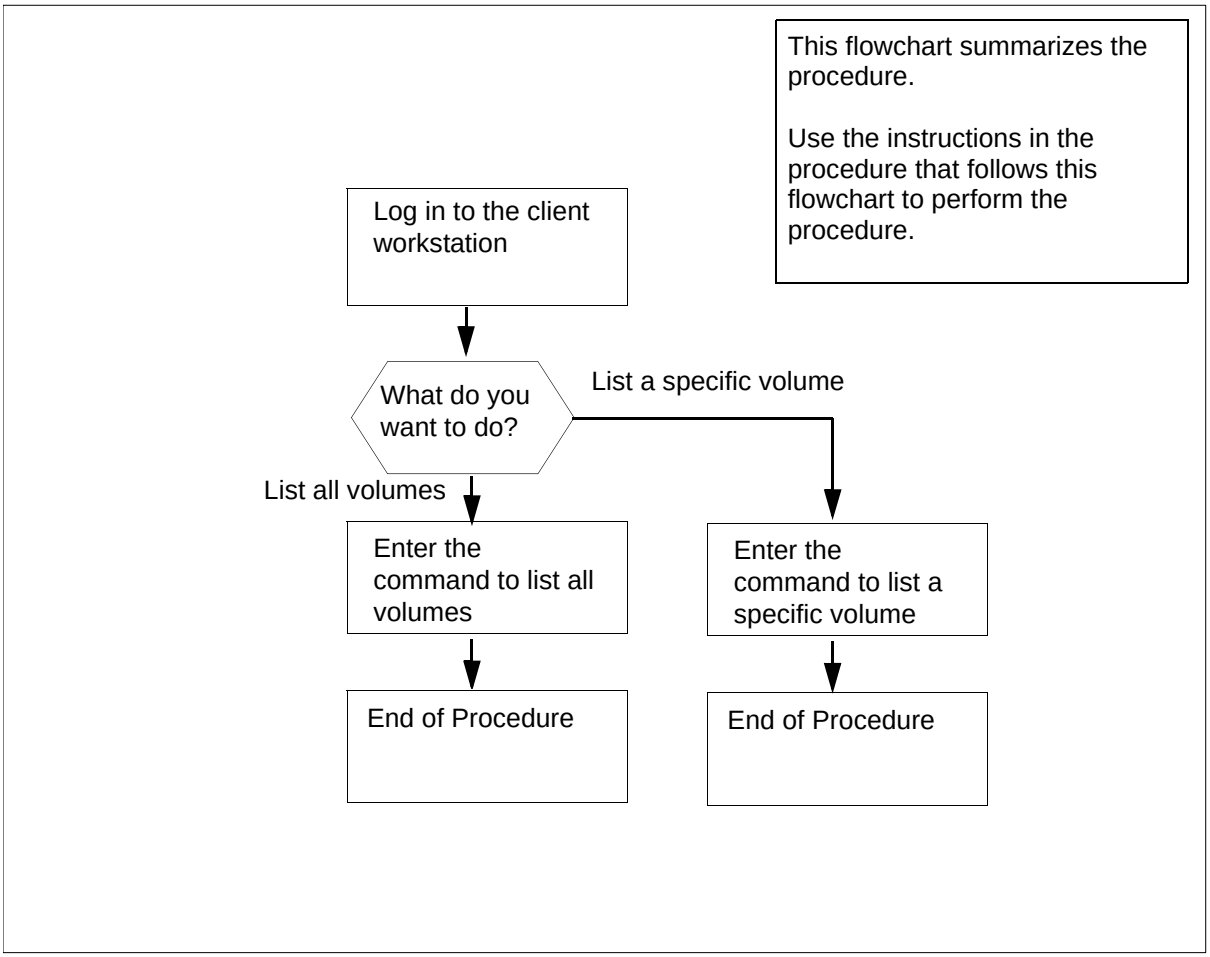
You must perform this procedure from the client workstation running UNIX or Linux with the SSH and the CMFT script installed.

You must have root user privileges to perform this procedure.

Action

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

Summary of listing volumes on Core using SCFT



Listing volumes on Core using SCFT

At the client workstation

1 Go to the next step depending on the type of command you use.

If you use	Do
ssh commands	step 2
cmft commands	step 6

2 Use the following table to determine your next step.

If you want to	Do
list all volumes	step 3
list a specific volume	step 4

3 List all volumes on the Core by typing

`> ssh <user>@<host>"scft -1 /"`

and pressing the Enter key.

where

user
the user name you are using to log on to the SDM

host
the name or IP address of the SDM

Example response:

```
SFDEV
S01DIMAGE
S00DIMAGE1
S00DAMA
S01DPMLOADS
S01DPERM
S01DDLOG
S01DTEMP


Command complete
```

If you	Do
want to list a specific volume	step 4
do not want to list a specific volume	you have completed this procedure

4 List a specific volume on the Core by typing

`> ssh <user>@<host>"scft -1 /<volume>"`

and pressing the Enter key.

where

user
the user name you are using to log on to the SDM

host
the name or IP address of the SDM

volume
is the name of the volume on the SDM

Example response:

```
LOGIN STDFAULT
IOC$
MSCDINV$
CMSHELF$
EADASOM$DATAFILL
NNASST$
OFCENG
VRDATA$
OM CONFIG
OFCOPT
OFCVAR
OFCSTD
NNASST
DATASIZE
OMKEYORD$INFO$FILE
PML


Command complete
```

5 You have completed this procedure.

6 Use the following table to determine your next step.

If you want to	Do
list all volumes	step 7
list a specific volume	step 8

7 List all volumes on the Core by typing

`> cmft -1 <user>@<host>:/`

and pressing the Enter key.

where

user
the user name you are using to log on to the SDM

host
the name or IP address of the SDM

Example response:

```
SFDEV
S01DIMAGE
S00DIMAGE1
S00DAMA
S01DPMLOADS
S01DPERM
S01DDLOG
S01DTEMP


Command complete
```

If you	Do
want to list a specific volume	step 8
do not want to list a specific volume	you have completed this procedure

8 List a specific volume on the Core by typing

`> cmft -1 <user>@<host>:/<volume>`

and pressing the Enter key.

where

user
the user name you are using to log on to the SDM

host
the name or IP address of the SDM

volume
is the name of the volume on theSDM

Example response:

```
LOGIN STDFAULT
IOC$
MSCDINV$
CMSHELF$
EADASOM$DATAFILL
NNASST$
OFCENG
VRDATA$
OM CONFIG
OFCOPT
OFCVAR
OFCSTD
NNASST
DATASIZE
OMKEYORD$INFO$FILE
PML


Command complete
```

9 You have completed this procedure.

Use the following procedure to use the ASCII Terminal Application (ATA) to connect to the Core. ATA provides two methods to connect to the Core:

- ATA client
- command line arguments

Prerequisites

This procedure requires the following information:

- access to the ATA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the Core to access

Procedure

Perform the following steps to complete this procedure.

Using the ATA client to connect to the Core

At your workstation

1 Log into the application client machine.

2 Change the directory to the sdm/bin directory:

> cd /sdm/bin

3 Start the ATA application:

> ata

The system prompts for a DCE principal name.

4 Enter your DCE userid and press the Enter key.

The system prompts for a password.

5 Enter your DCE password and press the Enter key.

The ATA application starts and the prompt changes to `ata>`.

6 List the CLLI of the available switches:

ata> list

ATA displays a list of CLLI.

7 Locate the CLLI of the switch with the Core to access.

8 Access the Core:

ata> open <switch_clli_name> cm

where

<switch_clli_name> is the CLLI of the switch with the Core you want to access

Example input:

open RLGHNC01ECB cm

ATA connects to the Core

Note: Once connected to the core and if you loose your connection, the core drops your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

9 lose the session with the Core before you quit ATA.**> logout**

10 Quit ATA:**> quit**

11 You have completed this part of the procedure.

Using command line arguments to connect to the Core

At your workstation

1 Log into the application client machine.

2 Start the ATA application and list the CLLI of the available switches:

> /sdm/bin/ata -list

The system prompts for a DCE principal name.

3 Enter your DCE userid.

The system prompts for a password.

4 Enter your DCE password.

A list of CLLI names is displayed.

5 Locate the CLLI of the switch with the Core to access.

6 Connect to the Core:

> /sdm/bin/ata -clli <switch_clli_name> -session CM

where

<switch_clli_name> is the CLLI of the switch with the Core you want to access

Example of command input:

/sdm/bin/ata -clli RLGHNC01ECB -session CM

The system prompts for a DCE principal name.

7 Enter your DCE userid and press the Enter key.

The system prompts for a password.

8 Enter your DCE password.

ATA connects to the Core.

Note: Once connected to the core and if you loose your connection, the core drops your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

9 Close the session with the Core before you quit ATA.

> **logout**

10 Quit ATA:
> quit

11 You have completed the procedure.

Purpose

Use the following procedure to use Enhanced Terminal Application (ETA) to access the Core.

Prerequisites

This procedure requires the following information:

- access to the ETA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the Core to access

Procedure

Perform the following steps to complete this procedure.

At your workstation

1 Log into the application client machine.

2 Go to the directory with the ETA application client:

> cd /sdm/bin

3 Start the ETA application client:

> ./eta

The system displays a copyright window.

4

ATTENTION

If the system displays a window with an error message and a Trace Back button, a serious software error may have occurred. Ask your system administrator to click the Track Back button, record the response for analysis, and click the OK button to continue. If necessary, contact Nortel Networks for assistance.

Wait 10 seconds.

ETA displays the DCE Login window.

Note: If you do not want to log in, click the **Abort** button. The system returns to the UNIX prompt.

5 Log in to DCE.

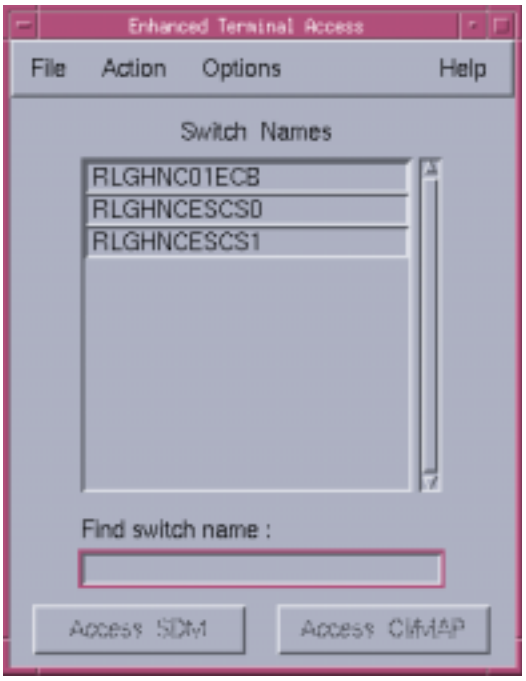
6 Enter your DCE userid in the field **Principal name**.

7 Enter your DCE password in the field **Password**.

8 Click the **OK** button.

ETA displays a list of available CLLI.

Example of an ETA window



9 Select the CLLI of the switch with the Core you want to access. If necessary, use the scroll bar on the right side of the list.

Example of an ETA window:

10 Access the Core by clicking the Access CI/MAP button.

ETA connects to the Core and displays a CI prompt.

Note: Once connected to the core, if you lose your connection, the core drops your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

11 Close all CI/MAP sessions before you quit ETA. To close the CI/MAP session with the Core, logout at the CI prompt:
CI> logout

12 To quit ETA, select Exit from the File menu in the main ETA window

13 You have completed this procedure.

Connecting to the SDM with ATA

Purpose

Use the following procedure to connect to the SDM using the ASCII Terminal Application (ATA) to ATA provides two methods to connect to the SDM.

- ATA client
- command line arguments

Note: Connecting to the SDM and then connecting to the Core is not recommended. Connect to the Core as a pass-thru user instead.

Prerequisites

This procedure requires the following information:

- access to the ATA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the SDM you want to access

Procedure

Perform the following steps to complete this procedure.

Using the ATA client to connect to the SDM

At your workstation

1 Log into the application client machine.

2 Change the directory to the sdm/bin directory:

> cd /sdm/bin

3 Start the ATA application:

> ata

The system prompts for a DCE principal name.

4 Enter your DCE userid.

The system prompts for a password.

5 Enter your DCE password.

The ATA application starts and the prompt changes to `ata>`.

6 List the CLLIs of the available switches:

ata> list

ATA displays a list of CLLI.

7 Locate the CLLI of the switch with the SDM you want to access.

8 Access the SDM

ata> open <switch_clli_name> sdm

where

<switch_clli_name> is the CLLI of the switch with the SDM you want to access

Example input:

open RLGHNC01ECB sdm

ATA connects to the SDM.

Example response:

```
There is 1 local login.
There are 3 ETA logins to the SDM.
There is 1 ETA logins to the CM.

Current SDM status:
SDM     CON     512     NET      APPL     SYS     HW
  .       .      ..       .        .        .       .
                 ..

maint:
```

Note: Once connected to the core, if you lose your connection, the core will drop your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

9 Close the SDM session before you quit ATA. To close the SDM session, logout at the prompt:
> logout

10 To quit ATA, enter:
> **quit**

11 You have completed this part of the procedure.

Using command line arguments to connect to the SDM

At your workstation

1 Log into the application client machine.

2 Start the ATA application and list the CLLIs of the available switches:

> /sdm/bin/ata -list

The system prompts for a DCE principal name.

3 Enter your DCE userid.

The system prompts for a password.

4 Enter your DCE password.

ATA displays a list of CLLI names.

5 Locate the CLLI of the switch with the SDM you want to access.

6 Access the SDM

> /sdm/bin/ata -clli <switch_clli_name> -session SDM

where

<switch_clli_name> is the CLLI of the switch with the SDM you want to access

Example input:

/sdm/bin/ata -clli RLGHNC01ECB -session SDM

The system prompts for a DCE principal name.

7 Enter your DCE userid.

The system prompts for a password.

8 Enter your DCE password.

ATA connects to the SDM.

Example response:

```
There is 1 local login.
There are 3 ETA logins to the SDM.
There is 1 ETA logins to the CM.

Current SDM status:
SDM     CON     512     NET     APPL     SYS     HW
  .       .      ..       .        .       .       .
                 ..


maint:
```

Note: Once connected to the core, if you loose your connection, the core will drop your login session within five seconds. If your login id is not released by the core after approximately five seconds, then login to the core with another userid and manually end the original login session.

9 Close the SDM session before you quit ATA. To close the SDM session, exit at the prompt:

`exit`

10 To quit ATA, quit at the prompt:

> quit

11 You have completed the procedure.

Connecting to the SDM with ETA

Purpose

Use the following procedure to use Enhanced Terminal Application (ETA) to connect to the SDM.

Note: Connecting to the SDM and then connecting to the Core is not recommended. Connect to the Core as a pass-thru user instead.

Prerequisites

This procedure requires the following information:

- access to the ETA client machine
- your DCE userid
- your DCE password
- the CLLI of the switch with the SDM you want to access

Procedure

Perform the following steps to complete this procedure.

At your workstation

1 Log into the application client machine.

2 Go to the directory with the ETA application client:

> cd /sdm/bin

3 Start the ETA application client:

> ./eta

The system displays a copyright window.

ATTENTION

If the system displays a window with an error message and a Trace Back button, a serious software error may have occurred. Ask your system administrator to click the Track Back button, record the response for analysis, and click the OK button to continue. If necessary, contact Nortel Networks for assistance.

Wait 10 seconds.

ETA displays the DCE Login window.

Note: If you do not want to log in, click the Abort button. The system returns to the UNIX prompt.

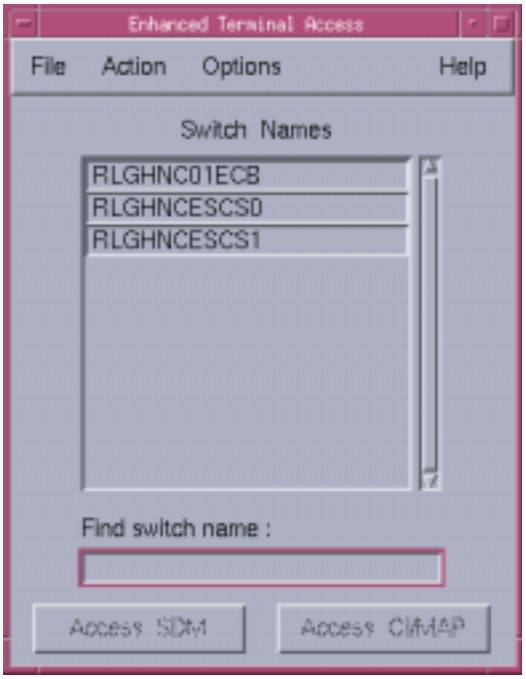
4 Enter your DCE userid in the field **Principal name**

5 Enter your DCE password in the field **Password.**

6 Click the **OK** button.

ETA displays a list of available CLLI.

Example of an ETA window



7 Select the CLLI of the switch with the SDM you want to access. If necessary, use the scroll bar on the right side of the list.

Example of an ETA window

8 Access the SDM by clicking the **Access SDM** button.

ETA connects to the SDM.

Example response:

```
There is 1 local login.
There are 3 ETA logins to the SDM.
There is 1 ETA logins to the CM.

Current SDM status:
SDM     CON     512     NET     APPL     SYS     HW
  .       .      ..       .        .       .       .
                 ..

maint:
```

Note: Once connected to the core, if you lose your connection, the core will drop your login session within five seconds. If your login id is not released by the core after that time, then login to the core with another userid and manually end the original login session.

9 Close all SDM sessions before you quit ETA. To close an SDM session, exit at the command prompt:

> exit

10 To quit ETA, select Exit from the File menu in the main ETA window.

11 You have completed the procedure.

Connecting to the SDM with SDMRLOGIN

Purpose

Use the following procedure to access the SDM from the Core with the SDMRLOGIN command.

Note: Connecting to the SDM in order to connect to the Core is not recommended. Connect to the Core as a passthru user instead.

Prerequisites

This procedure requires the following information:

- SDM userid
- SDM password

Note: SDMRLOGIN is supported only on DS-512 connected core managers.

Procedure

Perform the following steps to complete this procedure.

At the MAPCI

1 Start an SDMRLOGIN session.

> sdmrlogin

The Core starts a telnet session to the SDM and prompts for a login.

2 Enter your *SDM* userid.

The screen prompts for a password.

3 Enter your SDM password.

The Core connects to the SDM.

- The screen displays login history information
- The prompt changes to SDM>.

Note: Once connected to the core, if you lose your connection, the core drops your login session within five seconds. If your login id is not released by the core, then login to the core with another userid and manually end the original login session.

4 Quit the SDMRLOGIN session and return to the MAPCI level where you began this procedure.

> logout

5 You have completed this procedure.

Example

The following figure shows an example of an **SDMRLOGIN** session.

```
>sdmrlogin
SDM IP address is 47.245.8.70

SDM Remote Logins command in progress. Please wait...

telnet (brtppycf1)
AIX Version 4
(C) Copyrights by IBM and by others 19982, 1994.
login:
>maint
Password:
>
************************************************************
**
**
**               This is a private database.
**          All activity is subject to monitoring.
**      Any UNAUTHORIZED access or use is PROHIBITED.
**
**
**
************************************************************
Last unsuccessful login: Wed Jul 2 11:02:26 EDT 1997 o
Last login: Thu Jul 3 12:05:35 EDT 1997 on /dev/pts/2
SDM>
```

Connecting to another node as a passthru user

Purpose

Use following procedures to connect to another node through the SDM as a passthru user. The following types of connections are supported:

- Telnet to a node logically behind the SDM
- File Transfer Protocol (FTP) to the Core
- Secure Core File Transfer (SCFT) to the Core

A passthru connection occurs through the SDM. A passthru connection does not allow you to perform operations on the SDM.

Prerequisites

This procedure requires the following information and applications:

- Passthru userid and password

  Note: FTP access to the Core requires a password.

- Userid and password of destination node

  Note: FTP access to the Core does not require a destination userid and password.

- Secure File Transfer (SFT) installed on the SDM if you wish to FTP to the Core.

Procedures

Connecting to another node using telnet

At the workstation

1 Telnet to the SDM, and log in using your passthru user ID and password (if prompted).

A telnet connection is established to the destination node.

2 At the prompt, enter your user ID and password to log in to the destination node.

3 You have completed this part of the procedure.

Connecting to the Core using FTP

At the workstation

1 FTP to the SDM, and log in using your passthru user ID and password.

The prompt changes to `ftp>`

2 Connect to the Core:

ftp> site cm

Note: Once connected to the core, if you lose your connection, the core drops your login session within five seconds. If your login id is not released by the core, then login to the core with another userid and manually end the original login session.

3 You have completed the procedure.

Connecting to the Core using SCFT

At the workstation

1 Enter a command.

Note: Once SCFT is installed, you have a choice of several commands, which are listed in yStarting an SCFT client session.

2 You have completed the procedure.

Adding CM userIDs and passwords for ETA and ATA clients

ATTENTION
To complete this procedure, the DCE userids must have been configured. Refer to procedure Creating a DCE user on page 43 in this document.

You must configure CM userIDs and passwords and add them to a list of ERA values for each ETA client principal account. When the ATA or ETA client requests a MAP/CI session, the ETA server obtains the client CM userID and password ERA values, and uses them to log in to the switch for the client.

Use the following procedure to add ERA values for CM userIDs and passwords.

Adding CM userIDs and passwords

At the client workstation

1 Log into the client workstation.

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, and press the Enter key.

4 Access the bin directory:

cd /sdm/bin

and pressing the Enter key

5 Add the ERA value for the CM userID and password by typing

./add_cm_userid <principal_name> <CM_userID_list> [<CM_password_list>]

where

<principal_name>
is the DCE userID

<CM_userID_list>
s the CM userIDs

[<CM_password_list>]
is all CM passwords (optional)

Note 1: A CM userID can appear more than once.

Note 2: The CM password list is optional. If you do not provide this information, the add_cm_userid command automatically assigns * for each password. The password can then be changed through the ATA or ETA client (refer to procedure “Changing CM passwords from the ETA client” and “Changing CM passwords from the ATA client” in this document). If you provide this information, align each CM userID and password so that the first password corresponds to the first userID.

Example
./add_cm_userid ops_1 “admin cmap5 cmap8” “a_pwd pwd_5 pwd_8“

Three CM user accounts are created for the ATA or ETA client ops_1. The password for the admin userID is a_pwd; for the cmap5 userID, pwd_5; for the cmap8 userID, pwd_8.

Example
./add_cm_userid ops_1 “admin admin admin” “a_pwd pwd_5 pwd_8”

The CM admin userID has three different passwords (pwd_1, pwd_2 and pwd_3). Each password is used to access different switches.

6 You have completed this procedure.

You can proceed to the procedure Adding SDM userIDs and passwords for ETA and ATA clients on page 105 if you want to allow users access to the SDM using the ETA application.

Adding disks and creating a logical volume in datavg

Purpose

Use this procedure to add disks and create logical volumes in datavg.

Application

Use this procedure to

- add disks to the data volume group (datavg)
- create a new logical volume in the datavg

Note: The maximum number of datavg disks that can be provisioned on an SDM is 11 pairs.

ATTENTION
This procedure must be performed by a trained Advanced Interactive Executive (AIX) system administrator who has root user privileges to access the SDM.

ATTENTION
Perform this procedure after your system has been installed with the required I/O controller modules installed, in pairs, in the main or I/O expansion chassis. If you have not installed the required modules, refer to the procedure “Adding I/O controller Modules” in the SDM Upgrades document.

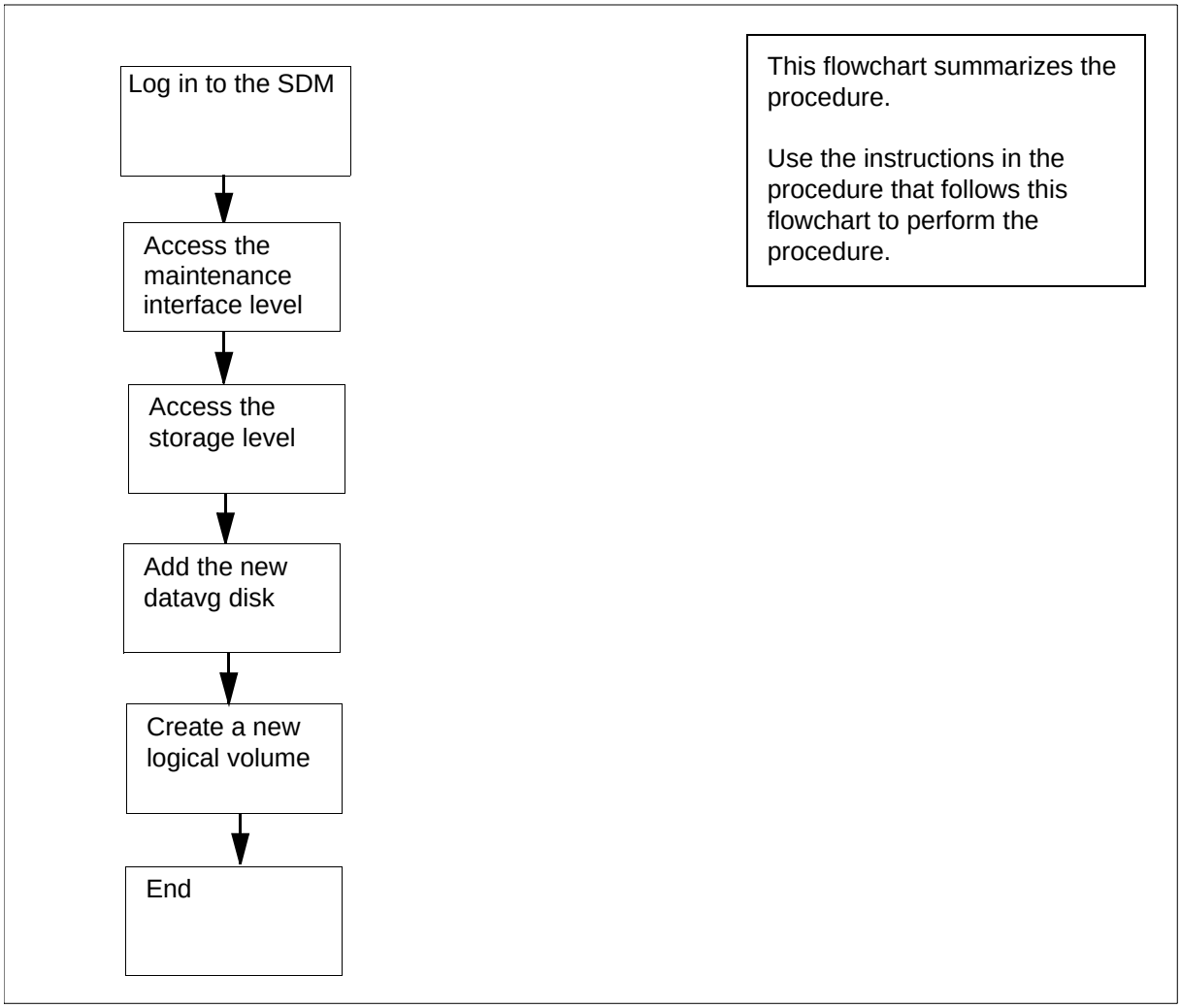
If you have a root volume group (rootvg) system, and you want to add datavg to your system, use the procedure “Migrating from a rootvg system to a rootvg/datavg system” in the SDM Upgrades document.

ATTENTION
The logical volume management feature allows you to create no more than 32 logical volumes.

Action

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

Summary of adding disks and creating a logical volume in datavg



Adding disks and creating a logical volume in datavg

At the local VT100 console

1 Log in to the SDM as the root user.

2 Access the maintenance interface:

 # sdmmtc

3 Access the storage menu level:

> storage

Example response:

```
Volume Group            Status            Free
(MB)   rootvg              mirrored
608
datavg                mirrored             7872

Logical Volume   Location
1 /             rootvg     20             25/ 80
2 /usr          rootvg     192            85/ 90
3 /var          rootvg                    11/ 80
4 /tmp          rootvg     24              6/ 90
5 /home         rootvg     300             4/ 70
6 /sdm          rootvg      300           44/ 90
7 /data         datavg     300           20/ 80
Logical volumes showing: 1 to 7 of 7
```

Note: The example response shows part of the information displayed at the storage level.

4 Determine your next step with regards to I/O modules.

If you have	Do
added an Input/Output (I/O) module and you want to add the module to the datavg before you create your logical volume	step 5
not added an I/O module and you have enough free disk space for the logical volume that you want to create	step 6

5 Add a new disk:

> add vg

Example response:

```
The following disks will be added to the system:

Datavg is currently being created...
```

The system informs you when the disk has been added successfully.

Example response:

```
All disks were successfully added.

Command complete.
```

Note 1: This step automatically adds the new disks to the datavg.

Note 2: An error message is displayed if the disks are not added successfully. If this occurs, contact the personnel responsible for the next level of support.

6 Create the new logical volume:

> add lv <xxx> <Mbyte>

where

<xxx> is the new logical volume name

<Mbyte>
is ithe size of the logical volume in Mbyte

Example response:

```
Creating volume XXX.
```

Example response:

```
Creating Volume XXX ...
Volume Successfully Created...
Volume was created...
Command complete
```

7 You have completed this procedure.

Adding or removing a maintenance user

Purpose

Use this procedure to add or remove a maintenance class user.

Application

Use this procedure to add or remove a maintenance class user. This procedure must be performed by the root user.

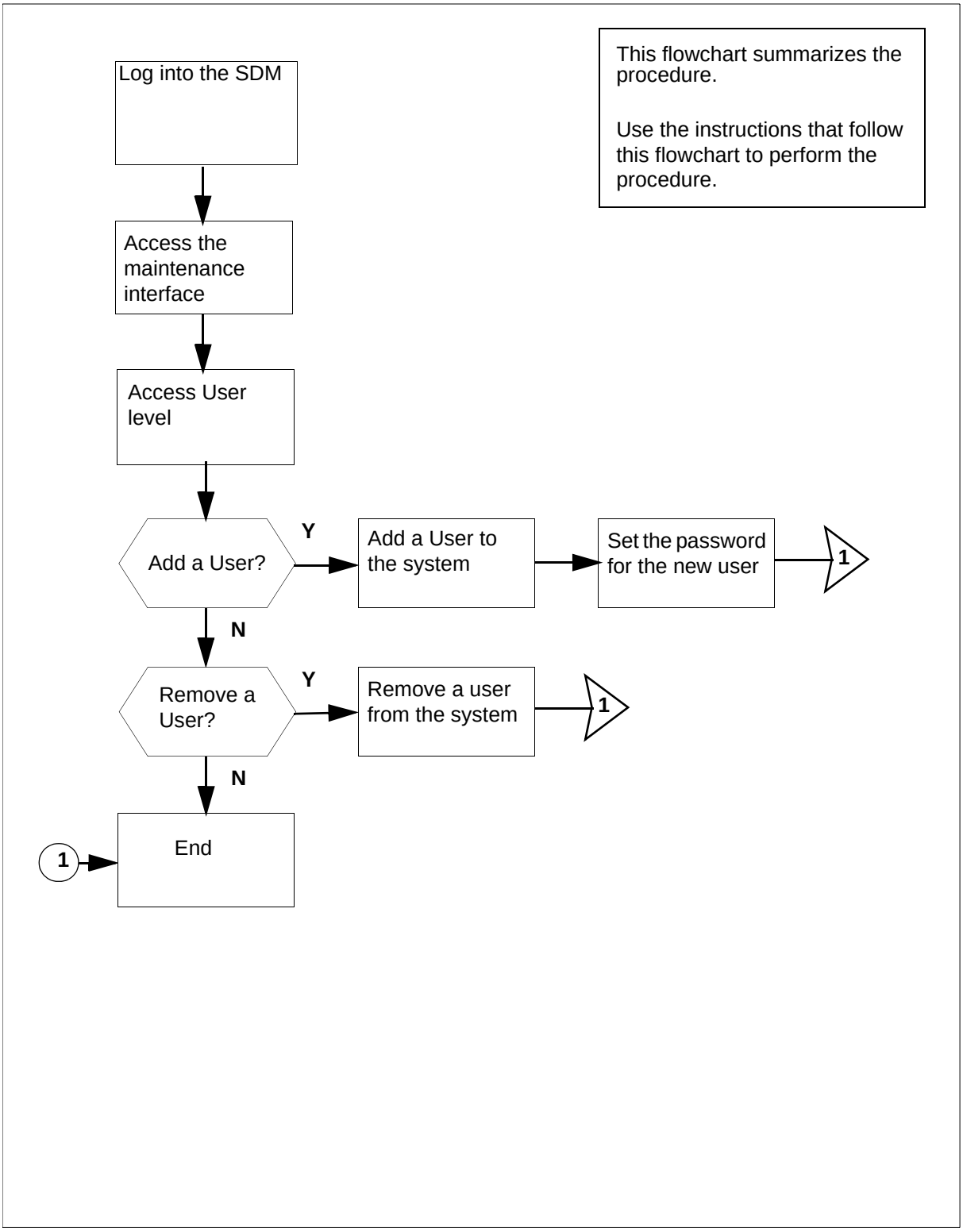
ATTENTION

For the current release, there is *no limit* to the number of telnet sessions allowed for maintenance and passthru users. For previous releases, a total of 16 telnet sessions is allowed.

Action

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

Summary of Adding or removing a maintenance user



Adding or removing a maintenance user

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 User level:

> user

Response:

4 Use the following table to determine your next step.

If you want to	Do
add a user	step 5
remove a user	step 10

5 Add a maintenance class user:

> add <userID>

where

<userID> is the userID of the new user

Note: To activate a user, you need to set the password. Use the change command to set the password.

6 Set password for the user:

> change <userID>

where

<userID> is the userID of the user for whom you are setting the password

Note: If no userID is specified, the system changes the password of the root user.

7 Enter the password for the new user, and press the Enter key.

The password must be at minimum a six-character string containing at least one alphabetic character, and at least one numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

8 Enter the password again.

9 Press Enter again to continue.

If you	Do
want to add another user	step 5
do not want to add another user	step 12

10 Remove a user:

> delete <userID>

where

<userid>
is the userID of the new user

```
Are you sure you want to delete this user?
Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N"):
```

11 Confirm that you want to delete the user:

> y

If you	Do
want to delete another user	step 10
do not want to delete another user	step 12

12 Exit the maintenance interface:

> quit all

13 You have completed this procedure.

Adding or removing passthru users

A passthru user is an SDM user ID that is used to connect to a node that is logically behind the SDM in a network, such as the CM or XA-Core. A passthru user cannot perform any functions on the SDM itself.

ATTENTION

For the *current release*, there is *no limit* to the number of telnet sessions allowed for maintenance and passthru users. For previous releases, a total of 16 telnet sessions is allowed.

You can configure a passthru user ID with or without a password. However, a password is required to transfer or retrieve files to or from a node using FTP. The Secure File Transfer (SFT) application must be installed on the SDM to use FTP with a passthru user ID. SFT must be configured in either Normal FTP access mode or Secure and Normal FTP access mode. Refer to the following SFT procedures:

- “Installing the SFT server software
- “Configuring the SFT server application software”
- “Transferring and retrieving files using SFT”

Note: The Distributed Computing Environment (DCE) is not required for SFT, but it can add more security to the file transfer environment.

Use the following procedure to add or remove one or more passthru users. You can change the information for an existing passthru user using the Change command.

Adding or removing passthru users

At the SDM

1 Log into the SDM using the root user ID an password.

2 Access the passthru level:

sdmmtc passthru

3 Create or delete a passthru user.

If you want to	Do
add a passthru user	step 4
delete a passthru user	step 13

4 Add a passthru user:

> **add**

5 When prompted, enter the user name for the new user (for example, `cmusr`).

6 When prompted, enter the real name for the passthru user (for example, `CM passthru`).

7 When prompted, type the telnet command arguments for the passthru user.

Note: The telnet command arguments can be the hostname or the IP address of the destination node. If you are adding a user ID that is used to connect to the CM or XA-Core, the telnet command arguments must be `cm`.

8 When prompted, indicate whether a password is required.

Note: A password is required for user IDs that is used to connect to the CM or XA-Core using FTP.

9 When prompted, confirm the data you entered:

> y

If you indicated a password	Do
is required	step 10
is not required	step 12

10 When prompted to set the initial password, enter a password.

11 When prompted, re-enter the password to confirm it.

Note: The user who accesses the SDM for the first time using this new passthru user ID, is first prompted for the initial password and then prompted to change it.

12 Add another user or finish this procedure.

If you	Do
want to add another user	step 4

If you	Do
do not want to add another user	you have completed this procedure

13 To delete the passthru user:

> **delete <username>**

and pressing the Enter key.

where

<username>
is the user ID of the user you want to delete

14 When prompted, confirm you want to delete the user:

> **y**

and pressing the Enter key.

15 Use the following table to determine your next step.

If you	Do
want to delete another user	step 13
do not want to delete another user	you have completed this procedure

Adding SDM userIDs and passwords for ETA and ATA clients

You must set an ERA value for the SDM userID of the ETA client using the add_sdm_userid command. When an ATA or ETA client initiates an SDM session, the ETA server obtains the ERA value for the SDM userID of that client. The value is used to start an SDM session.

Use the following procedure to set an ERA value for an SDM userID.

ATTENTION
To complete this procedure, you must have created the DCE principals for the ETA and ATA users. Refer to procedure Creating a DCE user on page 43 in the Security and Administration section.

Adding userIDs for the ATA and ETA client

At the client workstation

1 Log into the client workstation.

2 Log into DCE using the administrator userID:

> dce_login <DCE_admin_user>

where

<DCE_admin_user>
is your administrator userID

3 Enter your DCE password.

4 Access the bin directory:

> cd /sdm/bin

5 Add the ERA value for the userID:

> ./add_sdm_userid <principal_name> <sdm_userid>

and pressing the Enter key.

where

principal_name
is the DCE userID you wish to set ERA values for

sdm_userid
is the userID you wish to have

6 You have completed this procedure.

Assigning the master server for DCE

Purpose

Use this procedure to assign the DCE master server.

Application

ATTENTION
This procedure can cause some side effects on your DCE cell. You must be a Distributed Computing Environment (DCE) system administrator to perform this procedure. Perform this procedure with caution.

Use this procedure to perform one of the following items:

- assign a new master CDS clearinghouse
- exclude a replica CDS clearinghouse
- assign a new master security server
- remove a replica security server

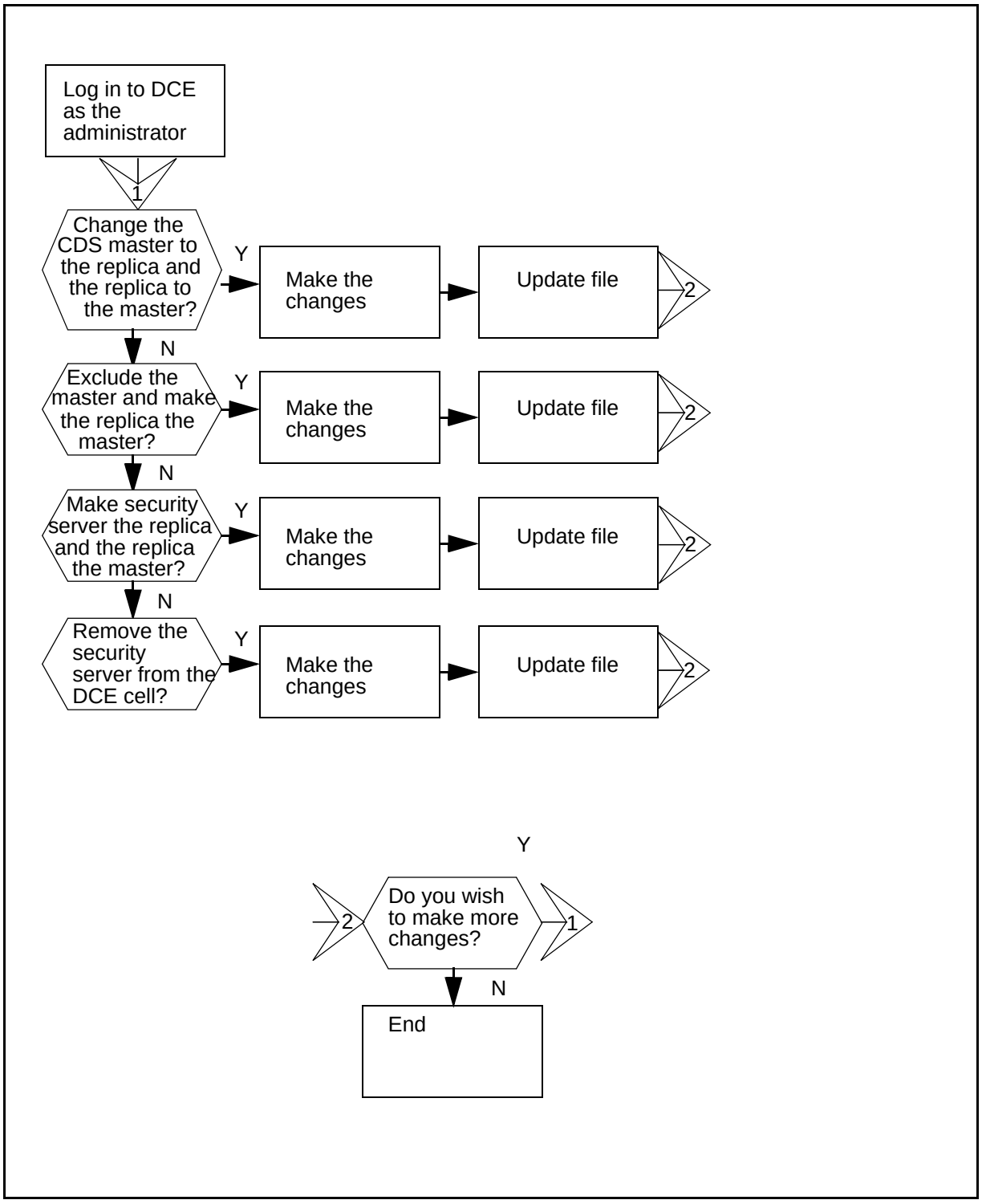
Interval

Perform this procedure to reconstruct the DCE cell.

Action

The flowchart that follows provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to perform the procedure.

Summary of assigning the master server for DCE



Assigning the master server for DCE

At the local or remote VT100 console

1 Login to the DCE cell as an administrator:

> dce_login <*principal name*>

and pressing the Enter key.

where

principle name
is the user ID of the administrator.

2 Determine which DCE re-mastering script to run.

If you are	Do
assigning a new master CDS clearinghouse	step 3
excluding a replica CDS clearinghouse	step 6
assigning a new master security server	step 9
removing a replica security server	step 12
not making any changes	step 14

3 Assign a new master CDS clearinghouse:

> /sdm/bin/remaster_cds_server master <new_master_hostname> replica <replica_hostname_list>

where

<new_master_hostname>
is the host name of the master server.

<replica_hostname_list>
is the list of hostnames for replica servers that remain in the CDS replica clearinghouse set.

4 Confirm the request:

> yes

After you confirm your request, the system displays the following response:

```
Remastering CDS server...
   Remastering/.:...
   Remastering/.:...
```

5 Update the cds_cache.wan file:

> .sdm/bin/update_cds_cache_wan

Return to step 2 to determine your next step.

6 Exclude a list of replica CDS clearinghouses:

> /sdm/bin/remaster_cds_server master <master_host_name> replica <replica_hostname_list> exclude <exclude_replica_hostname_list>

where

<master_hostname>
is the host name of the new master server.

<replica_hostname_list>
is the list of host names for replica servers.

<exclude_replica_hostname_list>
is the list of host names of replica servers you want to exclude from the CDS replica clearinghouse set.

7 Update the cds_cache.wan file:

> /sdm/bin/update_cds_cache_wan

8 Return to step 2 to determine your next step.

9 Assign the new master security server:

> /sdm/bin/remaster_sec_server <new_master_server_hostname>

where

<new_master_server_hostname>
is the hostname of the new DCE master security server.

10 Update the cds_cache.wan file:

> /sdm/bin/update_pe_site

11 Return to step 2 to determine your next step.

12 Remove the replica security server:

> /sdm/bin/remove_sec_server_data <replica_security_server_hostname>

where

<replica_security_server_hostname>
is the hostname of the replica security server you want to remove from the DCE cell.

13 Update the cds_cache.wan file:

> /sdm/bin/update_pe_site

and pressing the Enter key.

Return to step 2 to determine your next step.

14 You have completed this procedure.

Removing ERA values for CM userIDs and passwords

Purpose

Use the following procedure to remove ERA values for CM userIDs and passwords.

Application

The remove_cm_userid command removes ERA values for CM userIDs and passwords.

Removing ERA values for CM userIDs and passwords

At the client workstation

1. Log into the client workstation.
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. Change to the bin directory:

   cd /sdm/bin
5. Remove the ERA value for the CM userID and password:

   > ./remove_cm_userid <principal_name>

   where

   <principal_name>
   is the CM userID for the ERA value to remove
6. You have completed this procedure.

Removing DCE port restrictions

Purpose

Use the following procedure to return the SDM to the system default values.

Application

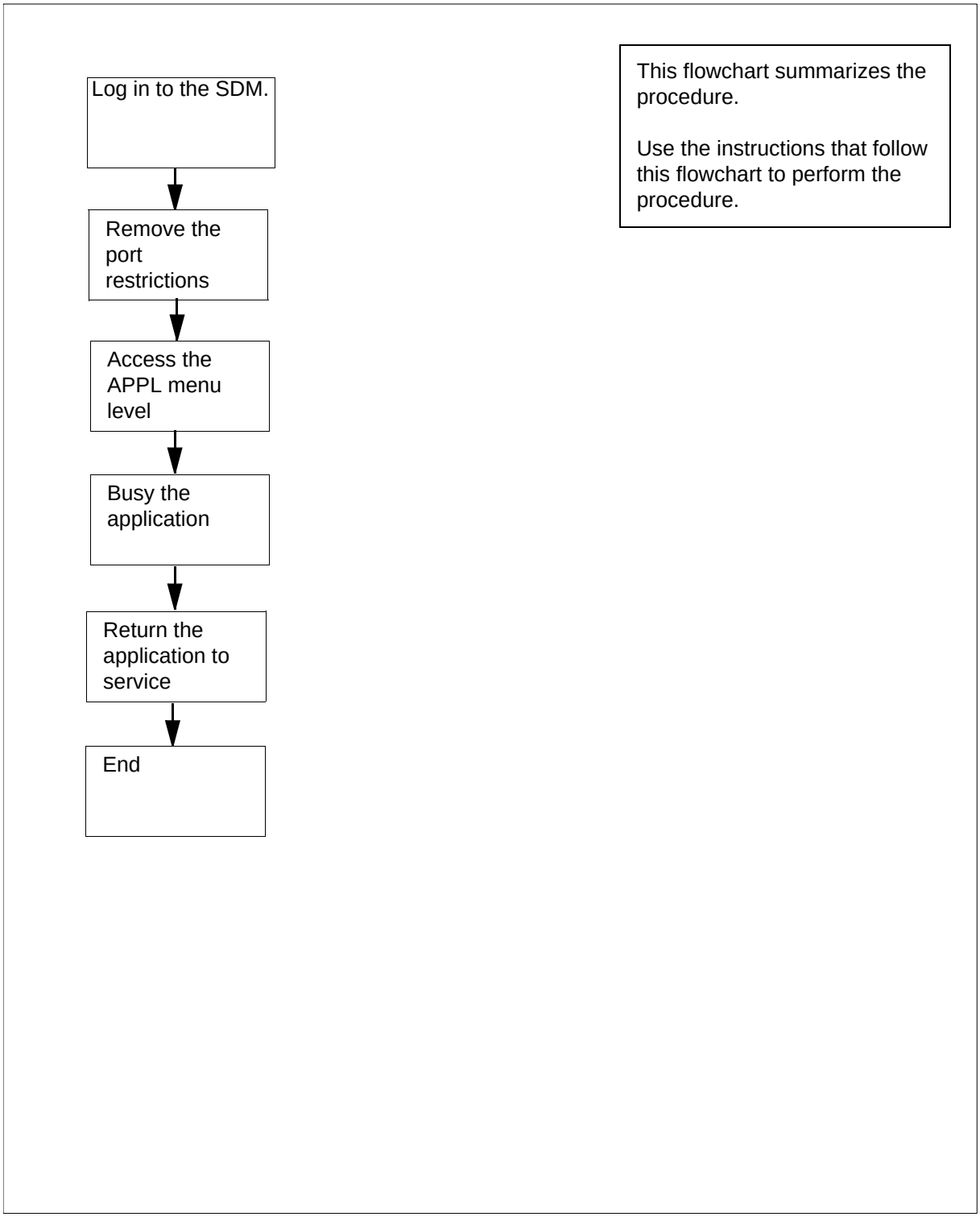
ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator who knows DCE administration procedures.

DCE ports will be randomly assigned when you complete this procedure. You must log in as the root user to perform this procedure.

Action

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

Summary of removing DCE port restrictions



Removing DCE port restrictions

At the client workstation

1 Log in to the SDM as the root user

2 Restrict the ports to an SDM-defined range:

 # restrict_dce_ports unrestricted

Example response:

```
DCE servers port range restrictions have been
removed.
```

3 Access the maintenance interface:

 # sdmmtc

4 Access the NET level:

> net

5 Wait for DCE to go to InSv. This may take several minutes.

Example response:

```
DCE State:  .
```

6 Access the application (appl) level:

> appl

Example response:

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

7 Determine the key number for the application (shown under the header “#”).

8 Manually busy the application software:

> bsy <n>

where

<n>
is the number next to the application to busy

Example response:

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

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

9 Confirm the Busy command:

> y

After you confirm the Bsy command, the following is displayed:

```
Application Bsy - Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappears. The word “initiated” also changes to “submitted”:

```
Application Bsy - Command submitted.
```

10 Return the application to service:

> rts <n>

where

<n>
is the number next to the application you busied previously

Example response:

```
Application RTS - Command initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

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

11 You have completed this procedure.

Removing the ERA value for the userID

Purpose

Use the following procedure to remove the ERA value for the userID.

Action

Removing the ERA value for the userID

At the client workstation

1. Log into the client workstation.
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. Access the bin directory:

   > cd /sdm/bin
5. Remove the ERA value for the userID:

   ./remove_sdm_userid <principal_name>

   where

   <principal_name>
   is the userID for the ERA value you are removing
6. You have completed this procedure.

Restricting DCE ports to a predefined range

Purpose

Use the following procedure to restrict the ports to a range that is predefined by the SDM software.

Application

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

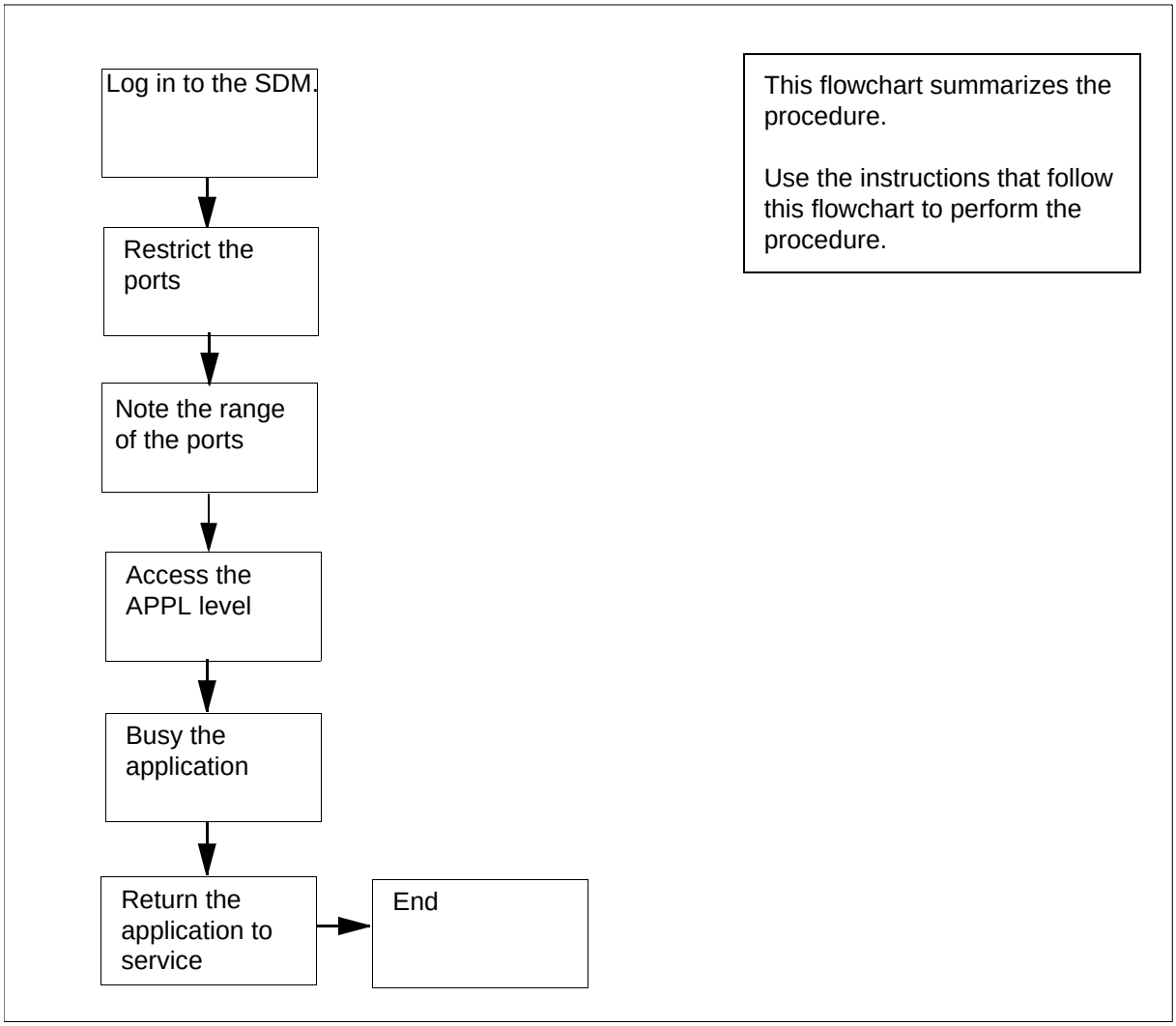
The range of ports must be compatible with other SDM applications.

You must have root user privileges to perform this procedure.

Action

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

Summary of restricting DCE ports to a predefined range



Restricting DCE ports to a predefined range

At the client workstation

1 Log in to the SDM as the root user.

2 Restrict the ports to an SDM-defined range:

 # restrict_dce_ports system_defined

Response:

```
The following port ranges have been configured
   TCP: 4500-4540    UDP: 4500-4540
Killing and restarting SDM's DCE daemons for the
change to take effect...
Stopping DCE daemons:
killing dced

Please run sdmmtce tool:
under the Mtc/LAN level: wait for DCE state to
change to InSv.
under the MTC/Appl level: BSY and then RTS any
application that uses DCE.
```

3 Record the range of ports that are printed by the script. Use these values for the firewall configuration.

4 Access the maintenance interface:

 # sdmmtc

5 Access the NET menu level:

> net

6 Wait for DCE to go to InSv. This may take several minutes.

Example response:

```
DCE State:    .
```

7 Access the application (Appl) level:

> appl

Example response:

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

8 Determine the key number for the application (shown under the header "#").

9 Busy the application software:

> bsy <app_no>

where

<app_no>
is the number next to the application to busy

Response:

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

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

10 Confirm the Busy command:

> y

After you confirm the Bsy command, the following is displayed:

```
Application Bsy- Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application Bsy - Command submitted.
```

11 Return the application to service:

> rts <num>

where

<num>
is the number next to the application you previously busied

Example response:

```
Application RTS - Command initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

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

12 You have completed this procedure.

Restricting DCE ports to a specific range

Purpose

Use the following procedure to restrict the ports to a specific range.

Application

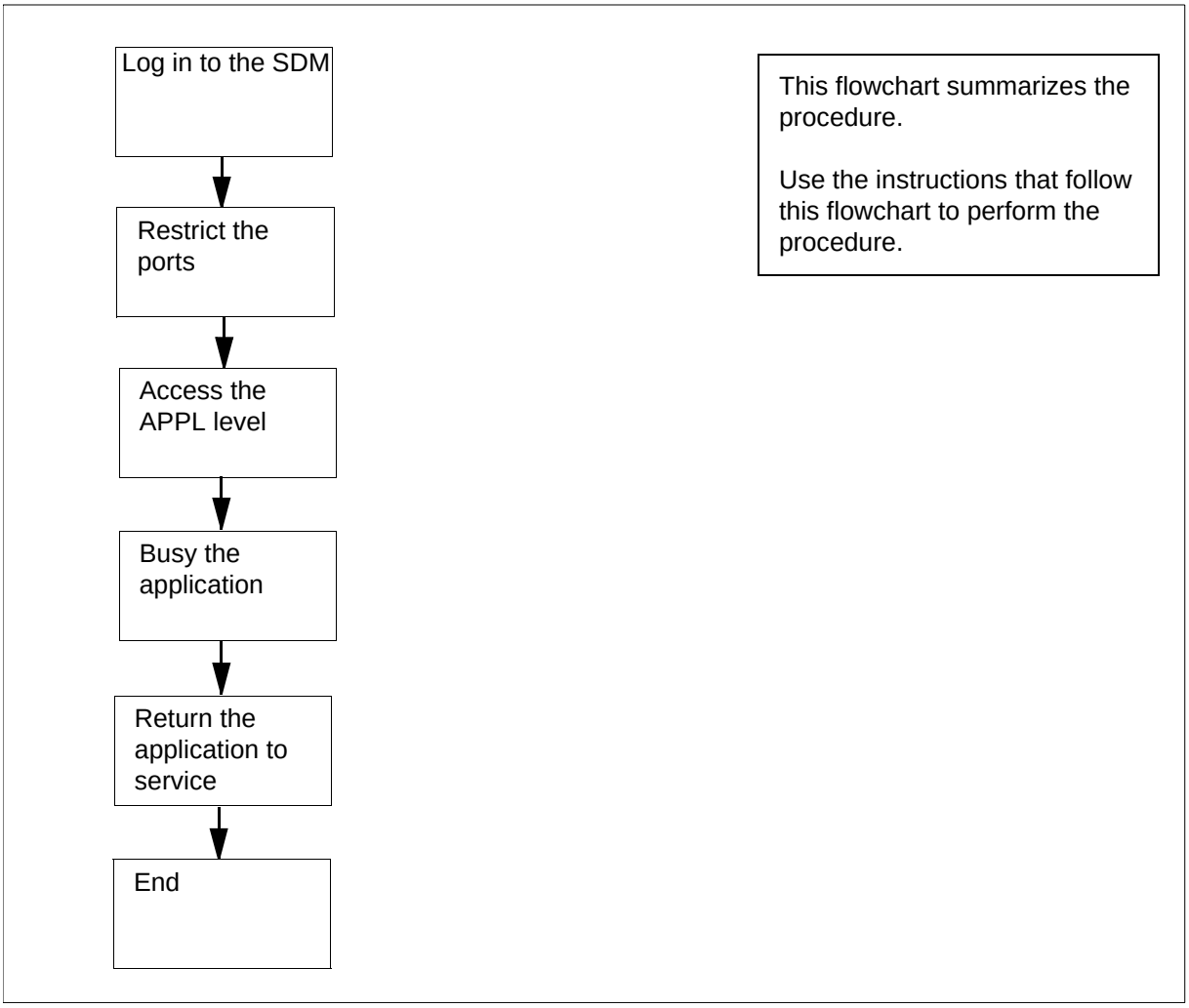
ATTENTION
This procedure must be performed by a trained Distributed Computing Environment (DCE) system administrator.

You must have root user privileges to perform this procedure.

Action

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

Summary of restricting DCE ports to a specific range



Restricting DCE ports to specific range

At the client workstation

1 Log in to the SDM as the root user.

2 Restrict the ports to an SDM-defined range:

 # restrict_dce_ports tcp <start_TCP>:<end_TCP> udp <start_UDP>:<end_UDP>

where

<start_TCP>
is the start of the range for TCP ports (must be greater than 1024)

<end_TCP>
is the end of the range for TCP ports (must be less than 32 000)

<start_UDP>
is the start of the range for universal datagram protocol (UDP) ports (must be greater than 1024)

<end_UDP>
is the end of the range for UDP ports (must be less than 32 000)

Example response:

```
The following port ranges have been configured
      TCP: 3000-3050        UDP: 3000-3050
```

3 Access the maintenance interface:

 # sdmmtc

4 Access the NET level:

> net

5 Wait for DCE to go to InSv. This can take several minutes.

Example response:

```
DCE State:     .
```

6 Access the application (APPL) level:

> appl

Example response:

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

7 Determine the key number for the application (shown under the header “#”).

8 Busy the application software:

> bsy <app_no>

where

<app_no>
is the number next to the application to busy

Example response:

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

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

9 Confirm the Busy command:

> y

10 After you confirm the Bsy command, the following is displayed:

```
Application Bsy - Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

```
Application Bsy - Command submitted.
```

11 Return the application to service:

> rts <app_no>

where

<app_no>
is the number next to the application you busied previously

Example response:

```
Application RTS - Command initiated.
Please wait...
```

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”:

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

12 You have completed this procedure.

Setting SFT access permissions

Purpose

Use the following procedure to set the SFT access permissions for an SFT client.

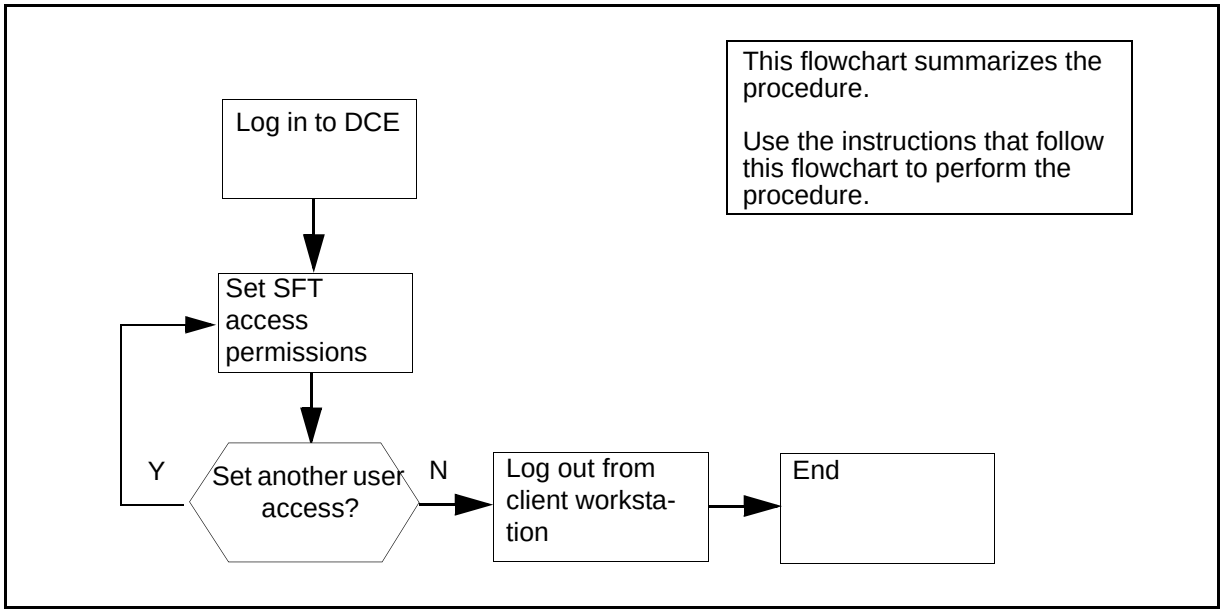
Application

The default permission for the SFT user is none. If you do not perform this procedure, the user does not have access to SFT

Action

The following flowchart summarizes the procedure. To complete the procedure, perform the procedures that follow the flowchart.

Summary of setting the SFT access permission



Setting the SFT access permissions

At a UNIX prompt on the client workstation:

1 Log in to DCE as the DCE administrator:

 # dce_login <admin_name>

where

<admin_name>
is the userID for the administrator account

2 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>

where

<DCE_principal>
is the DCE userID whose access permissions you are changing.

<SFT_permission>
is the access permission level for the user. Values are as follows:

- none (access is not permitted to the SFT services - default value)
- sdm_only (access is permitted to the SDM
- sdm_cm (access is permitted to both the SDM and the CM

5 Repeat step 4 to set SFT access for another user.

6 Log out from the client workstation:

 # exit

7 You have completed this procedure.

Setting the time zone, or the date and time

Application

Use this procedure to set the time zone, or the date and time on the SDM. Once you have entered the new time zone, or the date and time, the values are recalculated from the system clock and displayed on the screen to confirm the change.

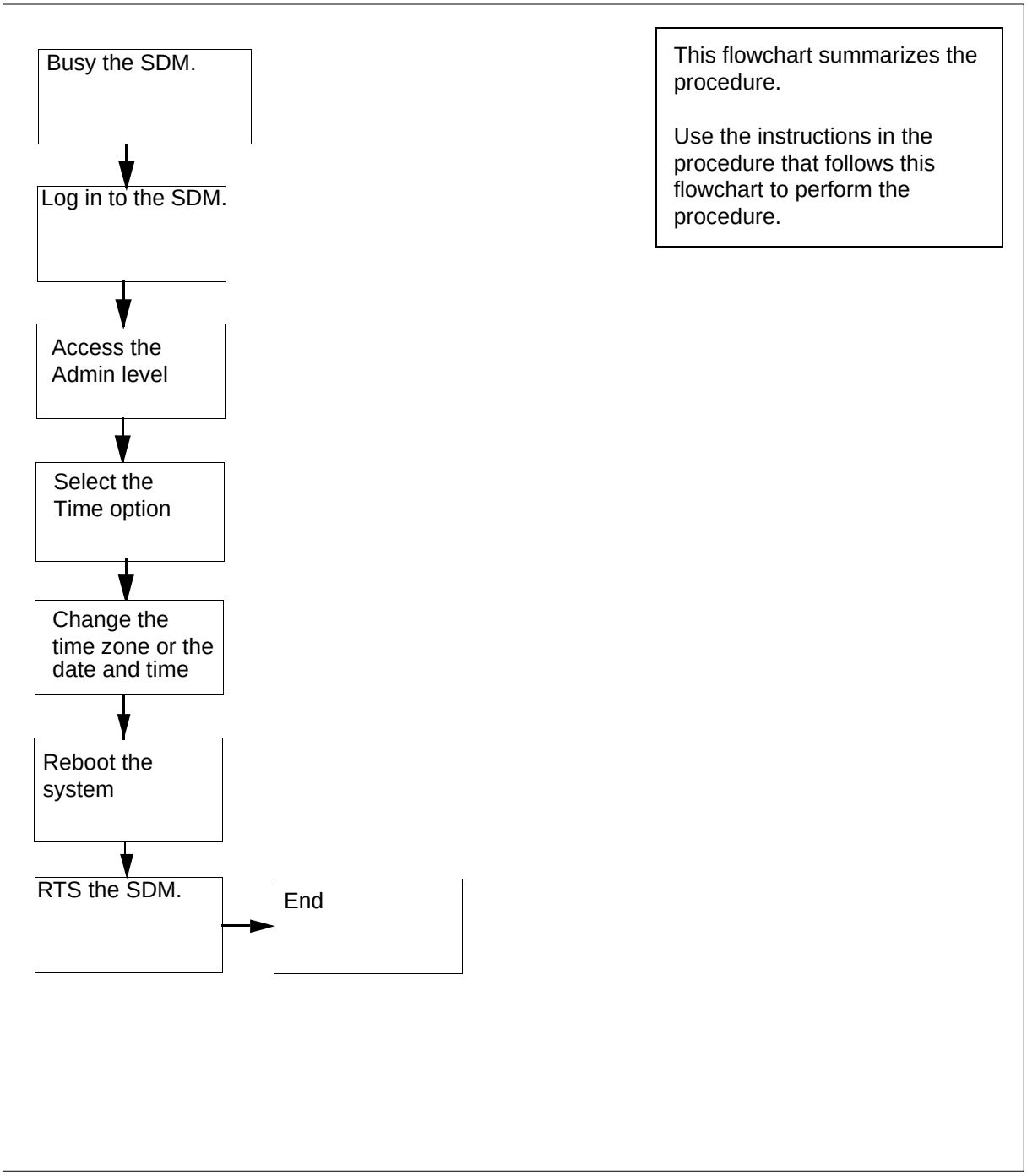
You must reboot the SDM after changing the time zone, or the date and time for the changes to take effect.

Note: This procedure tells you how to set or change the time zone or the date and time. This procedure does not allow you to set or change the time zone, date and time all together. You must complete the procedure once for setting or changing the time zone and again for setting or changing the date and time.

Action

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

Summary of setting the time zone, or the date and time



Setting the time zone, or the date and time

ATTENTION
This procedure must be performed only by UNIX system administration personnel who have root user permissions for accessing the SDM.

ATTENTION
The time zone, date and time on the SDM cannot be changed when DCE is operational. The SDM must also be in ManB or OffL state to change the time zone, date and time.

At the MAP display

1 Access the SDM from the APPL level of the MAP display by typing

```
> mapci;mtc;appl
```

and pressing the Enter key.

2 Use the following table to determine your next step.

If the SDM node state is	Do
in service (InSv)	step 4
anything else	step 3

3 A fault exists on the SDM, or another SDM maintenance activity is already in progress. Clear the fault or complete the maintenance activity, as appropriate. Clear the faults by checking for SDM-related alarms under the APPL header of the MAP display alarm banner, and use the appropriate alarm clearing procedure in the Fault Management category of documents to clear the fault before continuing this procedure.

4

CAUTION
Loss of service
Manually busying the SDM shuts down all applications without warning to the application users.

Busy the SDM by typing

> bsy

and pressing the Enter key.

Response:

```
SDM is in service.
This command will cause a service interruption.
Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

5 Confirm the Bsy command by typing

> y

and pressing the Enter key.

Response:

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

At the local or remote VT100 terminal

6 Log into the SDM as the root user.

7 Use the following table to determine your next step.

If you are configuring	Do
date and time	step 12
time zone	step 8

8 Configure the time zone by typing

 # sdmconfig

and pressing the Enter key.

9 Select the date and time zone by typing

> 2

and pressing the Enter key.

10 Refer to the procedure Recommissioning date and time zone in the Security and Administration section to configure the time zone. Return to this procedure after configuring the time zone.

11 Proceed to step 21.

12 Access the maintenance interface level by typing

 # sdmmtc

and pressing the Enter key.

13 Access the administration (Admin) level by typing

```
> admin
```

and pressing the Enter key.

14 Select Time by typing

```
> time
```

15 Confirm you want to proceed with the procedure by typing

```
> y
```

and pressing the Enter key.

16 The Change / Show Day and Time screen appears. Use the up and down arrows to move the cursor to a date or time entry you want to change. Repeat until you modify all the entries you want to change. Press the Enter key.

17 The Command Status screen appears. The command status is shown as “running” while the system processes the changes. The command status changes to “OK” when processing completes. The date, time and time zone appear.

18 Exit the command status screen by pressing the F10 key. You can also press the ESC key and the number 0 key to exit the screen.

At the SDM level of the MAP display

19 Reboot the SDM by typing

```
> rebootsdm
```

and pressing the Enter key.

Response:

```
Communication with the SDM will be down for
approximately 10 minutes.

Do you wish to proceed?

Please confirm (“YES”, “Y”, “NO”, or “N”):
```

20 Confirm that you want to proceed by typing

```
> y
```

and pressing the Enter key.

Response:

```
SDM 0 ManB                          Links_00S: .
/ RebootSDM in progress
SDM 0 RebootSDM initiated.
```

Note: The command response indicates that the command has been successfully received by the SDM. The maintenance flag, “Reboot SDM in progress” is displayed until the SDM recovers from the reboot. When the maintenance flag message disappears, continue with the next step.

21 Return the SDM to service by typing

```
> rts
```

and pressing the Enter key.

Response:

```
SDM InSv                            Links_00S:  .
SDM RTS initiated.
SDM RTS completed.
```

Note: If there are no other faults on the system, then the SDM applications automatically return to service immediately following the completion of the reboot.

22 You have completed this procedure.

Starting an FTP client

The following procedure describes how to start an FTP client.

Use the SFT client for secure FTP connections. Standard FTP userIDs and passwords are not encrypted when they are passed across the network.

CM FTP server

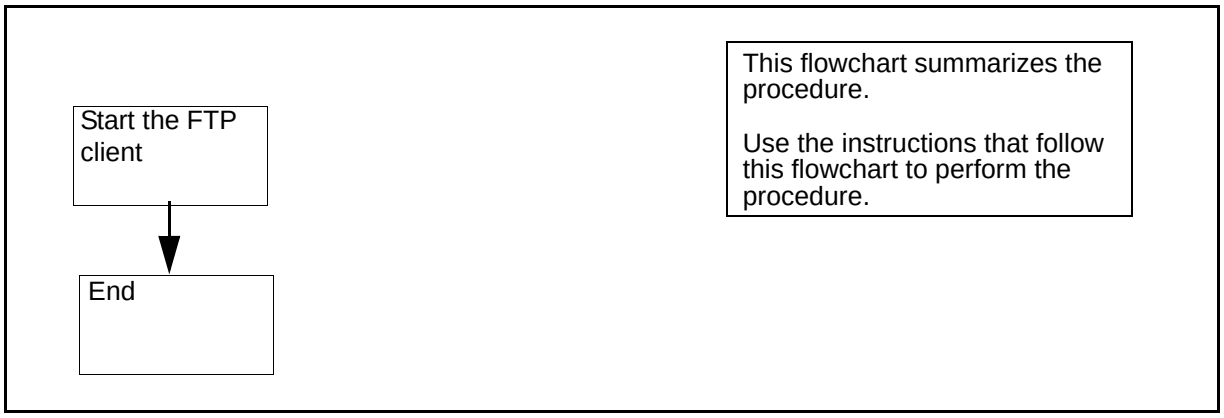
SFT and FTP clients can both access the CM FTP server by using the command SITE CM. You can use standard FTP commands with some exceptions.

The limits to standard FTP commands when accessing the CM FTP server are as follows.

- the user command is intercepted and disallowed by the SFT server. A user does not have to log in manually.
- the mkdir and rmdir commands are not supported by the CM FTP server. The CM file system contains volumes only. It does not support directory hierarchies within the volume.
- Files transferred to SFDEV are owned by the user $$SYS$$.
- SFT performs a clean-up routine after the SFT application is returned to service.
  If you attempt to use the SITE CM command immediately after the RTS command is issued, you may experience a delay of about 20 seconds before access to the CM is given.
- file names and volume names are case sensitive. Volume names are always in uppercase, for example, S01DVOL1. File names are usually in uppercase.

To complete the procedure for starting an FTP client, perform the procedure that follows the flowchart.

Summary of starting an FTP client



Starting an FTP client

At a UNIX prompt:

1 Start the FTP client workstation:

> ftp <address>

where

<address>
is the IP address, or the DNS address of the FTP server.

Note: The location of the FTP client varies.

2 You have completed this procedure.

Note: For additional instructions on FTP client usage, refer to the documentation for the client application.

Transferring files as a passthru user using FTPProxy

Application

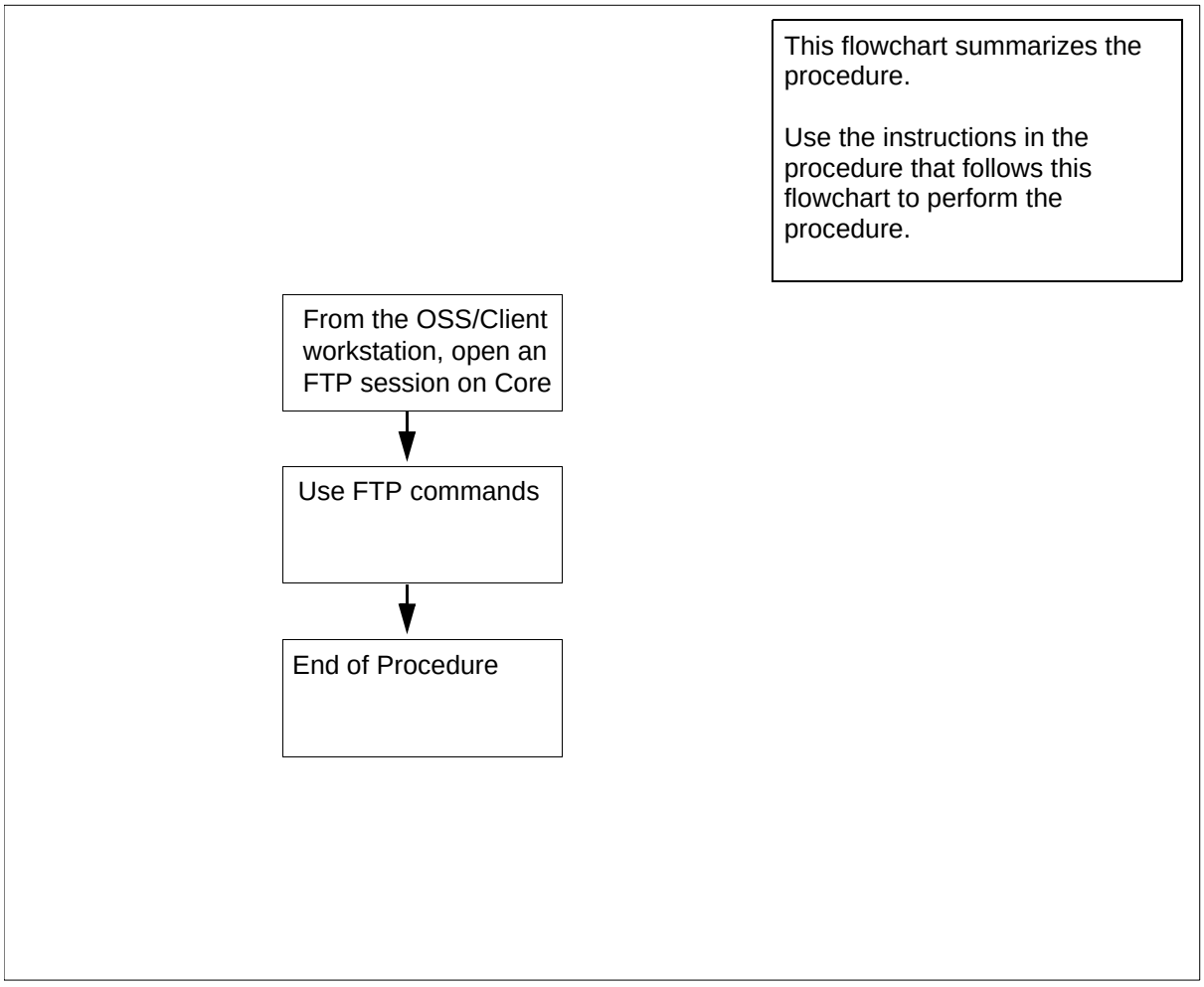
Use this procedure to transfer files between the OSS machine and the Core using the FTPProxy application. Use this procedure if you have passthru user privileges.

If you have core user privileges (mgcadm, mgcrw, mgcsprov, mgcmtce,and mgcro), refer to Transferring files as a core user using FTPProxy on page 143 in this document.

Action

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

Summary of transferring files as a passthru user using FTPProxy



Transferring files as a passthru user using FTPProxy

At the OSS/Client workstation

1 Open an FTP session.

a Log in to the SDM by typing

```
> ftp <IP address>
```

and pressing the Enter key.

where

<IP address>
is the IP address of the SDM.

b At the prompt, enter your userID.

c At the prompt, enter you password.

The FTPProxy application authenticates your userID and password and logs you in to the Core.

2 Use the commands in the table to transfer files.

If you want to	At the ftp> prompt, type the following command and press the enter key
transfer files in ASCII mode	ascii
transfer files in Binary mode	bin
get a file from the Core	get < filename on Core >
put a file to the Core from the OSS/client machine	put <filename on client machine>
list files on the Core - type	ls
- or type	dir
view the current directory on the core	pwd
log out of the ftp session	bye

3 You have completed this procedure.

Transferring files as a core user using FTPProxy

Application

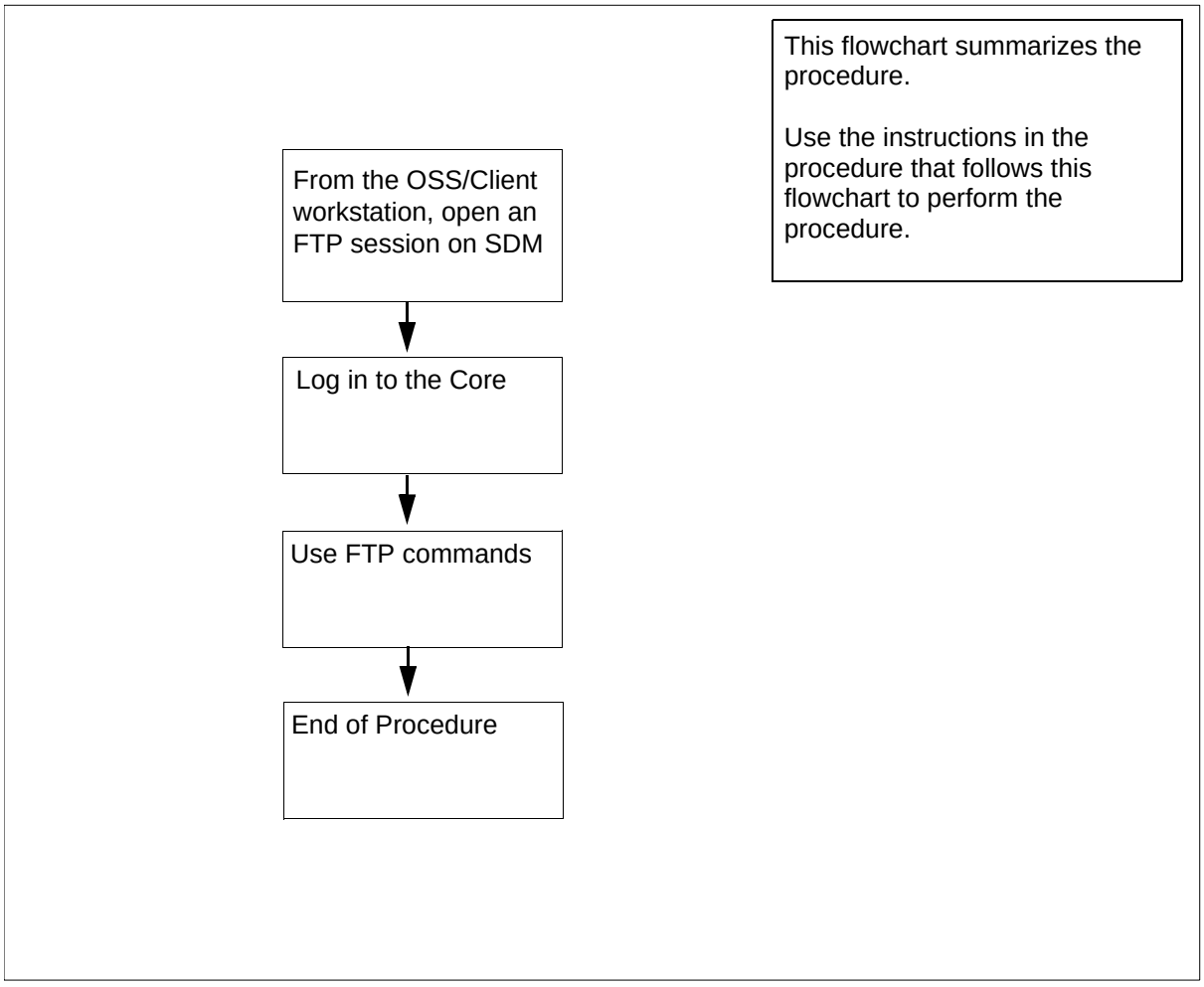
Use this procedure to transfer files between the OSS machine and the Core using the FTPProxy application. Use this procedure if you have core user privileges. Core user privileges include mgcadm, mgcrw, mgcsprov, mgcmtce,and mgcro.

If you have passthru user privileges, refer to Transferring files as a passthru user using FTPProxy on page 141 in this document.

Action

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

Summary of transferring files as a core user using FTPProxy



Transferring files as a core user using FTPProxy

At the OSS/Client workstation

1 Log in to the SDM.

a Open an FTP session by typing

```
> ftp <IP address>
```

and pressing the Enter key.

where

<IP address>
is the IP address of the SDM.

b At the prompt, enter your userID.

c At the prompt, enter you password.

The FTPProxy application authenticates your userID and password and logs you in to the SDM.

2 At the ftp> prompt, log in to the Core by typing

```
ftp>   site cm
```

and pressing the Enter key.

The command logs you in to the Core.

3 Use the commands in the table to transfer files.

If you want to	At the ftp> prompt, type the following command and press the enter key
transfer files in ASCII mode	ascii
transfer files in Binary mode	bin
get a file from the Core	get < filename on Core >
put a file to the Core from the OSS/client machine	put <filename on client machine >
list files on the Core - type	ls
- or type	dir
view the current directory on the core	pwd
log out of the ftp session	bye

4 You have completed this procedure.

Starting an SFT session

Purpose

The following procedure describes how to start an SFT session in secure access.

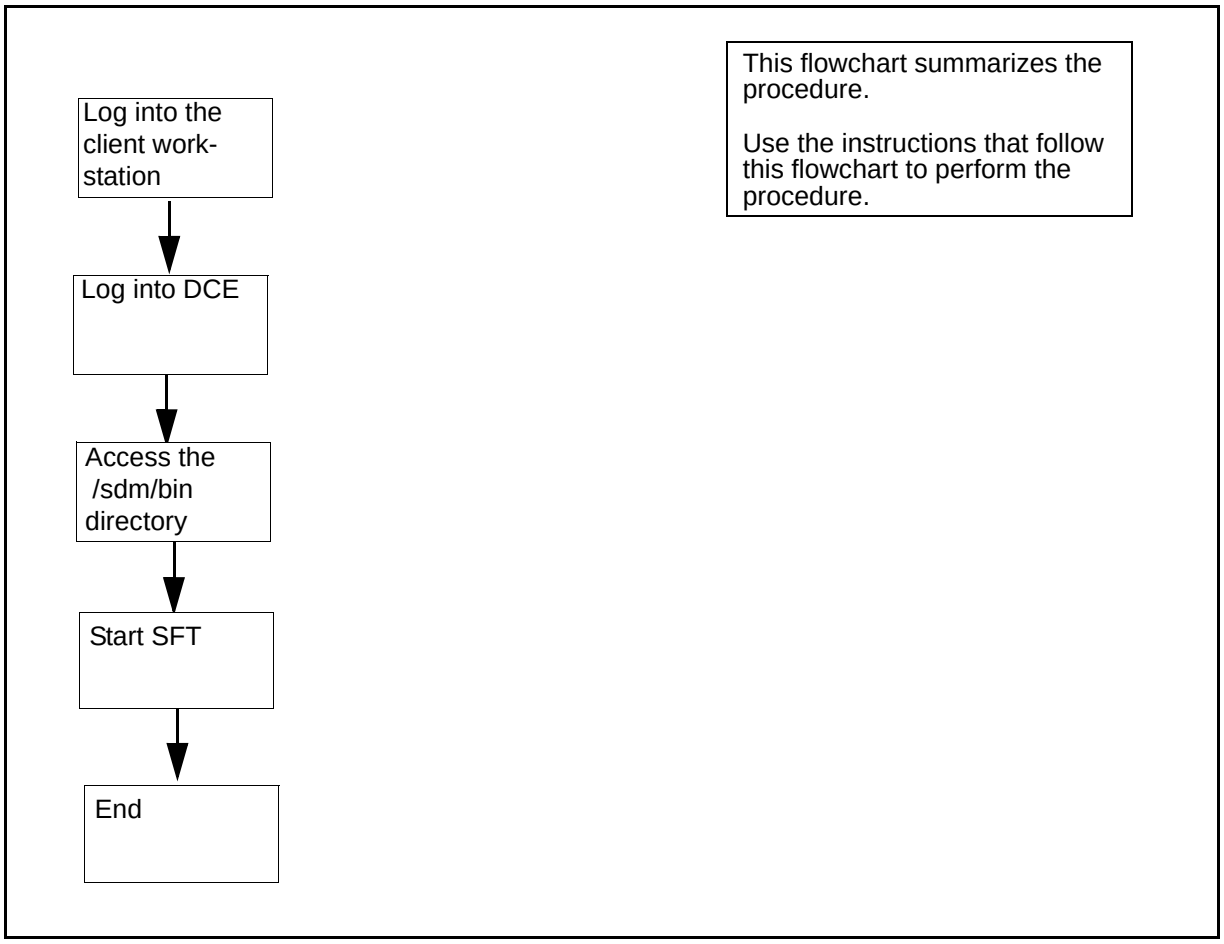
Application

Information is provided to enable the SFT client to access either the SDM, or the computing module (CM) for the purpose of doing file transfers. You must have a DCE account, and password to use SFT. If you do not have a DCE account, your DCE administrator can create one for you.

Note 1: If you are using anonymous or normal FTP access, refer to the procedure, Starting an FTP client on page 139 in this document.

Note 2: Ensure you have correctly defined the DCE principal names.

Summary of starting an SFT session



Procedure

Starting an SFT session

At the client workstation:

1 Log into the SFT client workstation.

2 Log into DCE:

> dce_login

Example response:

```
Enter Principal Name:
```

3 Enter your DCE user ID.

Example response:

```
Enter Password:
```

4 Enter your DCE password.

5 Change to the bin directory:

> cd /sdm/bin

6 Determine the CM CLLI.

If you	Do
know the value for the CM CLLI	step 7
do not know the value for the CM CLLI	step 8

7 Proceed as follows:

a Start the SFT application:

> ./sft <CLLI>

where

<CLLI>
is the CM CLLI, for example FCC11

Example response:

```
220 FCC11 SFTPD Server (Version 9.0.21.0 Jan
27 1998) ready.
```

b Go to step 9.

8 List the CM CLLIs and start SFT:

a List the CM CLLIs for all SDM nodes in the same DCE cell as your SFT client workstation:

> ./sft clist

Example response:

```
FCC11 ottwaonye6a
```

b Start the SFT application:

sft> open <CLLI>

where

<CLLI>
is the CM CLLI, for example FCC11

Example response:

```
220 FCC11 SFTPD Server (Version 9.0.21.0 Jan
27 1998) ready.
```

9 Perform substep a or b according to whether you want to transfer files to or from the CM, or to or from the SDM.

a Transfer files to or from the CM:

sft> site cm

b Transfer files to or from the SDM:

sft> site sdm

Note: You can repeat these substeps as required. You can toggle between the CM and SDM at any time.

10 You have completed this procedure.

Transferring and retrieving files using SFT

Purpose

Use this procedure to transfer and retrieve files using SFT.

Application

The following sections describe the procedures to transfer and retrieve files using SFT:

- Transferring a file to an SDM directory on page 151
- Retrieving a file from an SDM directory on page 154
- Transferring a CM file to a DMS volume on page 155
- Retrieving a CM file from a DMS volume on page 159
- Retrieving an active DIRP file on page 161
- Discontinuing a file transfer on page 163

The following procedures are referenced in this procedure:

- Starting an SFT session on page 147
- Starting an FTP client on page 139

Transferring a file to an SDM directory

Use this procedure to transfer a file from the client workstation to an SDM directory. The file can be in either binary or ASCII format. You must know the format of the file to complete this procedure.

To transfer a file from the client workstation to a SDM directory, the system uses the file extension and sets the correct transfer type. The system recognizes the following file extensions:

- .patch
- .xref

- .bin(<n>)

  where

  <n>
  is the logical record length to transfer a file to the DMS for a binary file type.

- .txt(<n>)

  where

  <n>
  is the logical record length to transfer a file to the DMS for an ASCII file type.

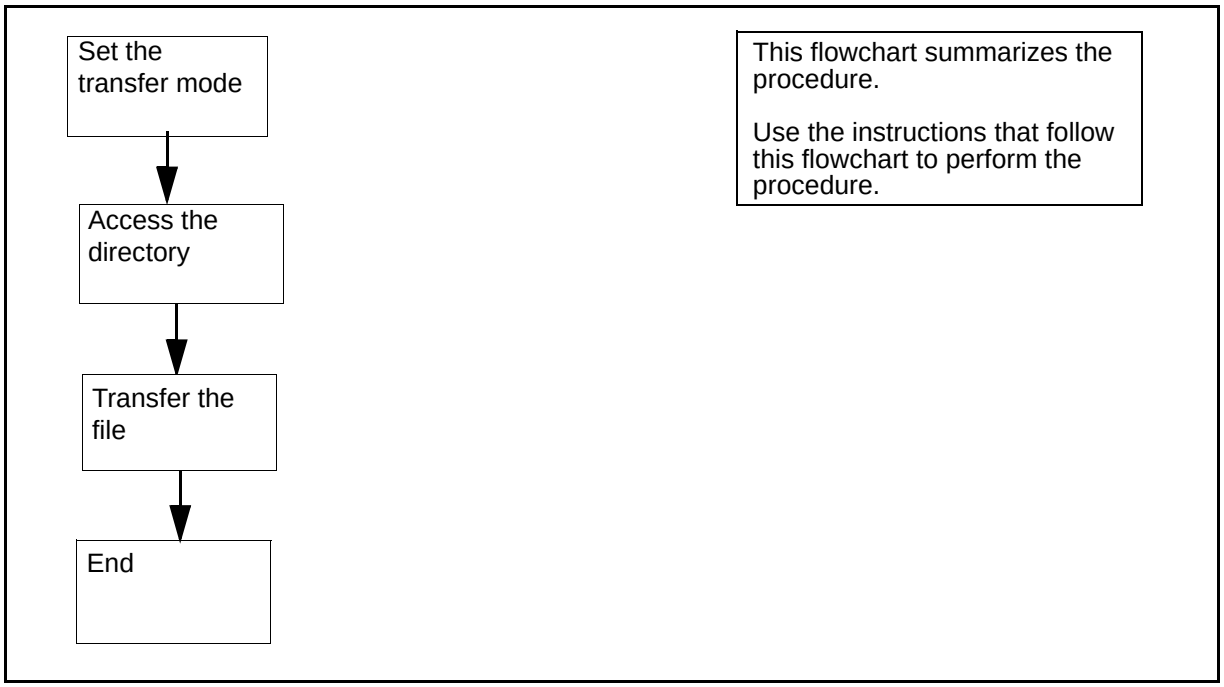
Note: If you are transferring files to or from the DMS Communication, the system recognizes the same file extensions as above, and sets the correct logical record length.

If the system does not know the transfer type, the transfer type is not changed and remains as the last specified transfer type. In this instance, the warning message Unrecognized File Type. Using Current Transfer Type. is displayed as the first sentence of the response.

This procedure assumes you have already started an SFT session in DCE mode including a “site sdm” command. If you have not done so, refer to procedures Starting an SFT session on page 147 or Starting an FTP client on page 139 in this document. This procedure also assumes that you have set your current local working directory to be the directory containing the file.

To transfer and retrieve files using SFT, perform the procedure that follows the flowchart.

Summary of transferring a file to an SDM directory



Transferring a file to an SDM

At the SFT prompt:

1 Set the transfer mode:

sft> <transfer_mode>

where

<transfer_mode>
is either binary or ASCII

2 Change to the SDM directory:

sft> cd <directory_name>

where

<directory_name>
is the name of the SDM directory

3 Transfer the file to the SDM directory:

sft> put <*file_name*>

where

<file_name>
is the name of the file.

4 You have completed this part of the procedure.

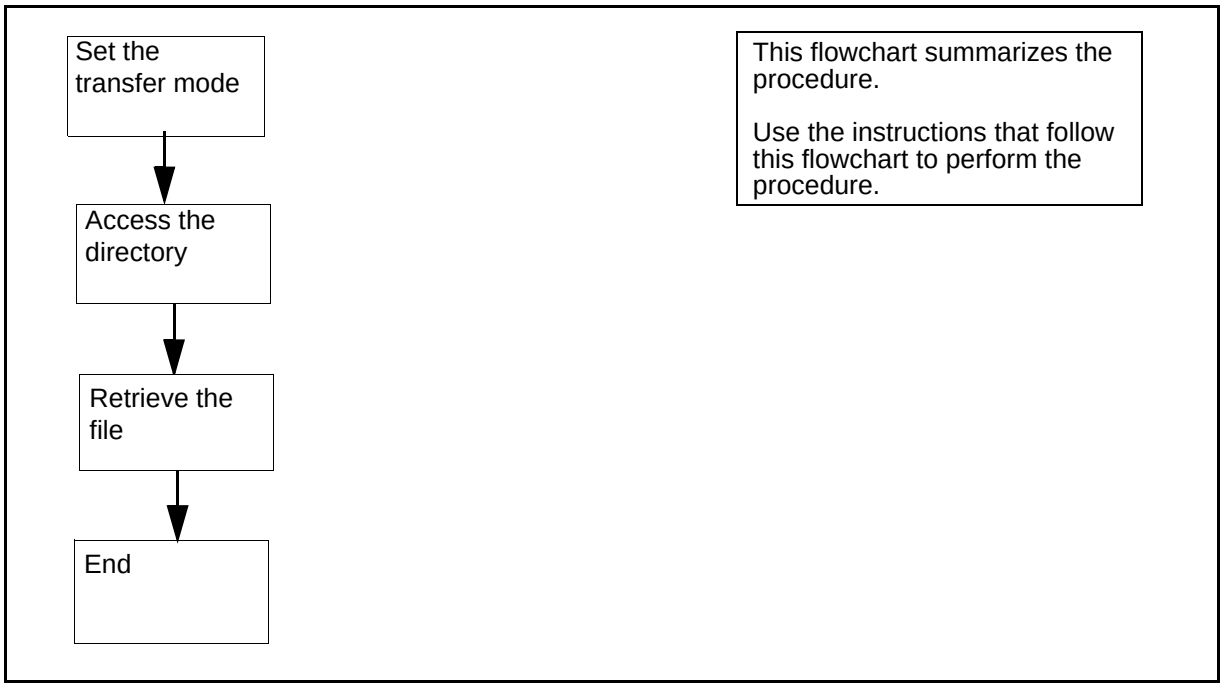
Retrieving a file from an SDM directory

Use this procedure to retrieve a file from an SDM directory to the client workstation. The file can be in either binary or ASCII format. You must know the format of the file to complete this procedure.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures, Starting an SFT session on page 147, or Starting an FTP client on page 139 in the Security and Administration section. This procedure also assumes that you have set your current local working directory to be the directory that is to receive the file.

To retrieve a file from the SDM directory, perform the step-action procedure that follows the flowchart.

Summary of retrieving a file from an SDM directory



Retrieving a file from an SDM directory

At an SFT prompt:

1 Set the transfer mode:

sft> <transfer_mode>

where

<transfer_mode>
is either binary or ASCII

2 Access the SDM directory:

sft> cd <directory_name>

where:

<directory_name>
is the name of the SDM directory

3 Retrieve the file from the SDM directory:

sft> get <file_name>

where:

<file_name>
is the name of the file.

4 You have completed this part of the procedure.

Transferring a CM file to a DMS volume

Use this procedure to transfer a CM file from the client workstation to a volume group on the DMS switch. The file can be in either binary or ascii format. You must know the format of the file to complete this procedure.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures Starting an SFT session on page 147 or Starting an FTP client on page 139. This procedure also assumes that you have set your local working directory to be the directory that is to receive the file.

Record lengths and formats for CM files

To transfer a CM file to a DMS volume, you must know the record length of the file. Use this information in the CM File Formats table below.

Table CM File Formats provides a sample of formats for selected CM files for reference purposes. It is not a complete list. Formats can vary.

CM File Formats (Sheet 1 of 2)

File	Fixed or variable length record	Transfer mode	Record length
Image files	Fixed	binary	1020
Patches	Fixed	binary	128

CM File Formats (Sheet 2 of 2)

File	Fixed or variable length record	Transfer mode	Record length
SMDR	Fixed	binary	2048
EDRAM	Fixed	binary	44
SOC	Variable	ASCII	
Translations	Variable	ASCII	

Record lengths and formats for peripheral module (PM) files

You must know the record length of the file to transfer a PM file to a DMS volume.

You can determine the record length for a peripheral module (PM) file by its file extension.

The following example shows a typical LCM file format.

LCM file: lcm ##**aa.**bin **nn**

where

is the XPM stream number of the load

aa is the version of the load

nn is the file extension number

The table PM file extensions describes typical PM file extensions.

PM file extensions (Sheet 1 of 2)

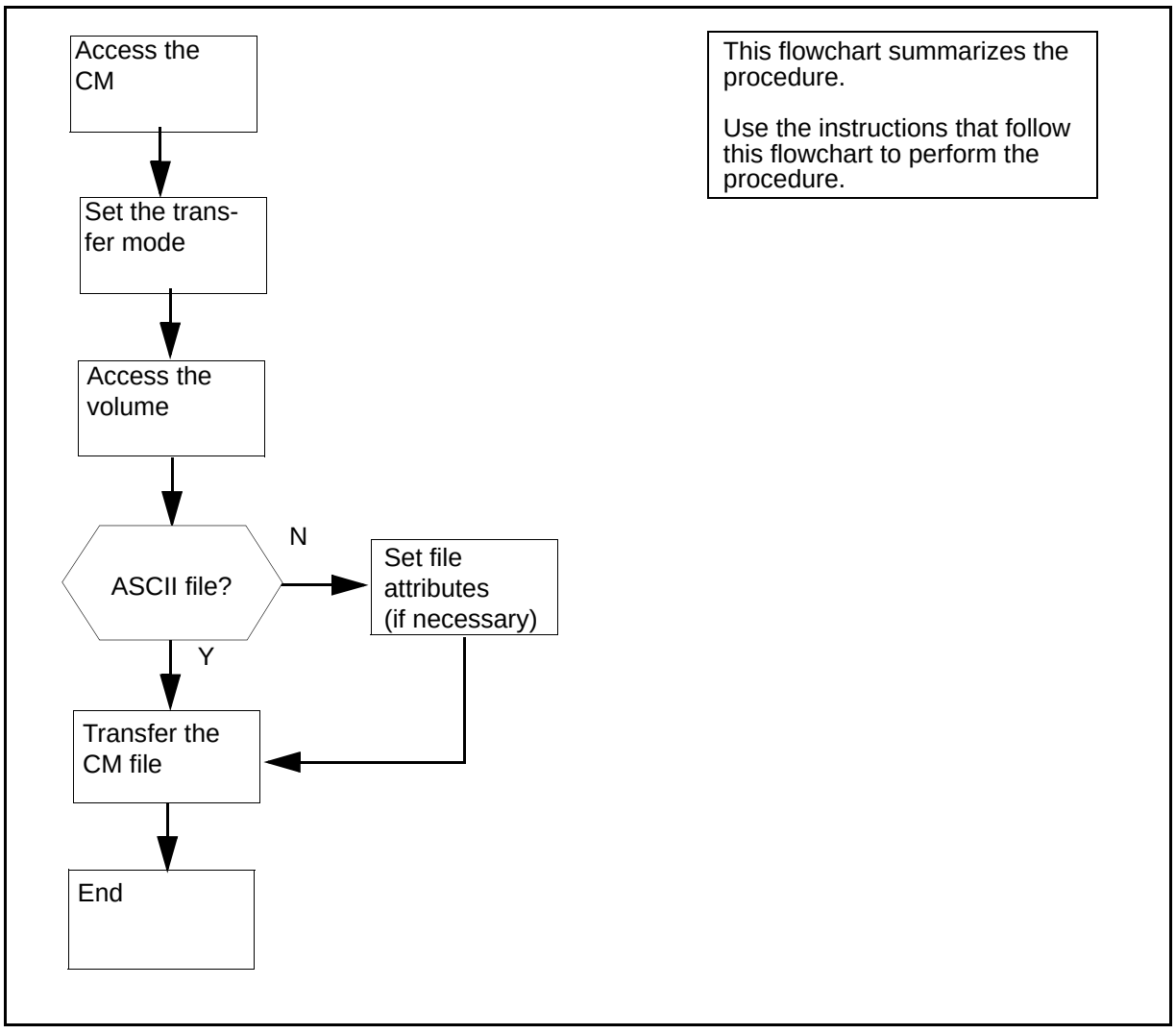
File extension	Type of image	Fixed- or variable-length record	Transfer mode	Record length
.bin1024	non-system	fixed-length	binary	1024
.txt55	non-system	variable-length	ASCII	55

PM file extensions (Sheet 2 of 2)

File extension	Type of image	Fixed- or variable-length record	Transfer mode	Record length
.bin1020	system	fixed-length	binary	1020

To transfer a CM file to a DMS volume, perform the procedure that follows the flowchart.

Summary of transferring a CM file to a DMS volume



Transferring a CM file to a DMS volume

At an SFT prompt:

1 Go to the DMS volume:

sft> cd /<volume_name>

where

<volume_name>
is the name of the DMS volume.

Note: Specify DMS volume names in uppercase characters.

2 Set the transfer mode:

sft> <transfer_mode>

where

transfer_mode
is either binary or ASCII.

3 Use the following table to determine your next step.

If you want to transfer	Do
an ASCII file	step 5
a binary file	step 4

4 Enter the file characteristics or attributes, if necessary.

You must enter the file characteristics if:

- the suffix of the transfer file does not match the pattern ".bin###" (where ### indicates the record length a value between 1 and 32767), or
- the file is a patch file

If you do not need to enter the file characteristics or attributes, proceed to step 5.

Set the record length of the file:

sft> site lrecl <Record_length>

where

<Record_length>
is the record length of the file

Note: See table CM File Formats for a format list of various CM file types.

5 Transfer the CM to the DMS volume:

sft> put <file_name>

where

<file_name>
is the name of the CM file

6 You have completed this procedure.

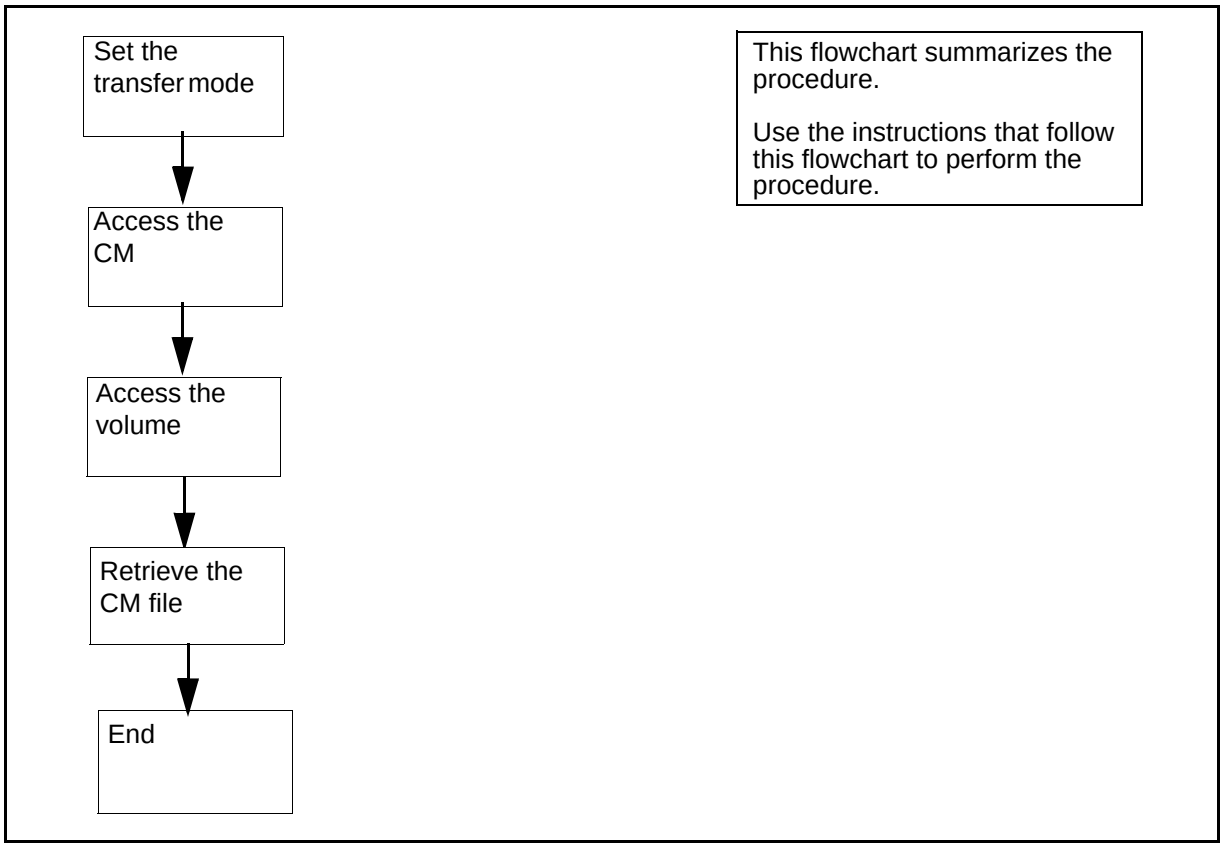
Retrieving a CM file from a DMS volume

Use this procedure to retrieve a CM file from a DMS volume and transfer it to the client workstation. The file can be in either binary or ASCII format. You must know the format of the file to complete this procedure.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures, Starting an SFT session on page 147 or Starting an FTP client on page 139. This procedure also assumes that you have set your current local working directory to be the directory that is to receive the file.

To complete the procedure for retrieving a CM file from a DMS volume, perform the procedure that follows the flowchart.

Summary of retrieving a CM file from a DMS volume



Retrieving a CM file from a DMS volume

At an SFT prompt:

1 Set the transfer mode:

sft> <transfer_mode>

where

<transfer_mode>
is either binary or ASCII

2 Change to the DMS volume:

sft> cd /<volume_name>

where

<volume_name>
is the name of the DMS volume

Note: Specify DMS volume names in uppercase characters.

3 Retrieve the CM file from the DMS volume:

sft> get <file_name>

where

<file_name>
is the name of the CM file.

4 You have completed this procedure.

Retrieving an active DIRP file

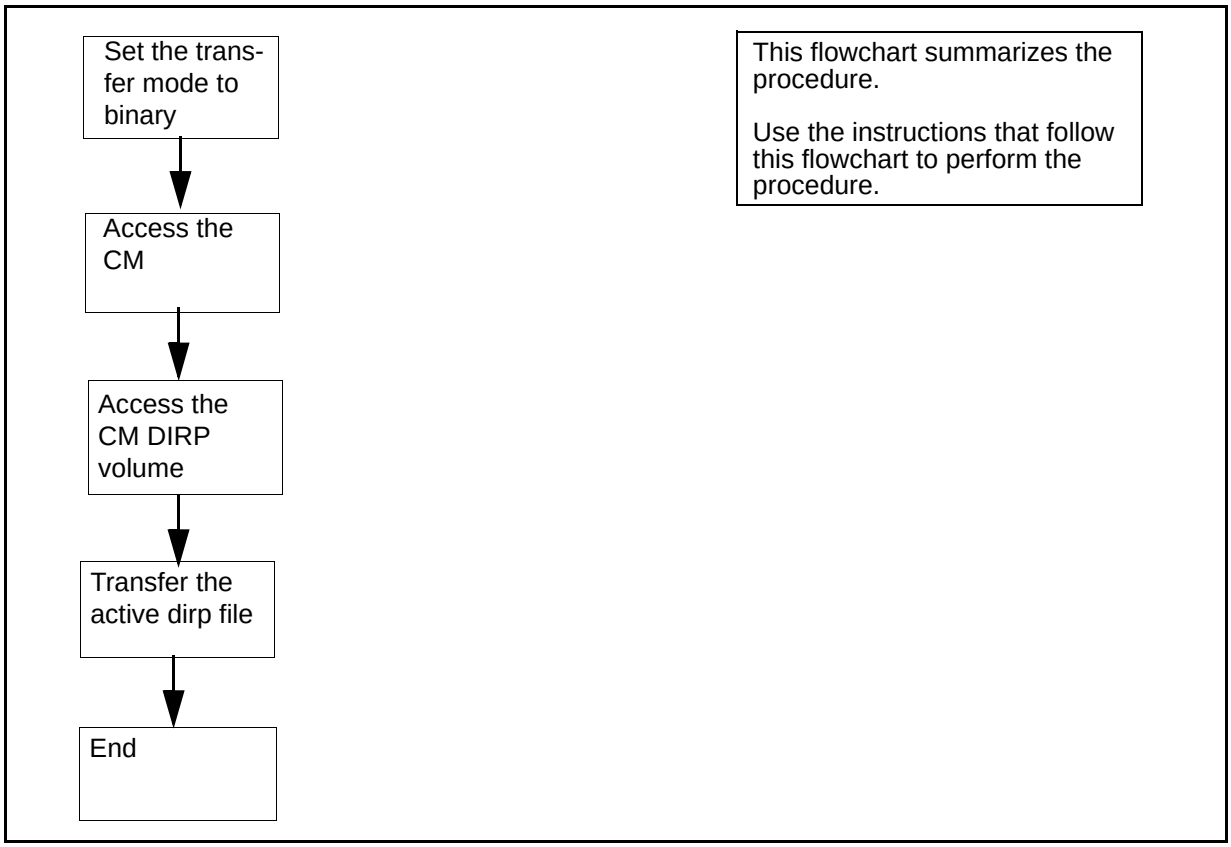
The Device Independent Recording Package (DIRP) is CM software that automatically directs data from the various administrative and maintenance facilities on the DMS switch to the appropriate recording devices.

Use the following procedure to retrieve an active DIRP file.

This procedure assumes you have already started an SFT session in DCE mode, including a site cm command. If you have not done so, refer to the procedures, Starting an SFT session on page 147 or Starting an FTP client on page 139. This procedure also assumes that you have set your current local working directory to be the directory that is to receive the file.

To complete the procedure for retrieving an active DIRP file, perform the procedure that follows the flowchart.

Summary of retrieving an active DIRP file



Retrieving an active DIRP file

At an SFT prompt

1 Set the transfer mode to binary:

sft> binary

2 Access the CM:

sft> site cm

3 Set the file characteristics for a DIRP file:

sft> site getdirp <DIRP_subsystem_number>

where

<DIRP_subsystem_number>
is the DIRP subsystem number

Note: For automatic message accounting (AMA), the DIRP subsystem number is 0.

4 Go to the DMS volume group:

sft> cd /<DIRP_volume>

where

<DIRP_volume>
is the name of the DIRP volume

Note: Specify DMS volume names in uppercase characters.

5 Retrieve the DIRP file:

sft> get <active_dirp_file_name>

where

<active_dirp_file_name>
is the name of the active DIRP file

6 You have completed this procedure.

Discontinuing a file transfer

Discontinue file transfers by entering the interrupt key sequence (<CTRL> C). Set the interrupt key sequence by using the STTY command. When you enter the interrupt key sequence, SFT terminates and closes all open sessions.

Changing the system time zone and daylight savings time parameters

Purpose

Use this procedure to change the time zone and daylight savings time parameters on the SDM.

Application

It is recommended that you perform this procedure at the same time you are performing an upgrade while the SDM is in split mode, or out of service (non-split mode). If you choose to do so, follow the steps under Changing the system time zone and daylight savings time parameters on page 167 in this procedure.

If you decide to perform this procedure independently of an upgrade, it is recommended that you use the split-mode process as opposed to the non-split mode process, which takes the SDM out of service for approximately 20 minutes.

- To use the split mode process, first follow the steps under Splitting the system on page 165 and then follow the steps under Changing the system time zone and daylight savings time parameters on page 167 in this procedure.
- To use the non-split mode process, first follow the steps under Busying the SDM on page 167 and then follow the steps under Changing the system time zone and daylight savings time parameters on page 167 in this procedure.

Splitting the system

At the VT100 console connected to SP0

1 Log on to the SDM as the root user.

2 Access the split-mode screen:

 # sdmmtc split

3 Begin the split-mode process:

> start

4 When prompted, confirm that you want to perform an upgrade:

> y

The system performs some checks.

5 Determine if errors were found.

If the system	Do
detects errors	go to the appropriate procedure to correct the errors, and perform this procedure again
does not detect errors	step 6

6 When prompted, select the first option on the list, Software upgrade:

> 1

7 When prompted, confirm that you want to proceed:

> y

8 Wait until the system split is 100% complete (minimum of 20 minutes), as indicated by the following message on the SP0 console.

20 min.+

```
Split: [100%] Completed
Configure: [User] Waiting for user input
```

Note: You do not have a connection available to the inactive console until the system is 100% split. Once the system is split, each VT100 console display reports, in the upper-right corner, the domain that it is connected to. For example, SP0 reports

```
Active Domain 0
```

At the VT100 console SP1 (inactive)

9 Wait until the FX-Bug prompt appears on the SP1 (inactive) console before you proceed to the next step.

10 At the FX-Bug prompt, manually reboot domain 1:

FX-Bug> pboot 6 0

11 Log into the inactive side (SP1) of the SDM as the root user.

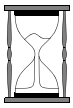
The system automatically displays the split-mode screen.

12

CAUTION

Possible loss of service

If the SDM begins the system stabilization process, do not attempt to perform any activities on the system until stabilization is complete.



7 min.

Wait until system stabilization is complete (approximately 7 minutes) before proceeding to the next step.

Note: When the stabilization process begins, the system displays a time estimate for its completion.

13 Proceed to Changing the system time zone and daylight savings time parameters in this procedure.

Busying the SDM

At the MAP display

1 Access the SDM level of the MAP display:

> mapci;mtc;appl;sdm

2 Check that the SDM is in a fault-free state.

- If the SDM is not in a fault-free state, correct all faults and alarms before continuing this procedure. Refer to the SDM Fault Management document for alarm-clearing procedures.
- If you have alarms or faults that you cannot clear, stop and contact your next level of support.

3 Busy the SDM:

> bsy

4 Confirm the busy request:

> y

5 Proceed to Changing the system time zone and daylight savings time parameters on page 167 in this procedure.

Changing the system time zone and daylight savings time parameters

At the local VT100 console

1 Log in as root user.

2 Enter the Time Zone level:

 # sdmmtc tz

Example response:

```
  SDM     CON    512    NET    APPL    SYS     HW    CLLI: SNM0
  ManB     .     . .     .     ManB     .      .     Host: wcary2p3
                 . .                                      Fault Tolerant

TimeZone
 0  Quit
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17 Help
 18 Refresh
  root
 Time 18:51  >

Time Zone: Eastern U.S.; Colombia
   EST5EDT (CUT -5)
   Daylight Start: M4.1.0/02:00:00 (Standard)
   End: M10.5.0/02:00:00
   Thu Sep 5, 2002 18:51
```

3 Change the time zone:

> c

Example response:

```
Time Zone: Daylight Savings?
Does this time zone go on Daylight Savings Time?
Please confirm (“YES”, “Y”, “NO”, or “N”):
```

4 Determine if Daylight Savings Time is to be used.

If the time zone	Do
goes into Daylight Savings Time	enter **y**
does not go into Daylight Savings Time	enter **n**

Example response: Screen 1

```
  SDM      CON    512    NET    APPL    SYS      HW    CLLI: SNM0
  ManB      .     . .     .     ManB     .       .     Host: wcary2p3
                  . .                                      Fault Tolerant

TimeZone
 0  Quit
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17 Help
 18 Refresh

Time Zone: Closest Match
Choose the Time Zone which is the closest match to yours:

1. Bering Straits              (BST11BDT)          (CUT -11)
2. Hawaii;Aleutian Islands     (HST10HDT)          (CUT -10)
3. Alaska                      (AST9ADT)           (CUT -9)
4. Pacific U.S.;Yukon          (PST8PDT)           (CUT -8)
5. Mountain U.S.               (MST7MDT)           (CUT -7)
6. Central U.S.;Honduras       (CST6CDT)           (CUT -6)
7. Eastern U.S.;Colombia       (EST5EDT)           (CUT -5)
8. Central Brazil              (AST4ADT)           (CUT -4)
9. Greenland;East Brazil       (GRNLNDST3GRNLNDDT) (CUT -3)
10 Falkland Islands            (FALKST2FALKDT)     (CUT -2)
11.Azores;Cape Verde           (AZOREST1AZOREDT)   (CUT -1)
12 Coordinated Universal Time  (CUT0GDT)           (CUT)
13.United Kingdom              (GMT0BST)           (CUT)
14.Norway, France              (NFT-1DFT)          (CUT +1)
15.South Africa                (USAST-2USADT)      (CUT +2)
16.Finland                     (WET-2WET)          (CUT +2)
  root
 Time 18:54   >MORE...(52%)
```

5 Press the Space Bar to display the next screen:

Example response: Screen 2

```
  SDM      CON    512     NET    APPL    SYS      HW     CLLI: SNM0
  ManB      .     . .      .     ManB     .       .      Host: wcary2p3
                  . .                                        Fault Tolerant

TimeZone
 0  Quit
 2              17. Turkey                      (MEST-3MEDT)       (CUT +3)
 3              18. Saudi Arabia                (SAUST-3SAUDT)     (CUT +3)
 4              19. Gorki;Central Asia;Oman     (WST-4WDT)         (CUT +4)
 5              20. Pakistan                    (PAKST-5PAKDT)     (CUT +5)
 6              21. Tashkent;Central Asia       (TASHST-6TASHDT)   (CUT +6)
 7              22. Thailand                    (THAIST-7THAIDT)   (CUT +7)
 8              23. People's Republic of China  (BEIST-8BEIDT)     (CUT +8)
 9              24. Taiwan                      (TAIST-8TAIDT)     (CUT +8)
 10             25. Western Australia           (WAUST-8WAUDT)     (CUT +8)
 11             26  Japan                       (JST-9JSTDT)       (CUT +9)
 12             27. Korea                       (KORST-9KORDT)     (CUT +9)
 13             28  Eastern Australia           (EET-10EEDT)       (CUT +10)
 14             29. Solomon Islands             (MET-11METDT)      (CUT +11)
 15             30. New Zealand                 (NZST-12NZDT)      (CUT +12)
 16
 17 Help        Enter a number from 1 to 30 to choose the time zone that
 18 Refresh     most closely matches yours. You will have the opportunity
                to customize the time zone if necessary: [7]
  root
 Time 18:54  >
```

6 Select a time zone:

> <n>

where:
<n> is the number of the time zone closest to the one in which you are geographically located.

Example:

The closest time zone to Newfoundland is *Greenland; East Brazil,* or number 9 in the list of time zones.To select the time zone for Newfoundland, enter:

> 9

Example response:

```
Time Zone: Edit this zone?
Selected Zone: Greenland;East Brazil
     GRNLNDST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 18:57


The above shows the values for the time zone that you
have selected. Proceed to set the time zone using the
current values, or edit them and make changes.

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

7 When prompted, confirm, reject, or edit the values.

If you entered	Do
y to confirm the values	you have completed this procedure
n to reject the values	return to step 3
e to edit the values	step 8

8 The system displays the current value of the time zone description, and prompts you enter another value.

Example response:

```
Time Zone: Description
Selected Zone: Greenland;East Brazil
     GRNLNDST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:01


The time zone description should include a few words
such as the name of your city which describes the area
where the time zone is in use.

Enter the description: [Greenland;East Brazil]
>
```

9 Enter the new description for your time zone.

Example:

To enter the value for Newfoundland, enter:

> Newfoundland

Example response:

```
Time Zone: Acronym
Selected Zone: Newfoundland
     GRNLNDST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:15


Enter the acronym associated with this time zone. For
example, the time zone acronym for New York is EST,
which is short for Eastern Standard time

Enter the acronym: [GRNLNDST]
>
```

10 Enter an acronym for your time zone.

Example:

To enter an acronym for Newfoundland Standard Time, enter:

> NST

Example response:

```
Time Zone: Offset from CUT
Selected Zone: Newfoundland
     NST3GRNLNDDT (CUT -3)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:19

The offset from CUT (Coordinated Universal Time) is
the number of hours BEFORE CUT for this time zone. For
example, EST in North America is 5 hours before CUT,
while NFT for France and Norway is -1 hours before
CUT. Specify the time in the form HH[:MM[:SS]] where
HH ranges from -12 to 11. Minutes and seconds are
optional.

Enter the offset from CUT: [3]

>
```

11 Enter the time zone offset from CUT (Coordinated Universal Time).

Example:

To set the time zone offset from CUT for Newfoundland, enter:

> 3:30

If the time zone	Do
goes into Daylight Savings Time (you entered **y** in step 4)	step 12
does not go into Daylight Savings Time (you entered **n** in step 4)	step 19

12 The system displays the following response.

Example response:

```
Time Zone: Daylight Savings Acronym
Selected Zone: Newfoundland
     NST3:30GRNLNDDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:21


The daylight savings time acronym is the name
associated with daylight savings for this time zone.
For example, for EST (Eastern Standard Time), the
associated daylight savings acronym is EDT (Eastern
Daylight Time).

Enter the daylight savings acronym: [GRNLNDDT]
>
```

13 Enter the daylight savings acronym for the time zone.

Example:

To set the daylight savings acronym for Newfoundland Daylight Time, enter:

> NDT

Example response:

```
Time Zone: Daylight Savings offset from CUT
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:24


The daylight savings offset from CUT (Coordinated
Universal Time) is the number of hours BEFORE CUT for
daylight savings in this time zone. For example, EDT
in North America is 4 hours before CUT, while DFT for
France and Norway is -2 hours before CUT. The daylight
savings offset is normally 1 hour less that (ahead of)
the standard offset. Specify the time in the form
HH[:MM[:SS]] where HH ranges from -12 to 11. Minutes
and seconds are optional.


Enter the daylight savings offset from CUT: [2]
>
```

14 Enter the daylight savings offset from CUT for the time zone.

Example:

To set the daylight savings offset from CUT for Newfoundland, enter:

> 2:30

Example response:

```
Time Zone: Daylight Savings Start Day
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:27


The daylight savings start day indicates the day of the
year when daylight savings takes effect. The day can
be specified one of two forms: M<month>.<week>.<day>
or J<julianday> where:
  <month> is the month, a number from 1 to 12
  <week> is the week during that month, an number from
         1 to 5,
  <day> is the day of that week, a number from 0 to 6,
         0 indicating Sunday,
  <julianday> is the day of the year, a number from
         1 to 365, leap days are not counted.

Enter the daylight savings start day: [M4.1.0]
>
```

15 Enter the starting day for daylight savings for your time zone.

Example:

Newfoundland changes on the first Sunday of April, which is the current value in the example. To accept a current value, press the Enter key.

Example response:

```
Time Zone: Daylight Savings Start Time
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:30

The daylight savings start time indicates the time on
the daylight saving start day when daylight savings
takes effect. The time is specified in the format
HH[:MM[:SS]] where HH ranges from 00 to 23. Minutes
and seconds are optional.

Enter the daylight savings start time: [02:00:00]
>
```

16 Enter the daylight savings start time for your time zone.

Example:

Newfoundland changes as 02:00:00, which is the value already specified in the example. To accept the current value, press the Enter key.

Example response:

```
Time Zone: Daylight Savings End Day
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:33


The daylight savings end day indicates the day of the
year when daylight savings ends. The day can be
specified in one of two forms:
 M<month>.<week>.<day> or J<julianday> where:
  <month> is the month, a number from 1 to 12,
  <week> is the week during that month, a number
         from 1 to 5
  <day> is the day of that week, a number
         from 0 to 6, 0 indicating Sunday
  <julianday> is the day of the year, a number
         from 1 to 365, leap days are not counted.


Enter the daylight savings end day: [M10.5.0]
>
```

17 Enter the daylight savings end day for your time zone.

Example:

Newfoundland changes on the last Sunday in October, which is the current value in the example. To accept the current value, press the Enter key.

Example response:

```
Time Zone: Daylight Savings End Time
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:36

The daylight savings end time indicates the time on
the daylight saving end when daylight savings ends.
The time is specified in the format HH:[MM[:SS]]
where HH ranges from 00 to 23. Minutes and seconds
are optional.

Enter the daylight savings end time: [02:00:00]
>
```

18 Enter the daylight savings end time for your time zone.

Example:

Newfoundland changes at 02:00:00, which is the default in the example. To accept the current value, press the Enter key.

Example response:

```
Time Zone: Edit this zone?
Selected Zone: Newfoundland
     NST3:30NDT2 (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
     End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:39

The above shows the values for the time zone that you
have selected. Proceed to set the time zone using the
current values, or edit them and make changes.

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

If you want to	Do
confirm the values	enter **y**, and go to step 19
reject the values	enter **n**, and go to step 3
edit the values	enter **e**, and return to step 8

19 The system displays the values for both the current and the commissioned time zones. and a prompt for a system reboot.

Example response:

```
Current Zone: Eastern U.S.: Colombia
     EST5EDT (CUT -5)
     Daylight Start: M4.1.0/02:00:00 (Standard)
              End: M10.5.0/02:00:00
     Thu Sep 5, 2002 19:42

Commissioned Zone: Newfoundland
     NSTE:30NDT (CUT -3:30)
     Daylight Start: M4.1.0/02:00:00 (Standard)
              End:   M10.5.0/02:00:00
     Thu Sep 5, 2002 19:42

Time Zone: Reboot Required
The commissioned time zone will not take effect until
after the system has been rebooted.

Reboot the system now?
Please confirm: ("YES", "Y", "NO", or "N")

>
```

If you want to	Do
reboot now	enter **y**
reboot later	enter **n**

20 You have completed this procedure.

Using an FTP client

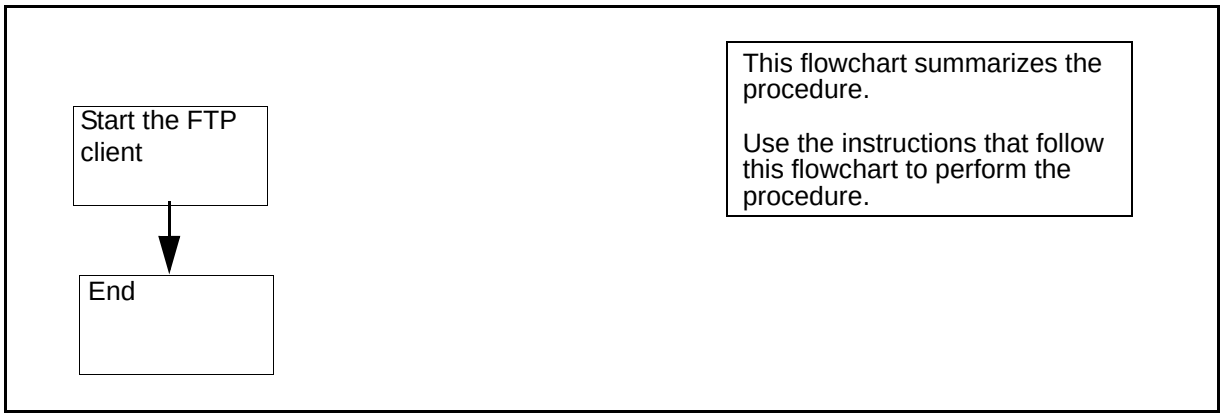
Starting an FTP client

The following procedure describes how to start an FTP client.

Note 1: Nortel Networks recommends that you use the SFT client. FTP userIDs and passwords are passed unencrypted across the network. Standard FTP cannot determine which users are allowed to transfer files to and from the CM.

Note 2: To complete the procedure for starting an FTP client, perform the step-action procedures that follow the flowchart.

Summary of Starting an FTP client



Starting an FTP client

At a UNIX prompt:

1 Start the FTP client workstation by typing

`> ftp <address>`

and pressing the Enter key.

where

address
is the IP address, or the DNS address of the FTP server.

Note: The location of the FTP client varies.

2 You have completed this procedure.

For additional instructions on FTP client usage, refer to the documentation of the client application. For instructions on using CM FTP, refer to section CM FTP server.

CM FTP server

SFT clients and FTP clients can both access the CM FTP server by typing SITE CM.You can use standard FTP commands with some exceptions. A list of exceptions follows.

Command limits and restrictions

The following describes limits to standard FTP commands when accessing the CM FTP server.

- The user command is intercepted and disallowed by the SFT server. A user does not have to log in manually.
- The mkdir and rmdir commands are not supported by the CM FTP server. The CM file system only contains volumes. It does not support directory hierarchies within the volume.
- Files transferred to SFDEV are owned by the user $$SYS$$.
- SFT performs a clean-up routine after the SFT application is returned to service. If you attempt to use the SITE CM command immediately after the RTS command is issued, you may experience a delay of about 20 seconds before access to the CM is given.
- File names and volume names are case sensitive. Volume names are always in uppercase, for example, S01DVOL1. File names are usually in uppercase.

Note: For more information on commands, refer to the commands glossary.

Allowing ATA and ETA to operate across a firewall

Special measures must be taken for DCE-based applications when the SDM is separated by a firewall or other filtering device, or from:

- the DCE cell security and cell directory servers (CDS)
- a workstation that runs an ETA client program

The ETA server on the SDM connect back to the ATA or ETA client, in response to a request to establish a session from the client. It is necessary to control the TCP port that the client uses for the reverse connection.

Restricting ports for incoming connections works in combination with firewalls by implementing a packet-filtering technique. Consult the firewall vendor documentation to determine whether your firewall can be used in this manner.

Restricting the port range

Use the following procedure to restrict the ATA and ETA client reverse connection ports on the client workstation.

Restricting the port range

At the local or remote VT100 console

1 Log into the client workstation as the root user.

2 Change to the ETA directory:

> cd /sdm/bin

3 Start the port range configuration script:

> ./eta_port_range

Example response:

```
 ENHANCED TERMINAL ACCESS PORT RANGE
CONFIGURATION
This configuration script allows you to control
the ETA Client reverse connection ports on the
client workstation.
The current port restriction range for the ETA
Client is:
Range start: -
  Range end:   -
   (no port restriction range)
```

```
Set a new port restriction range by entering 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 At the "Port restriction range:" prompt, enter two numeric values separated by a space:

Port restriction range: <a> <b>

where

<a>
is the beginning the range for ports (must be greater than 1024)

<b>
is the end of the range for ports (must be less than 32 000)

Note 1: These values are not range checked. Check that the values range from 1024 to 32 000. The lowest value must be entered first.

Note 2: The range size is determined by the maximum number of simultaneous instances of the ETA client program that are expected to run on the machine where the client is installed. This number is the number of ETA client instances, not the number of SDM console sessions or DMS MAP terminal sessions, because all sessions started by an ETA client instance share the same port number.

5 Exit the program:

> quit

6 You have completed this procedure.

Changing a DCE user password

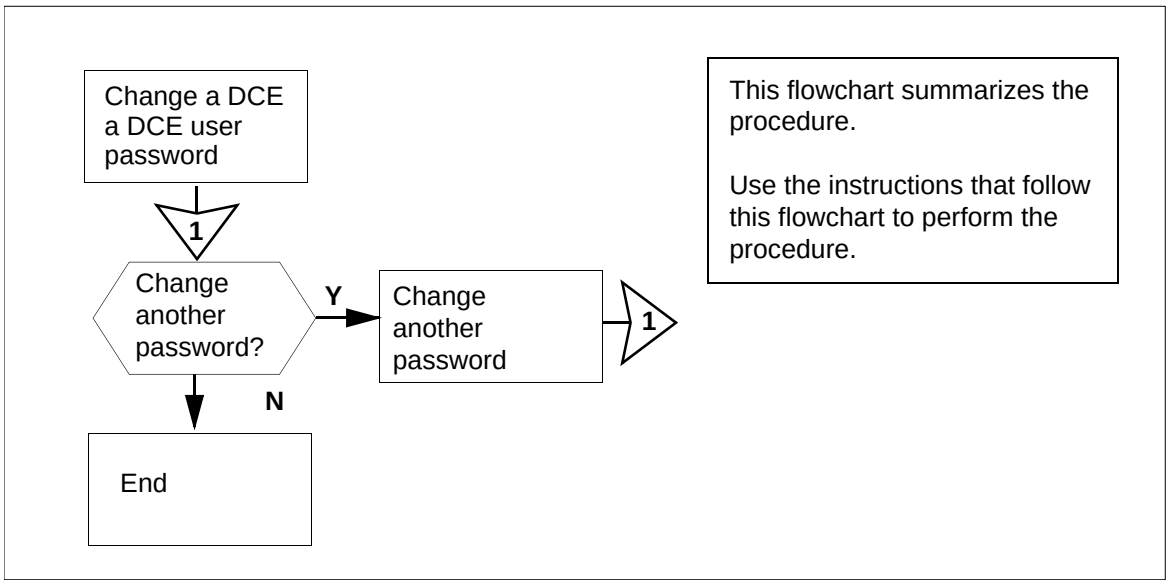
Application

Use this procedure to change a DCE user password.

Action

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

Summary of changing a DCE user password



Changing a DCE user password

At the SDM client workstation

1 Change a DCE user password:

> /sdm/bin/change_dce_password

Example response:

```
DCE user ID:
```

2 Enter the user ID of the user for whom you are changing the password, and press the Enter key.

Example response:

```
Old password:
```

3 Enter the old password.

Example response:

```
New password:
```

4 Enter the new password, and press the Enter key.

Example response:

```
Re-enter password:
```

5 Re-enter the user password, and press the Enter key.

Example response:

```
The password for “ops_1” has been changed.
```

6 You have completed this procedure.

Changing a user password on the SDM

Purpose

Use this procedure to change a user password on the SDM, or to set up a temporary password for a new user.

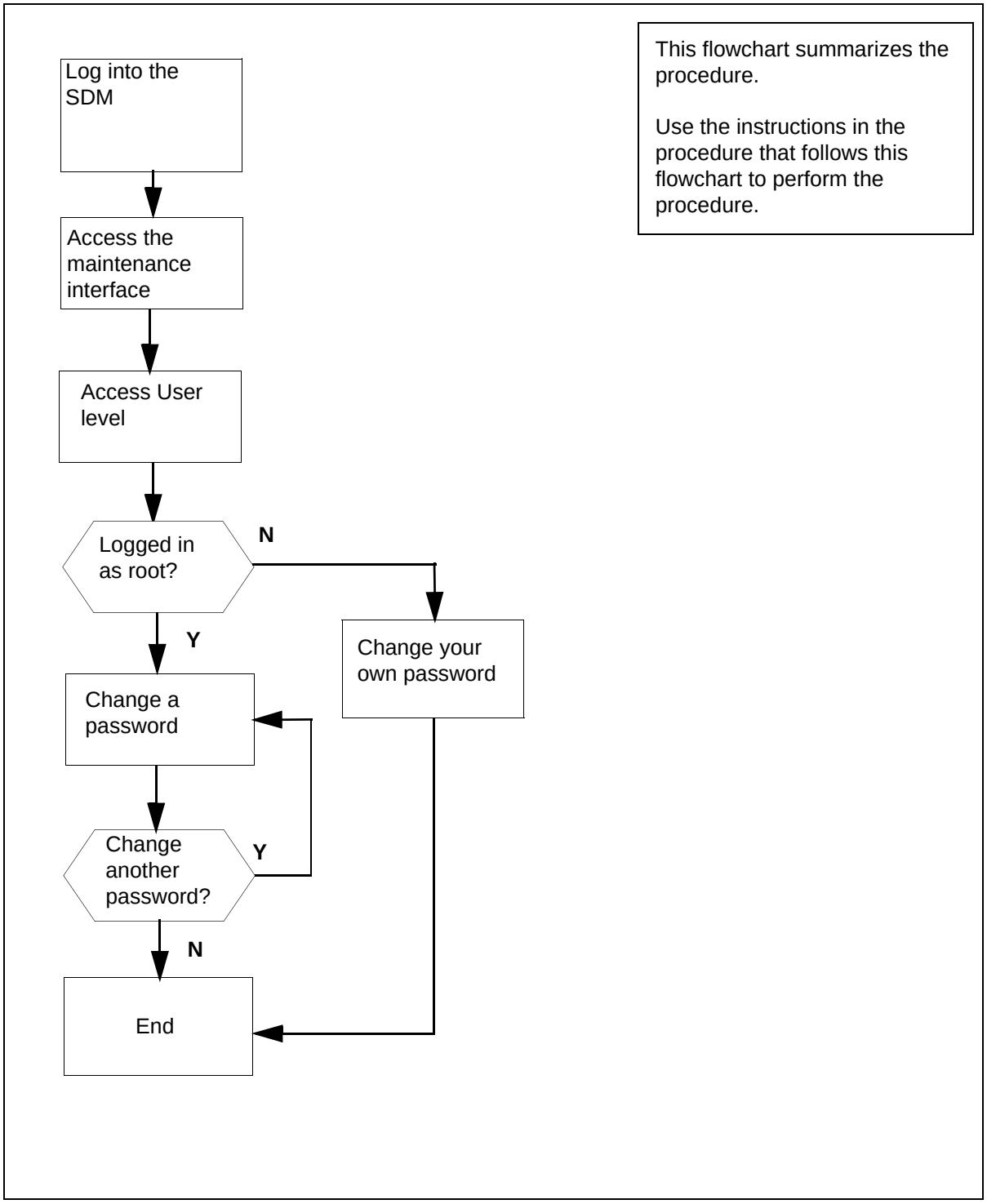
Application

Maintenance class and root users can change their own password. The root user can change the password of any other user class on the system.

Action

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

Summary of Changing a user password



Changing a user password

At the local or remote VT100 terminal

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

2 Access the maintenance interface:

 # sdmmtc

3 Display the User screen:

> user

4 Set the appropriate password.

If you are a	Do
maint class user	step 9
root user	step 5

5 Change a user password:

> change <userID>

where

<userID>
is the userID of the user for whom you are changing the password

Note: If no userID is specified, the system attempts to change the password of the root user.

6 When prompted, enter a new password.

Note: The password must be a minimum of six characters, containing at least one alphabetic character, and at least one numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

7 When prompted, re-enter the password.

Note: If the root user changes a maint class user password, the change is temporary. The maint class user is prompted to change their password again at the next login.

8 Press Enter to continue.

If you	Do
want to change another password	step 5

If you	Do
do not want to change another password	step 14

9 Change your password:

> change

10 When prompted, enter your old (current) password.

11 When prompted, enter a new password.

Note: The password must be a minimum of six characters, containing at least one alphabetic character, and at least one numeric or special character. Although a password can contain more than eight characters, only the first eight characters are processed.

12 When prompted, re-enter the new password.

13 Press Enter to continue.

14 Exit the maintenance interface:

> quit all

15 You have completed this procedure.

Changing a user password on an SSPFS-based server

Application

Use this procedure to change a user password on a Succession Server Platform Foundation Software (SSPFS)-based server.

ATTENTION
User accounts and passwords are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change the password for a specific user by typing

passwd <userid>

and pressing the Enter key.

where

userid
is a variable for the user's login identification

6 When prompted, enter a password of at least three characters.

Note: It is not recommended to set a password with an empty value. Use a minimum of three characters.

7 When prompted, enter the password again for verification.

8 You have completed this procedure.

Changing a passthru user password

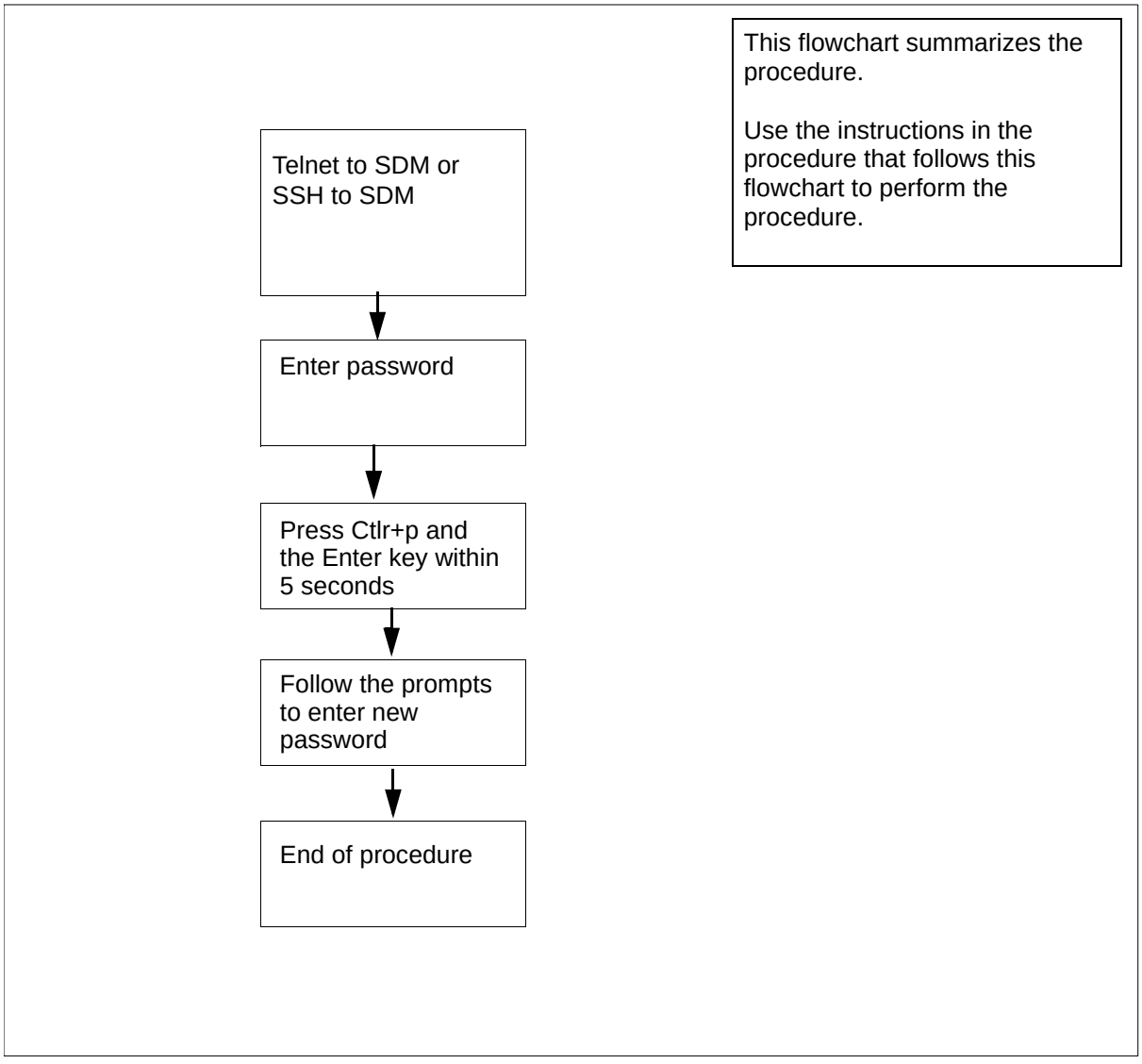
Application

Use this procedure to change a password for a passthru user who is configured as "password required".

Action

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

Summary of changing a passthru user password



Changing a passthru user password

At the workstation

1 Log in to the SDM as a passthru user.

If you	Do
use telnet	step a
use SSH	step b

a Telnet to the CBM by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

<IP address>
is the IP address of the SDM.

Continue with step 2.

b Open an SSH session by typing

```
> ssh-l<passthru userID><IP address>
```

and pressing the Enter key.

where

<IP passthru userID>
is the IP address of the SDM.

2 At the prompt, enter your password.

Note: The following response is only displayed when the pasthru user is configured as "password required". Otherwise, the connection will be directly forwarded to the Core login prompt.

Response:

```
This is a passthru user.

Please type "Ctrl+p" and Enter for changing your password.

type "Enter" or wait for 5 seconds to continue.
```

3 Open the password change session by pressing the Ctrl and p keys at the same time and then pressing the Enter Key.

Note: you must complete this step within 5 seconds or the connection will be forwarded to the Core login prompt.

4 At the prompt, enter the old password and press the Enter key.

5 At the prompt, enter the new password and press the Enter key.

6 At the prompt, re-type the new password and press the Enter key.

7 You have completed this procedure.

Changing CM passwords from ATA client

Changing CM passwords consists of Changing CM passwords in the DCE security database and Changing the CM password on the DMS switch. ASCII Terminal Access (ATA) clients can change their own user passwords.

Note: You can change the CM password on the DMS switch before or immediately after you have changed the CM password in the DCE security database.

Changing CM passwords in the DCE security database

Use the following procedure to change your CM password in the DCE security database.

Changing CM passwords in the DCE security database

At the client workstation

1. Log into the client workstation.
2. Log into DCE:

   > dce_login <DCE_user>

   where

   <DCE_user>
   is the DCE administrator user ID
3. Enter your DCE password, and press the Enter key.
4. Access the bin directory:

   cd /sdm/bin
5. Change the CM password:

   ./ata -passwd

   Example response:

```
This operation will only change your MAP/CI
password in the central database. Make sure you
have the same password for the user ID on the
DMS.

Available MAP/CI User Ids:
   user1 user2 user3 user4
```

Note: You can also change the CM password from the ATA prompt. For example,
ata> passwd

6 When prompted, enter the MAP/CI user ID associated with the password to change.

7 When prompted, enter the old password for the user ID.

8 When prompted, enter the new password for the user ID.

9 When prompted, enter the new password again to confirm.

Example response:

```
Password change successful.

Continue Change Password (y/n):
```

If you	Do
want to change another password	type y, press the Enter key, and repeat steps 6 through 9
do not want to change another password	step 10

10 Exit the password command:

> n

11 You have completed this part of the procedure

Changing the CM password on the DMS switch

Use the following procedure to change your CM password. You must complete this procedure before or immediately after you change your CM password in the DCE security database.

Changing the CM password on the DMS switch

At the ATA prompt:

1 Log in to the DMS switch:

ata> <clli name> cm

2 Change the CM password on the DMS switch:

> password

3 Type your new password, and press the Enter key.

Example response:

```
Please enter new password again to verify.
```

4 Type your new password again, and press the Enter key.

Example response:

```
Enter your current password to verify.
```

5 Type your old (current) password, and press the Enter key.

A message informs you that the password has been successfully changed, and that it must be changed in 30 days.

6 You have completed this procedure.

Changing CM passwords from ETA client

Changing CM passwords consists of Changing CM passwords in the DCE security database and Changing the CM password on the DMS-100 switch. ETA clients can change their own user passwords at the ETA main window.

Note: You can change the CM password on the DMS switch before or immediately after you have changed the CM password in the DCE security database.

Changing CM passwords in the DCE security database

Use the following procedure to change your CM password in the DCE security database.

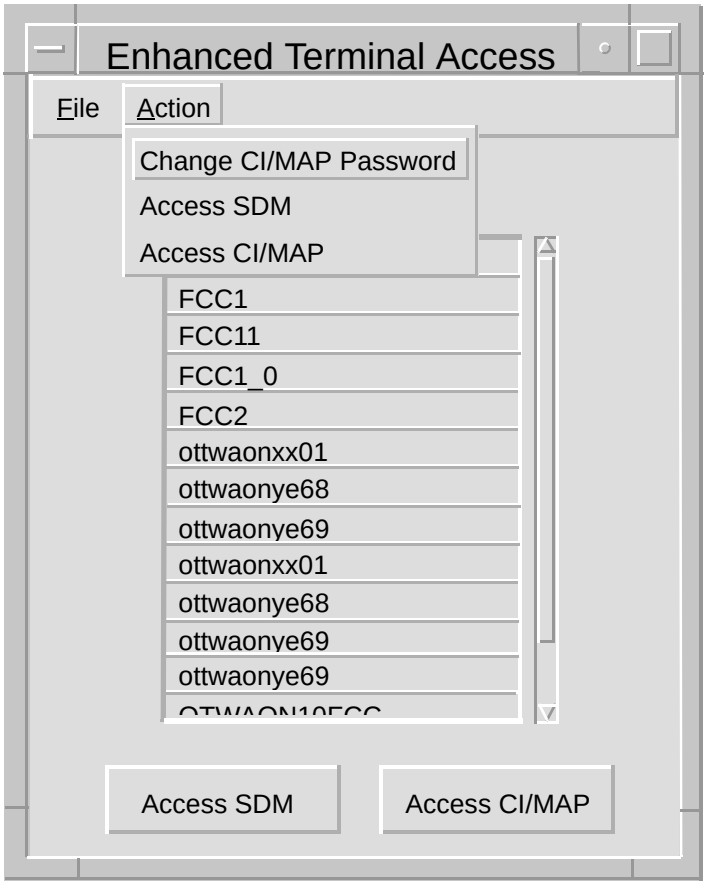
Changing CM passwords in the DCE security database

At the ETA main window

1 Select Change CI/MAP Password from the Action pull-down menu.

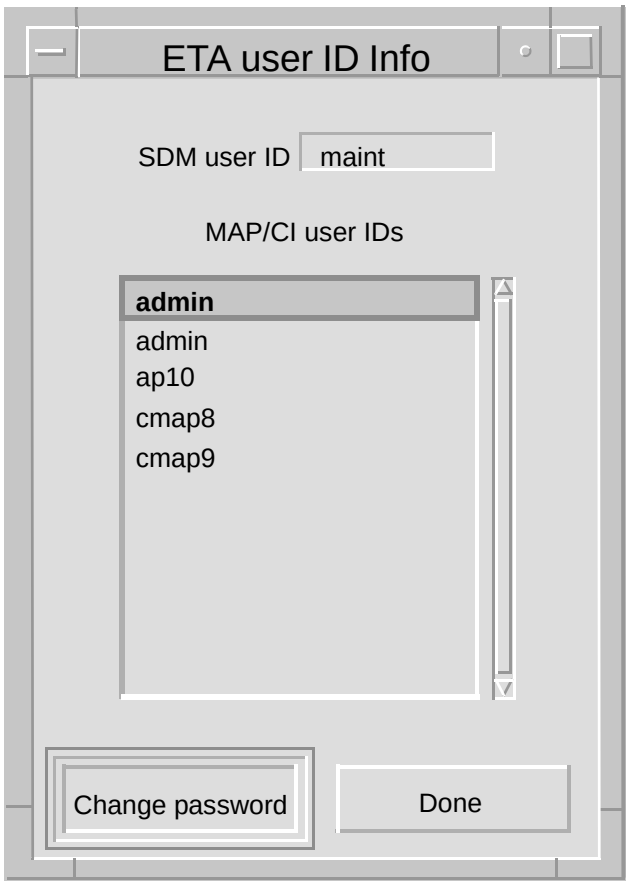
The ETA user ID Info window appears.

ETA window



2 Click on the CM user ID for which you want to change the password.

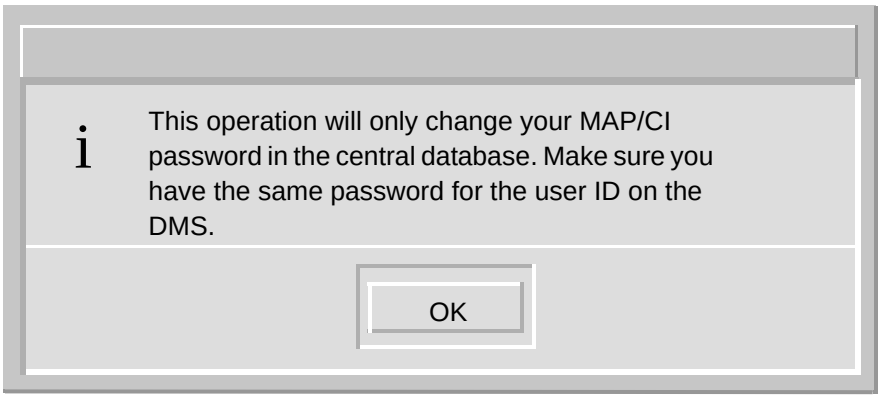
ETA user ID info window



3 Click on Change password button.

A warning message appears.

MAP/CI password change warning message

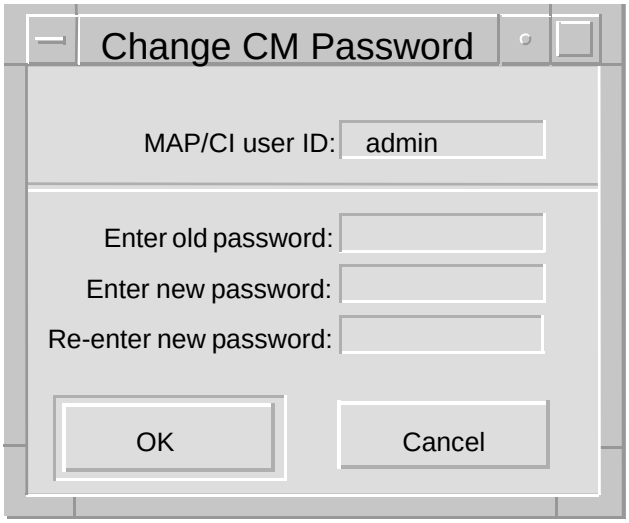


4 Click OK to continue.

Note: The two administration user IDs are used to access different DMS switches. This allows multiple passwords to be used with each CM user ID.

The Change CM Password window appears.

Change CM Password window



5 Enter the old password, the new password, and re-enter the new password. Click the OK button when you are finished.

The Change CM Password window disappears after you click Ok.

6 Use the following table to determine your next step.

If you are	Do
changing another password	step 2
finished changing passwords	step 7

7 Click on Done from the ETA User ID Info window.

8 You have completed this procedure.

Changing the CM password on the DMS switch

Use the following procedure to change your CM password. You must complete this procedure before or immediately after you change your CM password in the DCE security database.

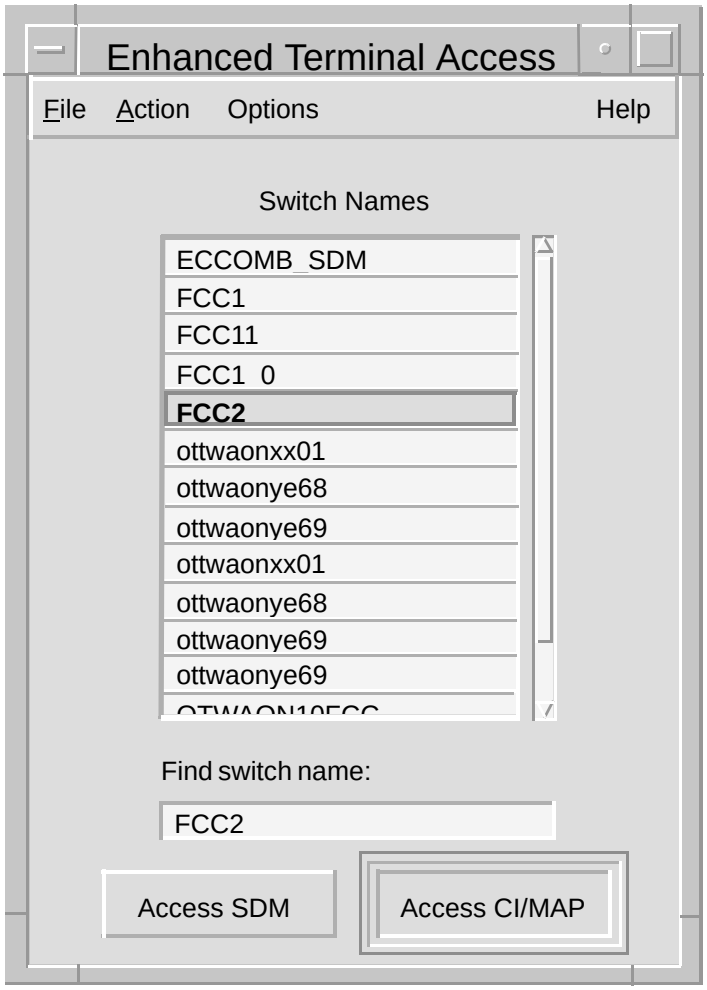
Note: Under certain conditions, the CM response from a user-entered command and subsequent user keyboard input compete for the display cursor. The CM output and the user input can be interleaved causing garbled data to appear. This limitation also exists on the telnet sessions using an Ethernet Interface Unit (EIU). To correct this problem, refresh the screen. This limitation does not corrupt data or user commands on the CM.

Changing the CM password on the DMS-100 switch

At the ETA main window:

1 Select the name of the DMS switch.

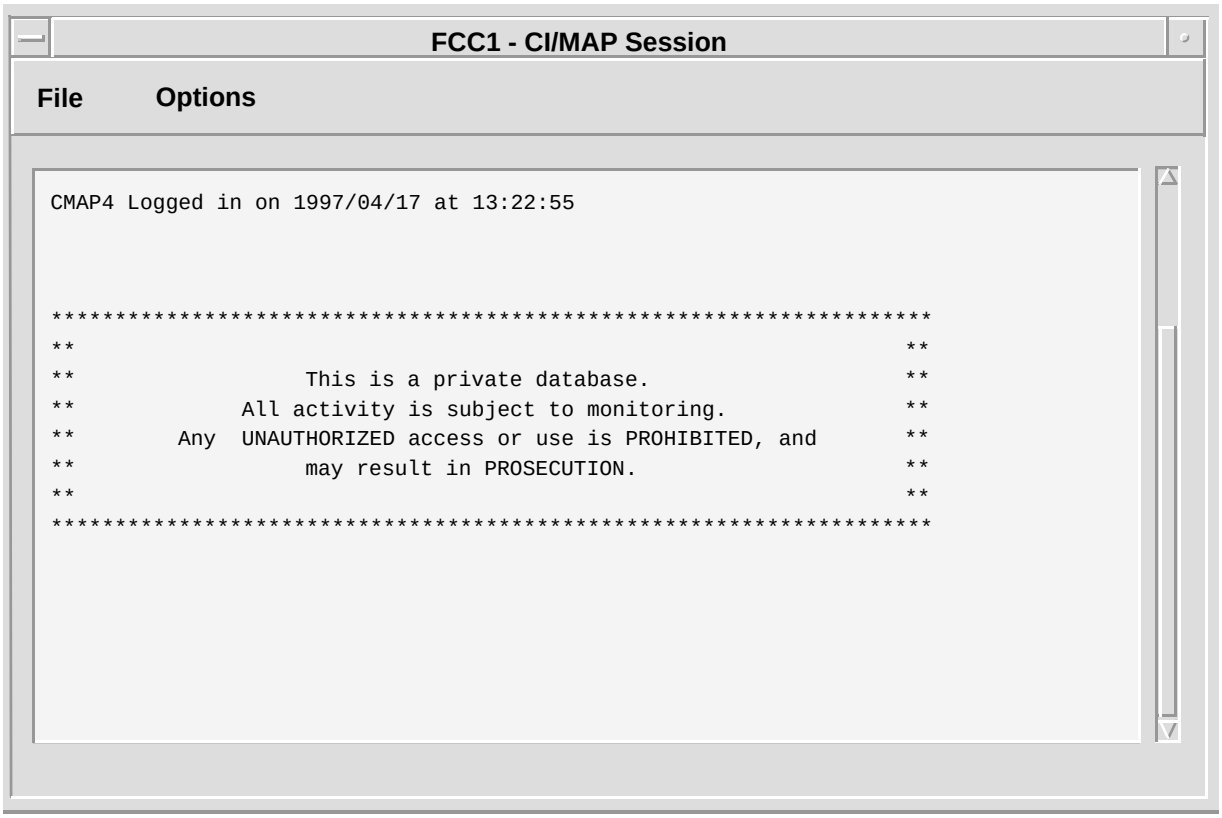
ETA main window



2 Click the Access CI/MAP button.

A CI/MAP session window appears.

Example CI/MAP session window



3 Change the CM password on the DMS switch:

> password

4 Enter your new password.

Example response:

```
Please enter new password again to verify.
```

5 Enter your new password again.

Response:

```
Enter your current password to verify.
```

6 Enter your old (current) password.

A message informs you that the password has been successfully changed, and that it must be changed in 30 days.

7 You have completed this procedure.

Changing logical volume thresholds

Purpose

Use this procedure to change SDM logical volume thresholds.

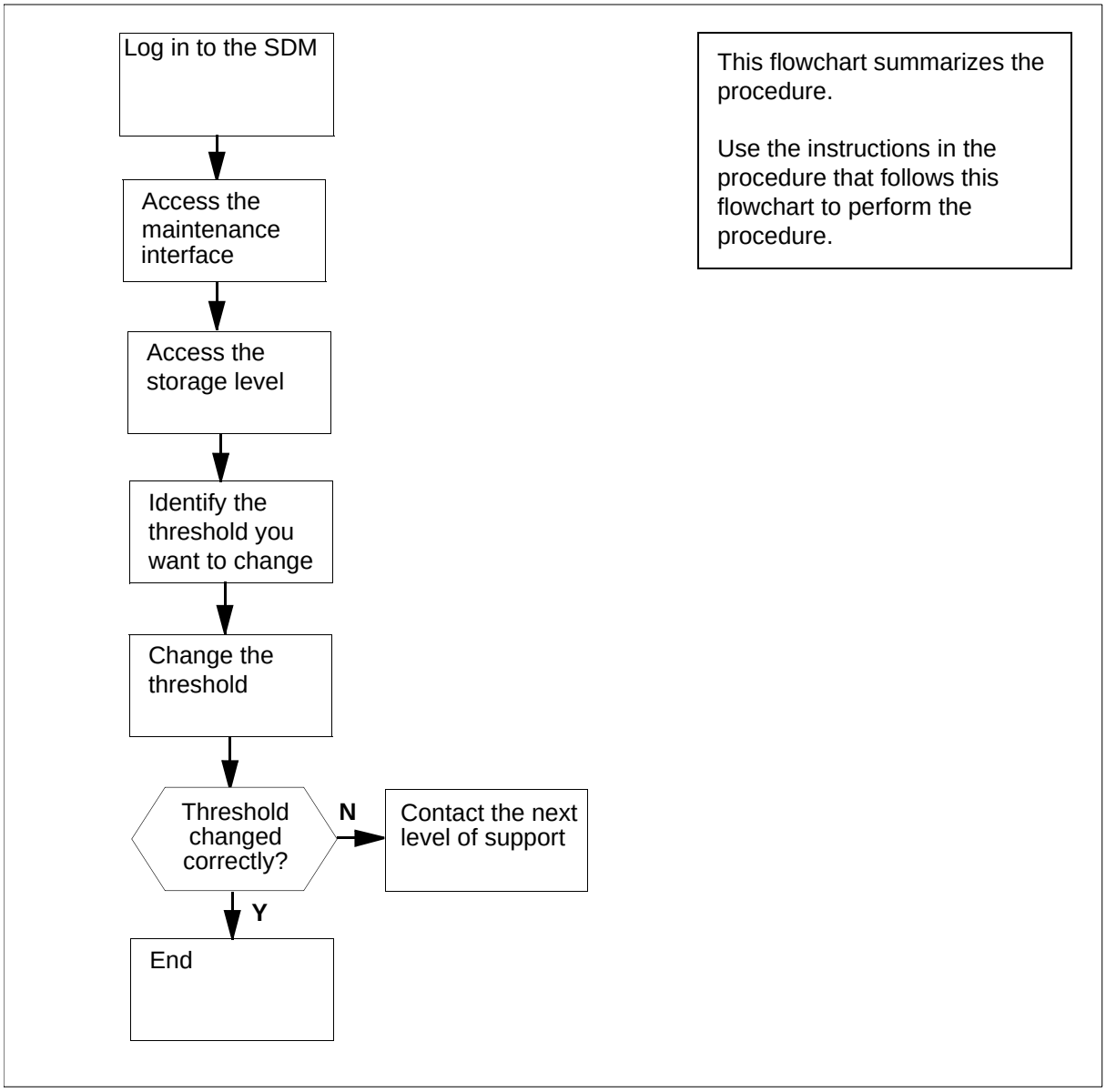
Application

Use this procedure to change SDM logical volume thresholds.

Action

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

Summary of changing logical volume thresholds



Changing system thresholds

At the local VT100 console

1 Log into the SDM.

2 Access the maintenance interface:

 # sdmmtc

3 Access the storage level:

> storage

Example Response:

```
Volume Group        Status          Free (MB)
rootvg              Mirrored        1932
datavg              Mirrored        7760

Logical Volume  Location   Size(MB)    % full/
threshold
1 /            rootvg     88              25/ 80
2 /usr          rootvg      600            85/ 90
3 /var          rootvg      200            11/ 80
4 /tmp          rootvg      24              6/ 90
5 /home         rootvg      304             4/ 70
6 /sdm          rootvg      504            44/ 90
7 /data         datavg      208             6/ 80
                Logical volumes showing: 1 to 7
of 7
```

4 Identify the logical volume threshold to change. Note the entry number of the logical volume on the left of the storage menu.

5 Change the logical volume threshold:

> change <n> <x>

where

<n>
is the entry number of the logical volume for which you want to change the threshold

<x>
is the new threshold value

Example input:

> change 5 80

6 Wait 5 seconds. Check to see that the logical volume threshold changed to the value that you entered.

If the logical volume threshold did not change correctly, contact your next level of support.

7 You have completed this procedure.

Changing system thresholds

Purpose

Use this procedure to change SDM system thresholds.

Application

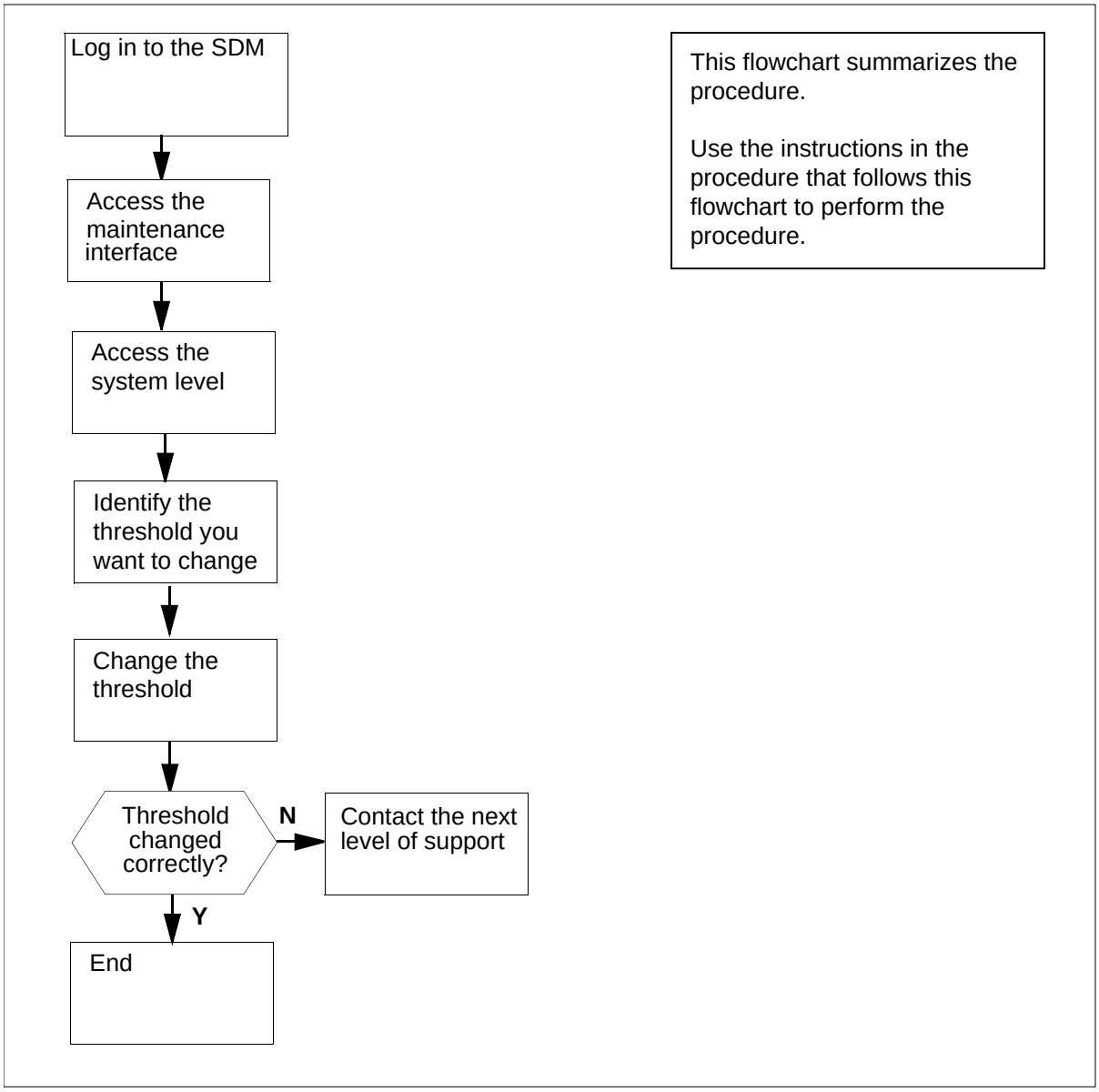
You can change the following SDM system thresholds at the system menu level of the Remote Maintenance Interface (RMI):

- CPU (run queue entries)
- number of Processes
- number of Zombies
- Swap Space (% full)
- number of Swap Queue Entries

Action

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

Summary of changing system thresholds



Changing system thresholds

At the local VT100 console

1 Log into the SDM.

2 Access the maintenance interface:

 # sdmmtc

3 Access the system (Sys) level:

> sys

Example response:

```
SDM Storage State:          .

#
Description                          Current/Thres
hold
1 CPU (run queue entries):                1/  5
2 Number of Processes:                   63/250
3 Number of Zombies:                      0/  3
4 Swap Space (% full):                   72/ 70*
5 Number of Swap Queue Entries:           0/  2
```

4 Identify the system threshold to change. Record the entry number of the system threshold located on the left System menu. The number is shown under the header #.

In the example in step 3:

- entry number for CPU threshold is 1
- entry number for the Number of Processes threshold is 2
- entry number for the Number of Zombies is 3
- entry number for the Swap Space threshold is 4, and
- entry number for Number of Swap Queue Entries is 5

The current threshold value is shown in the right column under the header Current/Threshold.

5 Change the system threshold:

> change <n> <x>

where

<n>
is the entry number of the threshold you want to change

<x>
is the new threshold value

Example input:

> change 4 80

6 Wait 5 seconds. Check if the system threshold changed to the value that you entered.

If the system threshold did not change correctly, contact your next level of support.

7 You have completed this procedure.

Recovering the system when root password unknown

Purpose

Use this procedure to change the root user password when it is not known.

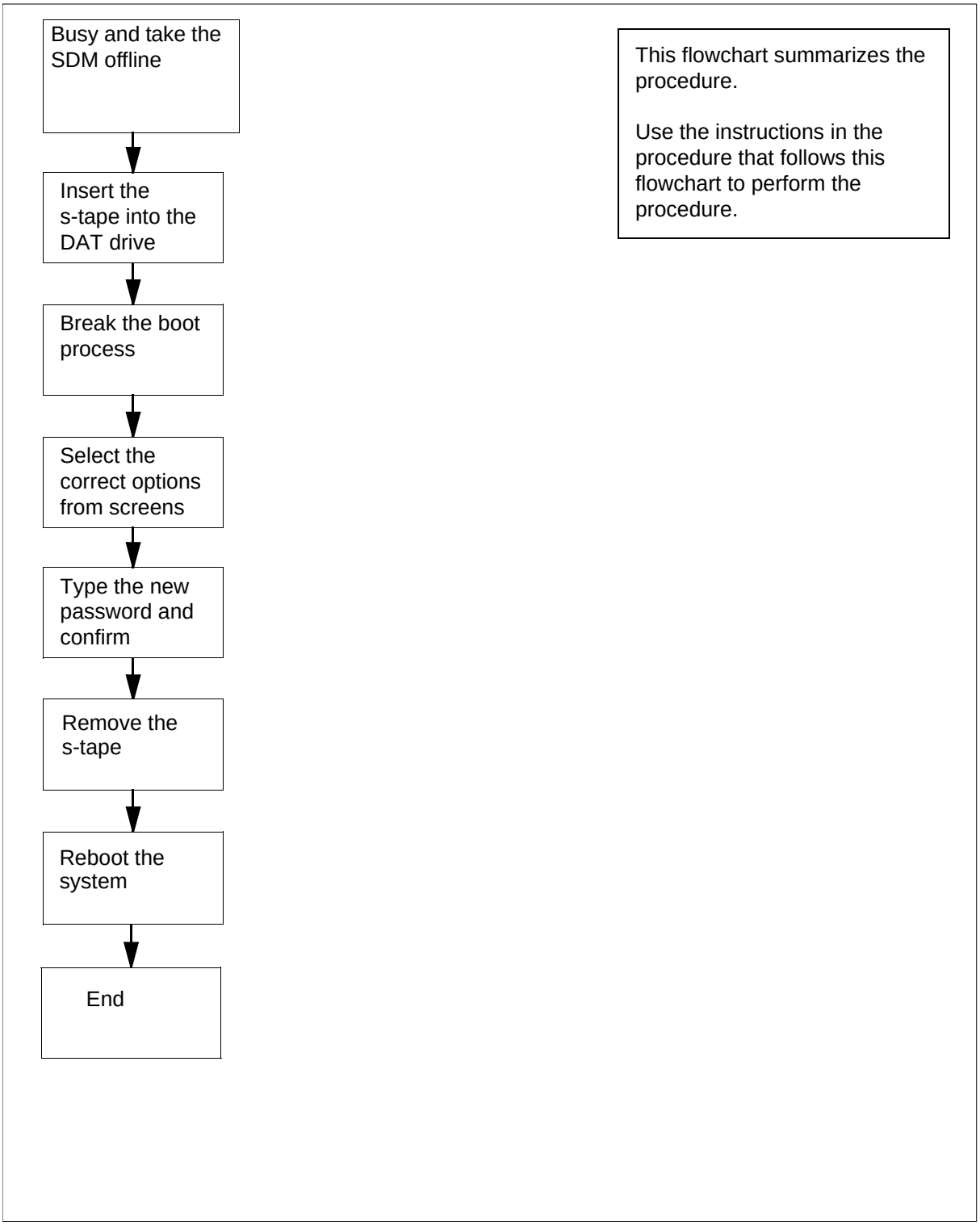
Application

If the ETA application is installed and in service, use the ETA application to open a root user session. Then, use the procedure Changing a user password in this section to change the root password.

Action

The following flowchart summarizes the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the tasks.

Summary for recovering the system when root password unknown



Recovering the system when root password unknown

At the SDM level of the MAP display

1 Busy the SDM:

> bsy

You are prompted to confirm whether you want to busy the SDM.

2 Confirm that you want to busy the SDM:

> y

At the SDM

3 Insert the latest system backup tape (s-tape) into DAT drive 0 (slot 2).

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

At the SDM level of the MAP display

4 Reboot the SDM:

> rebootsdm

At the local console

5 When the system displays COLD Start, press the Break key or the Esc key twice to interrupt the boot process.

6 Reboot the system:

Fx-Bug> pboot 1 50

The system displays progress messages. When they are completed, proceed to the next step.

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

7 At the “Please define the system console” display, enter:

> 1

8 At the second interactive screen, select 1 for English.

9 At the “Welcome to base operating system installation and maintenance” display, select 3 to begin the maintenance mode for system recovery.

10 At the Maintenance display, select 1 to access a root volume group.

11 At the Warning display, select 0.

The “Access a Root Volume Group” display lists the volume groups with the disks they contain. Each disk has a name, (for example, hdisk0) and a location code (for example 4056 c1-f2-00-0,0).

12 Enter the number of the volume group whose location code contains the characters c1-f2. Press the Enter key.

```
Example output:
1) Volume Group 002e43cdaa6655f5 contains these
disks:       hdisk1 4056 c1-f4-00-0,0    hdisk2
4056 c1-f4-00-1,0        hdisk3 4056
c1-f4-00-0,0  hdisk4 4056c1-f15-00-1,0
2) Volume Group 002e43cda6d92fc7 contains these
disks:       hdisk0  4056 c1-f2-00-0,0  hdisk3
4056c1-f13-00-0,0
```

13 At the Volume group information display, select 1 to access the volume group and start a UNIX shell.

14 At the UNIX prompt enter:

 # passwd root

and press the Enter key. The system prompts you for a new root password.

15 Enter the new root password. When prompted, re-enter the new root password.

16 Confirm the password change:

 # ls -l /etc/passwd

```
Example output:
-rw-r--r--1 root root11539 Jul 912:37
/etc/passwd
```

17 Check that the date and time that are displayed as a result of step 16 are the current date and time.

If the current date and time	Do
are displayed	step 18
are not displayed	contact your next level of support

18 Remove the s-tape.

19 Reboot the system:

 # shutdown -Fr

When the reboot completes, the login prompt appears. You must then use the new password to log in as the root user.

20 You have completed this procedure.

Recommissioning date and time zone

Application

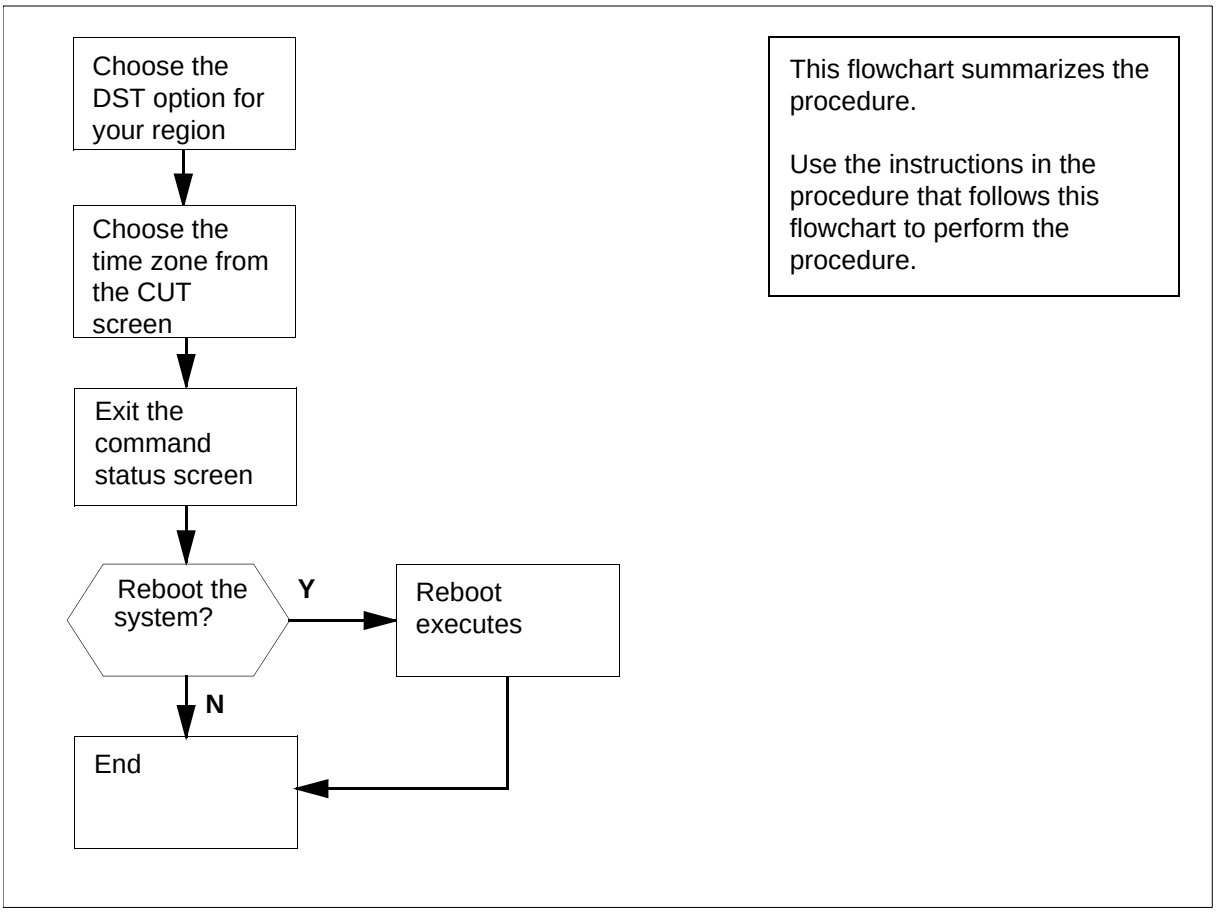
Use this procedure to commission the date, time, and time zone on the SDM.

To recommission the date, time, and time zone, the node state must either be ManB or OffL, and the node must not be DCE synchronized. Refer to the procedure, “Removing an SDM from a DCE” in the Configuration section. This restriction does not apply to initial commissioning.

Action

The following flowchart summarizes the procedure. Use the instructions in the procedure that follows the flowchart to perform the task.

Summary of commissioning miscellaneous items: date, time, and time zone



Commissioning miscellaneous items: date, time, and time zones

CAUTION
Inability to recommission time zone
To recommission the date, time, and time zone, the node state must either be ManB or OffL, and the node must not be DCE synchronized. With the exception of initial commissioning, you do not have the option of recommissioning the date, time, and time zone if the SDM is not ManB or Offl and if DCE is running and in service.

At the local VT100 console

1 Log in to the SDM.

2 Access the commissioning level by typing

```
# sdmconfig
```

and pressing the Enter key.

3 Select the Time and Time Zone option by typing

```
> 2
```

and pressing the Enter key.

The system displays the prompt for the date, time, and time zone configuration preview window.

```
SDM COMMISSIONING

DATE, TIME AND TIME ZONE

You will be prompted for time and date
information. Once you have entered the
information, you will need to reboot the SDM for
the changes to take effect.

HIT ENTER TO CONTINUE
```

4 Press the Enter key to continue.

The system displays the Change / Show Date, Time, and Time Zone screen.

5 Use the following table to determine your next step.

If you	Do
follow the daylight saving time conventions for North America	step 7
do not follow the daylight saving time conventions for North America	step 6

Note 1: Under North American conventions, the move from standard time to daylight saving time occurs on the first Sunday of April. On this day, clock time is moved forward one hour at 2:00 a.m. The move from daylight saving time to standard time occurs on the last Sunday of October. On this day, clock time is moved backward one hour at 2:00 a.m.

Note 2: If you do not follow the North American daylight saving time zone conventions, check with appropriate personnel for the dates and times that daylight saving changes occur in your region.

6 Select Change Time Zone Using User Entered Values on the Change / Show Date, Time, and Time Zone screen, and press the Enter key. The Change Time Zone screen appears.

Use the up and down arrow keys to move the cursor and highlight the entries in the entry fields. Change the value in the field after you highlight it. When you finish changing the values in the fields, press the Enter key and go to step 9.

The following table explains each of the value fields in the Change Time Zone window, and their formats.

(Sheet 1 of 4)

Field or subfield	Value	Description
Standard Time ID	Alphabetic characters	Any identifier you wish to use for your region's standard time.
Standard Time Offset from CUT		Identifies the value that must be added to or subtracted from local standard time to equal Coordinated Universal Time (CUT). This field contains the subfields HH:MM:SS, as follows.

(Sheet 2 of 4)

Field or subfield	Value	Description
[+|-] HH (required)	Range of integers between -12 and +11	Identifies the number of hours in the offset, and whether to add or subtract the offset.
MM (optional)	Numeric between 0 and 59. Always preceded by a colon (:)	Identifies the number of minutes in the offset.
SS (optional)	Numeric between 0 and 59. Always preceded by a colon (:)	Identifies the number of seconds in the offset.
Daylight Saving Time ID	Alphabetic characters	Any identifier you want to use for your region's daylight saving time.
Daylight Saving Time Offset from CUT		Identifies the value that must be added to or subtracted from local daylight time to equal CUT. This field contains the subfields HH:MM:SS (as explained under Standard Time Offset from CUT, preceding.)
Start Daylight Saving Day		Identifies the date on which daylight saving time starts. This field contains the subfields Mmm.ww.dd or Jn, as follows.
M	Constant	Indicates that the date is being specified using the mm.ww.dd subfields.
mm	Numeric between 1 and 12	Identifies the month.

(Sheet 3 of 4)

Field or subfield	Value	Description
ww	Numeric between 1 and 5 (one digit), always preceded by a period (.)	Identifies the number of the week within the month, as follows: • 1 if the date falls on the 1st to the 7th day • 2 if the date falls on the 8th to the 14th day • 3 if the date falls on the 15th to the 21st day • 4 if the date falls on the 22nd to the 28th day • 5 if the date falls on the 29th to the 31st day
dd	Numeric between 0 and 6, always preceded by a period (.)	Identifies the day of the week, as follows: • 0 for Sunday • 1 for Monday • 2 for Tuesday • 3 for Wednesday • 4 for Thursday • 5 for Friday • 6 for Saturday
J	Constant	Indicates that the date string is being specified using a 365-day calendar.
n	Numeric between 1 and 365	Indicates the number of the date in a 365-day calendar year.

(Sheet 4 of 4)

Field or subfield	Value	Description
Start Daylight Saving Time	None	Identifies the time at which Daylight Saving Time starts. This field contains the subfields HH:MM:SS (as explained in Standard Time Offset from CUT, preceding, but without a plus or minus sign on the HH subfield).
Stop Daylight Saving Day	None	Identifies the date on which Daylight Saving Time stops. This field contains the subfields Mmm.ww.dd or Jn (as explained in Start Daylight Saving Day, preceding).
Stop Daylight Saving Time		Identifies the time at which Daylight Saving Time stops. This field contains the subfields HH:MM:SS (as explained in Standard Time Offset from CUT, but without a plus (+) or minus (-) sign on the HH subfield).

7 Select Change Time Zone Using System Defined Values on the Change / Show Date, Time, and Time Zone screen, and press the Enter key.

The Use Daylight Savings Time? screen appears.

8 Use the up and down arrow keys to select an option in response to the question, “Does this time zone go on daylight saving time?” Select “yes” (option 1) if at some time in the year daylight saving time is applied to this time zone. Otherwise, select “no” (option 2). Press the Enter key when you have selected the appropriate response.

The system displays the CUT (Coordinated Universal Time) Time Zone screen.

Each option in the CUT Time Zone screen corresponds to a Greenwich Mean Time (GMT) value, as shown in the following table.

(Sheet 1 of 2)

Name on screen	Text on screen	Offset CUT value on screen	GMT value
CUT0GDT	Coordinated Universal Time	CUT	GMT
GMT0BST	United Kingdom	CUT	GMT
AZOREST1AZOREDT	Azores; Cape Verde	CUT -1	GMT -01:00
FALKST2FALKDT	Falkland Islands	CUT -2	GMT -02:00
GRNLNDST3GRNLNDDT	Greenland; East Brazil	CUT -3	GMT -03:00
AST4ADT	Central Brazil	CUT -4	GMT -04:00
EST5EDT	Eastern U.S.; Columbia	CUT -5	GMT -05:00
CST6CDT	Central U.S.; Honduras	CUT -6	GMT -06:00
MST7MDT	Mountain U.S.	CUT -7	GMT -07:00
PST8PDT	Pacific U.S.; Yukon	CUT -8	GMT -08:00
AST9ADT	Alaska	CUT -9	GMT -09:00
HST10HDT	Hawaii; Aleutian	CUT -10	GMT -10:00
BST11BDT	Bering Straits	CUT -11	GMT -11:00
NZST-12NZDT	New Zealand	CUT +12	GMT +12:00
MET-11METDT	Solomon Islands	CUT +11	GMT +11:00
EET-10EETDT	Eastern Australia	CUT +10	GMT +10:00
JST-9JDT	Japan	CUT +9	GMT +09:00
KORST-9KORDT	Korea	CUT +9	GMT +09:00
WAUST-8WAUDT	Western Australia	CUT +8	GMT+08:00

(Sheet 2 of 2)

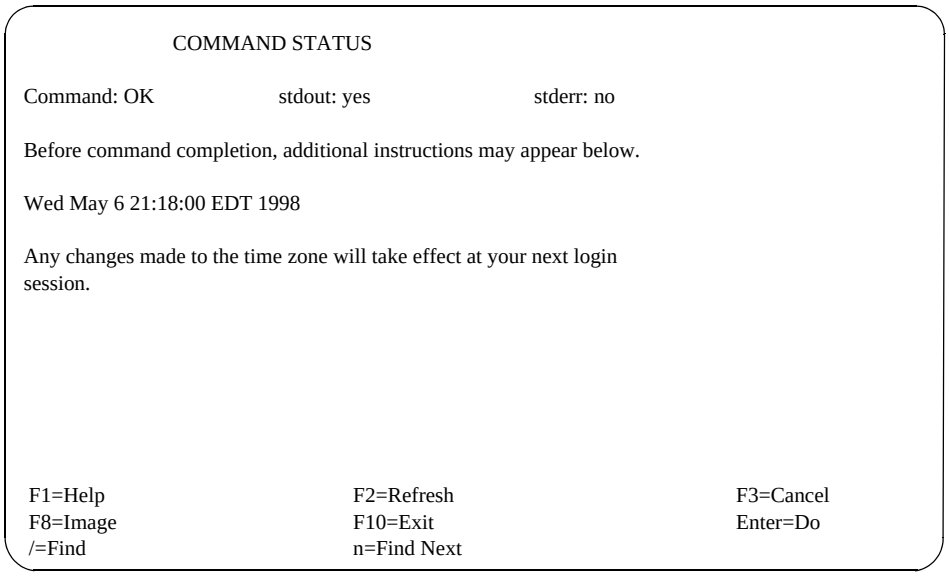
Name on screen	Text on screen	Offset CUT value on screen	GMT value
TAIST-8TAIDT	Taiwan	CUT +8	GMT +08:00
THAIST-7THAIDT	Thailand	CUT +7	GMT +07:00
TASHST-6TASHDT	Tashkent; Central Asia	CUT +6	GMT +06:00
PAKST-5PAKDT	Pakistan	CUT +5	GMT +05:00
WST-4WDT	Gorki, Central Asia; Oman	CUT +4	GMT +04:00
MEST-3MEDT	Turkey	CUT +3	GMT +03:00
SAUST-3SAUDT	Saudi Arabia	CUT +3	GMT +03:00
WET-2WET	Finland	CUT +2	GMT +02:00
USAST-2USADT	South Africa	CUT +2	GMT+ 02:00
NFT-1DFT	Norway; France	CUT +1	GMT +01:00

9 Use the up and down arrow keys to select the time zone you use. Then press the Enter key. The Change Time Zone screen appears.

10 You do not need to change the variables on the Change Time Zone screen. Press the Enter Key.

11 The Command Status screen appears. The command status is shown as “running” while the changes are being processed. The command status changes to “OK” when processing is complete. The date, time, and time zone appear.

Example response:



Note: If the command status changes to “Failed”, repeat this procedure.

12 Exit the Command Status screen by pressing the F10 key, Esc+10, or PF10 keys.

Response:

```
SDM COMMISSIONING
DATE, TIME AND TIME ZONE

Your time and date information has been entered.
For this information to take effect, you will
need to reboot the SDM.

Do you wish to reboot the SDM now?
Please confirm (“YES”, “Y”, “NO”, or “N”)
```

If you wish to	Do
defer rebooting the SDM	type n and press the Enter key you have completed this procedure
reboot the SDM	step 13

13 Confirm the system reboot by typing

> y

and pressing the Enter key.

Wait until the reboot completes and the login prompt reappears.

14 You have completed the procedure.

Changing the system date or time

Purpose

Use this procedure to change the system date or time on the SDM.

Application

This procedure does not replace the commissioning procedure Changing the system time zone and daylight savings time parameters on page 165.

ATTENTION

This procedure is for in-operation SDMs only. If you are configuring the SDM for the first time, use the procedure Changing the system time zone and daylight savings time parameters on page 165.

ATTENTION

To change the date or time the node state must either be ManB or OffL and the node must not be DCE synchronized. If the node is DCE synchronized, change the time on the DCE server. The DCE server controls the time change for all nodes under its control in the DCE cell.

ATTENTION

This procedure cannot be used to change the date or time while the SDM is in split-mode.

Interval

Perform this procedure to change the system date or time when the SDM is in operation, and not controlled by a DCE server.

Action

Ensure that the SDM is either ManB or OffL.

Changing the system date or time

At the local VT100 terminal

1 Log in to the SDM.

2 Access the maintenance interface level:

 # sdmmtc

3 Access the admin level:

> admin

4 Select “Time” from the menu:

> 9

The Time screen is displayed with one menu option “Change.”

Note: You must select the “Time” menu item to change the date or the time.

5 Select “Change” from the menu:

> 5

6 Accept or change the year.

If you want to	Do
accept the specified “Year”	press Enter, and proceed to step 7
change the specified “Year”	edit the value, press Enter, and proceed to step 7

7 Accept or change the month.

If you want to	Do
accept the specified “Month”	press Enter, and proceed to step 8
change the specified “Month”	edit the value, press Enter, and proceed to step 8

8 Accept or change the Day.

If you want to	Do
accept the specified “Day”	press Enter, and proceed to step 9
change the specified “Day”	edit the value, press Enter, and proceed to step 9

9 Accept or change the Hour.

If you want to	Do
accept the specified “Hour”	press Enter, and proceed to step 10
change the specified “Hour”	edit the value, press Enter, and proceed to step 10

10 Accept or change the Minutes.

If you want to	Do
accept the specified “Minutes”	press Enter, and proceed to step 11
change the specified “Minutes”	edit the value, press Enter, and proceed to step 11

11 Accept the new date and time:

> y

12 You have completed this procedure.

Stopping and restarting an application

Purpose

Use this procedure to stop and restart applications.

Note:

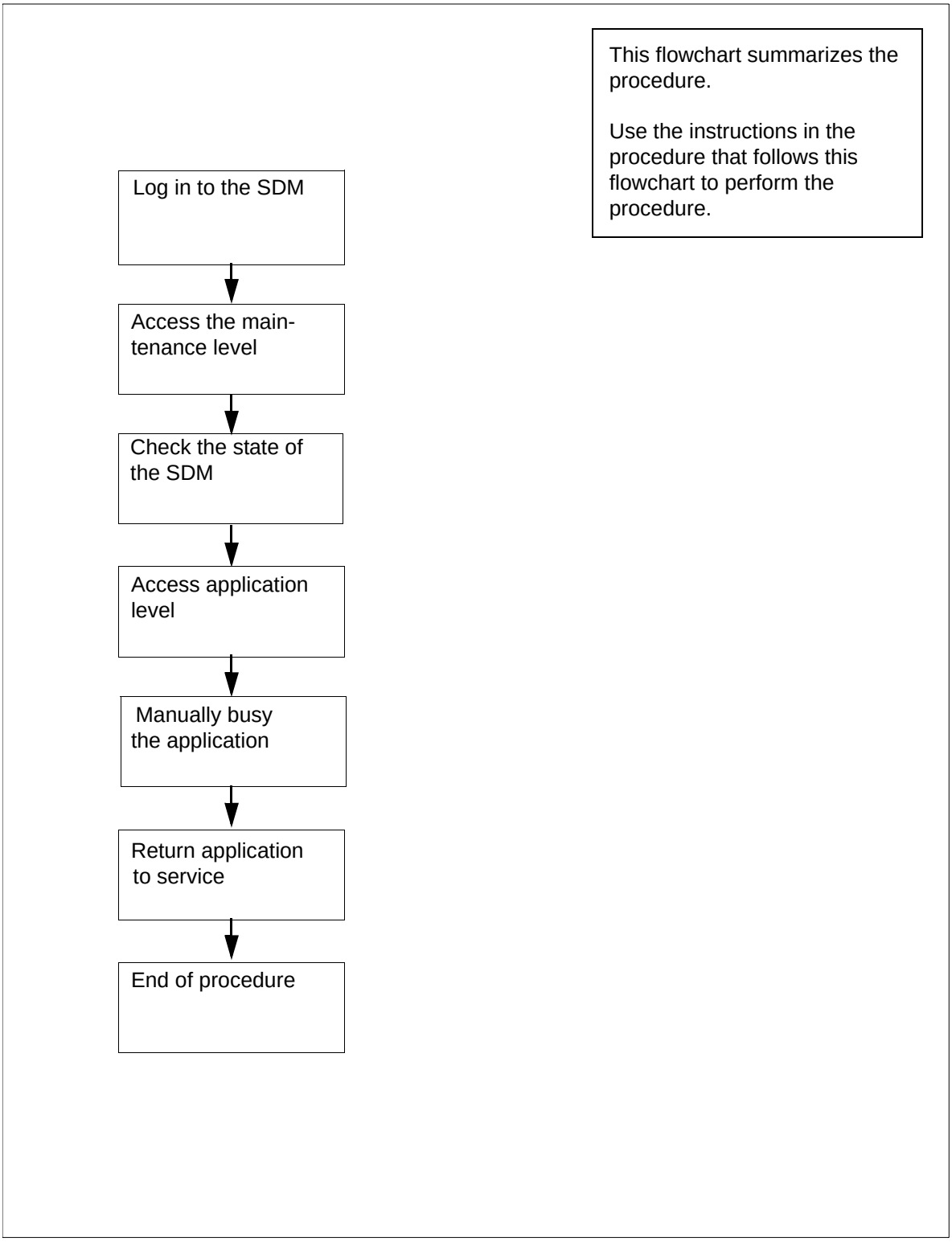
Application

Use this procedure to stop (manually busy) and restart (return to service) SDM software applications.

Action

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

Summary of stopping and restarting an application



Stopping and restarting an application

At the local or remote VT100 terminal

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

2 Access the maintenance interface:

 # sdmmtc

3 Access the application level:

> appl

4 Busy the software application:

> bsy <n>

where

<n>
is the number next to the application to busy

Example response:

```
The application is in service.
This command will cause a service interruption.
Please confirm (“YES”, “Y”, “NO”, or “N”):
```

Note: Busying the application as shown performs an orderly shutdown and can take up to 2 minutes.

5 Confirm the Busy command:

> y

After you confirm the Bsy command, the following is displayed:

Example response:

```
Application Bsy- Command initiated.Please
wait...

Application Bsy - Command complete.
```

6 Return the application to service:

> rts <n>

where

<n>
is the number next to the application you want to return to service

Example response:

```
Application RTS - Command initiated.
Please wait...

Application RTS - Command complete.
```

7 You have completed this procedure.

Deleting a DCE user

Purpose

Use this procedure to delete a DCE user.

Application

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

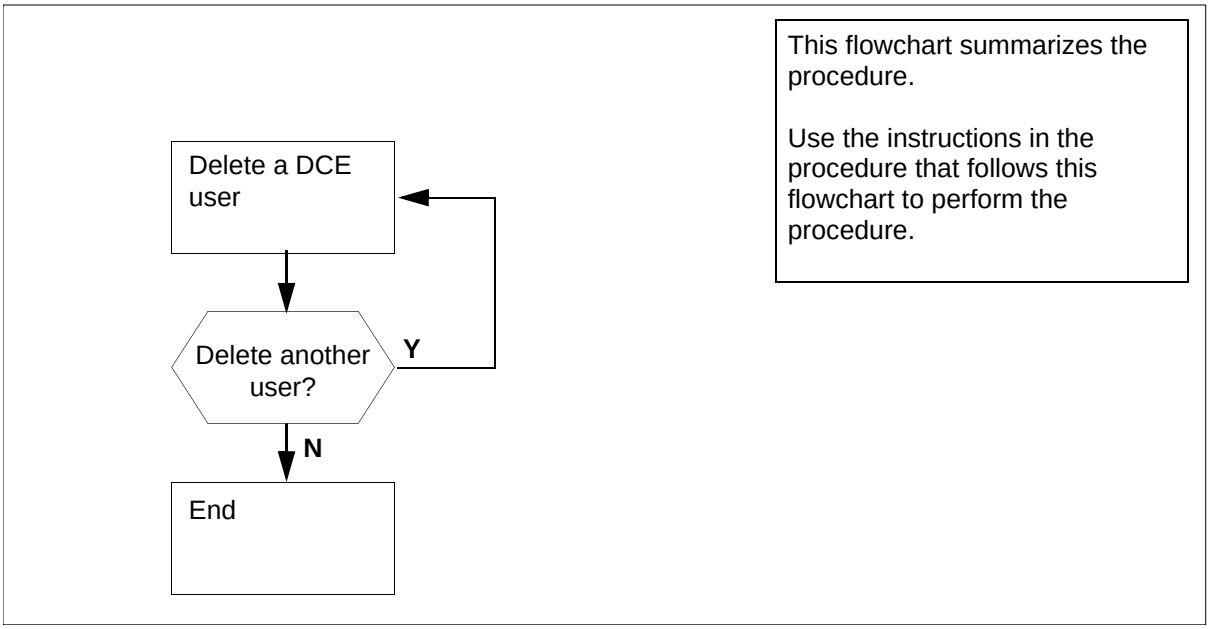
ATTENTION
Use a DCE master administration account (cell_admin) or a DCE sub administrator account (sdm_admin) to perform this procedure. You cannot use the sdm_admin account to delete a DCE user created by a cell_admin account.

The cell_admin account can delete any DCE users created by either the cell_admin or sdm_admin account.

Action

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

Summary of Deleting a DCE user



Deleting a DCE user

At the SDM remote client workstation

1 Delete a DCE user:

> /sdm/bin/delete_dce_user

Example response:

```
DCE administrator user ID [sdm_admin]:
```

2 Enter the DCE user ID.

Note: If you do not enter a user ID, the system enters the default value (sdm_admin).

Example response:

```
sdm_admin password:
```

3 Type your DCE administrator password.

Response:

```
DCE user ID to be deleted:
```

4 Enter the DCE user ID you want to delete.

Example response:

```
The DCE user ID “ops_1” has been deleted.
```

5 You have completed this procedure.

Establishing a modem connection

Purpose

Use the following procedure to establish a dial-up modem connection to the SDM from a remote location.

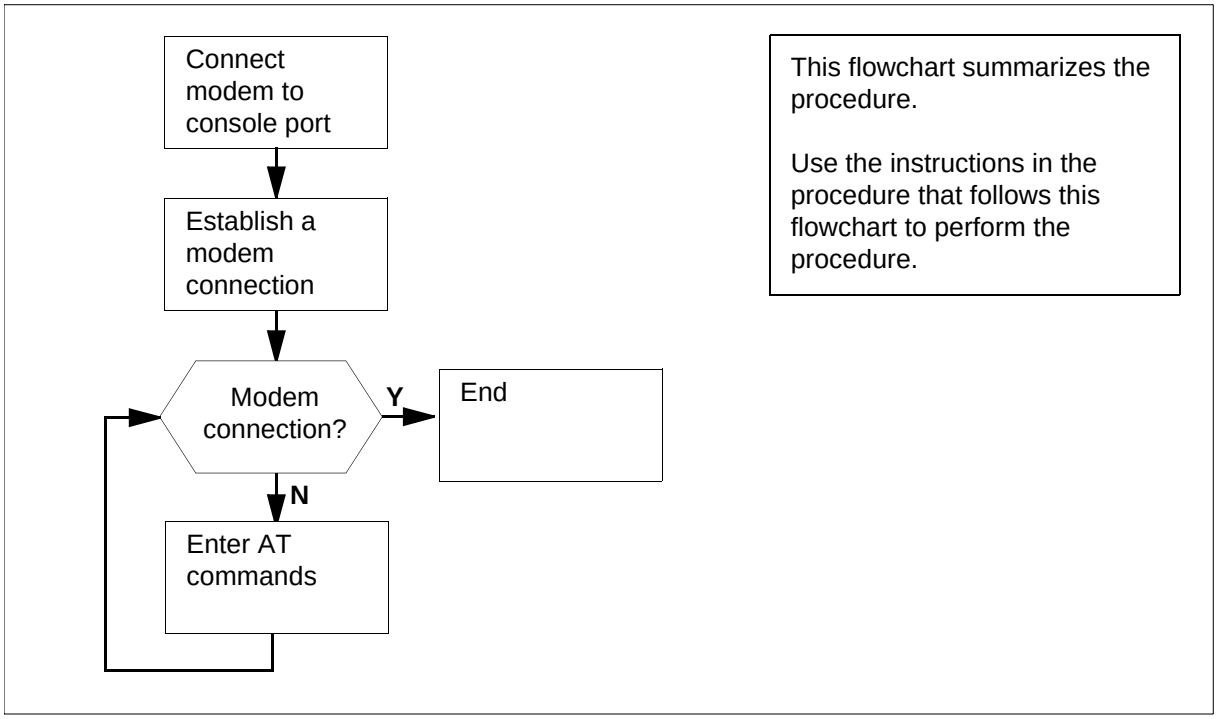
Application

Use the General DataComm (GDC) maintenance modem provided with the SDM equipment whenever a console dial-up modem connection to the SDM from a remote location is required. The GDC maintenance modem is installed and configured as part of the installation of the SDM.

Action

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

Summary of establishing a modem connection



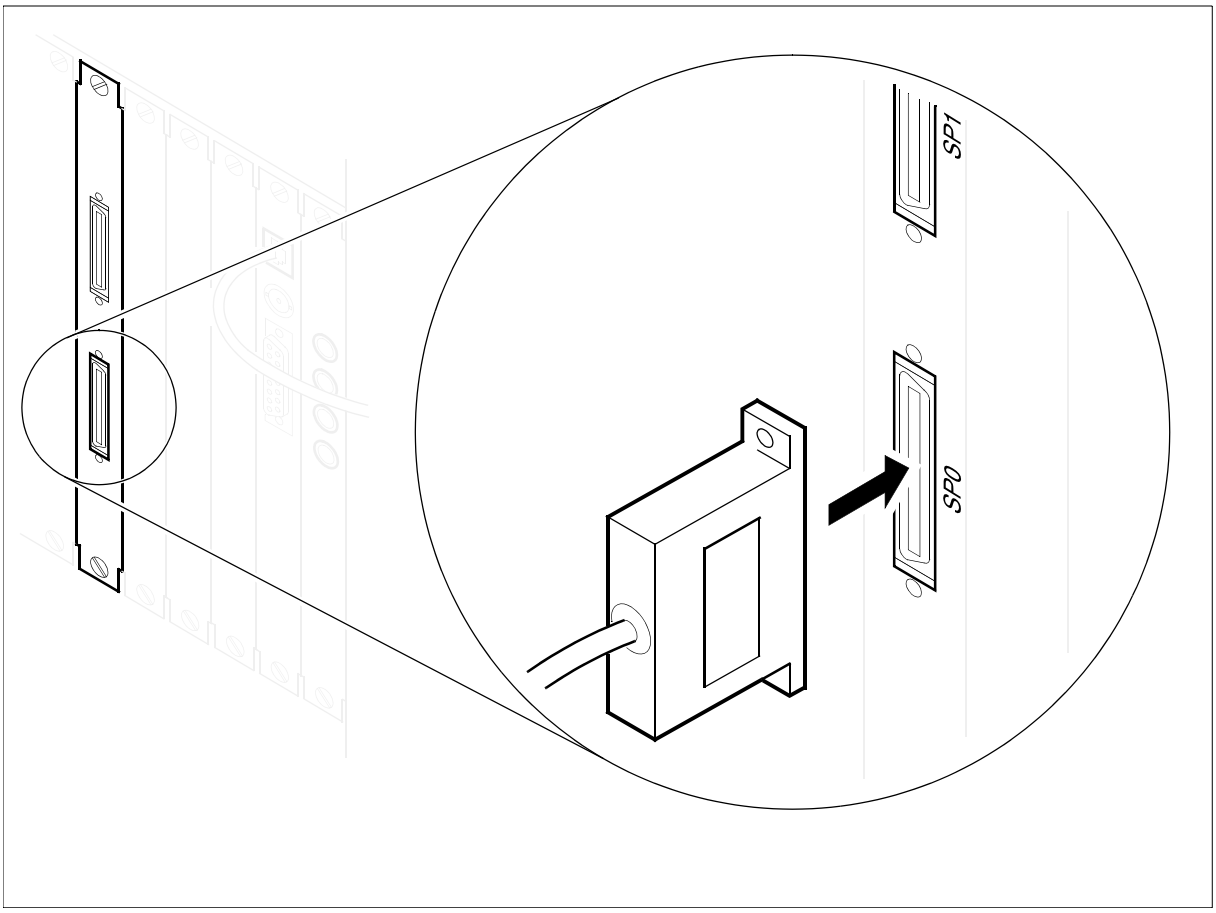
Establishing a modem connection

At the SDM

1 If necessary, connect the GDC maintenance modem to the SDM by first ensuring no other terminal device cables are connected to console port SP0 on the CPU personality module.

2 If necessary, connect the NTRX5093 cable connected to the GDC maintenance modem to port SP0, and ensure a phone line is connected to the GDC maintenance modem. See the diagram below.

Note: The modem is located in the appropriate MIS frame.



At a remote VT100 console

3 Use a terminal connected to a V.34 Hayes-compatible modem (or to other compatible communications equipment connected to a V.34 modem) to establish remote connection to the SDM console port.

4 Establish a modem connection to the SDM by entering

> atdt <dial_in_number>

where

<dial_in_number>
is the telephone number for the modem attached to serial port 1

Note: For information on establishing a modem-to-modem connection, refer to the dial-up connection instructions provided with the communications equipment you are using.

5 Determine if the connection has been established.

If you	Do
receive a login prompt	log in using your user ID and password you have completed this procedure
do not receive a login prompt	step 6

6 Execute the following steps to reconfigure your modem, starting at step 8. If you have connection problems, contact your next level of support.

7 Configure the GDC maintenance modem by connecting a VT100 console set to communicate at 9600 baud directly to the DTE connector on the GDC maintenance modem.

8 Enter the AT commands by first entering:

> AT&F0

Note 1: Echo of the command entry depends on the previous configuration.

Note 2: If you make a mistake when entering the AT commands, restart the procedure at step 1

9 When the modem responds “OK”, enter

> AT\T7

10 When the modem responds “OK”, enter

> AT&R2

11 When the modem responds “OK”, enter

> AT&C1

12 When the modem responds “OK”, enter

> ATE0

13 When the modem responds “OK”, enter

> AT%K1

Note: This command is not echoed on the screen.

14 When the modem responds “OK”, enter

> ATQ1

Note: The command is not echoed on the screen.

15 Enter:

> AT&W0

Note: The command is not echoed on the screen.

16 Enter:

> AT&Y0

Note: The command is not echoed on the screen.

17 Return to step 4 and try to establish a modem connection again.

18 You have completed this procedure.

Getting ERA values for CM userIDs

Use the following procedure to display the ERA values for CM userIDs.

The show_cm_userid command displays an ERA value for CM userIDs. The information assists the administrator to reset the ERA values for CM userIDs.

Getting ERA values for CM userIDs

At the client workstation

1. Log into the client workstation.
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. Access the bin directory:

   > cd /sdm/bin
5. Get the ERA value for the CM userID:

   ./show_cm_userid <principal_name>

   where

   <principal_name>
   is the CM userID for the CM ERA values to obtain
6. You have completed this procedure.

Getting the ERA value for SDM userID

Purpose

Use this procedure to reset the ERA value for the userID.

Application

Getting the ERA value for the userID

At the client workstation

1 Log into the client workstation.

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 Change to the bin directory:

> cd /sdm/bin

5 Get the ERA value for the userID and password.

> ./show_sdm_userid <principal_name>

where

<principal_name>
is the userID for the ERA value you wish to obtain.

6 You have completed this procedure.

Increasing the size of a logical volume

Purpose

Use this procedure to allocate more disk space to a logical volume.

Application

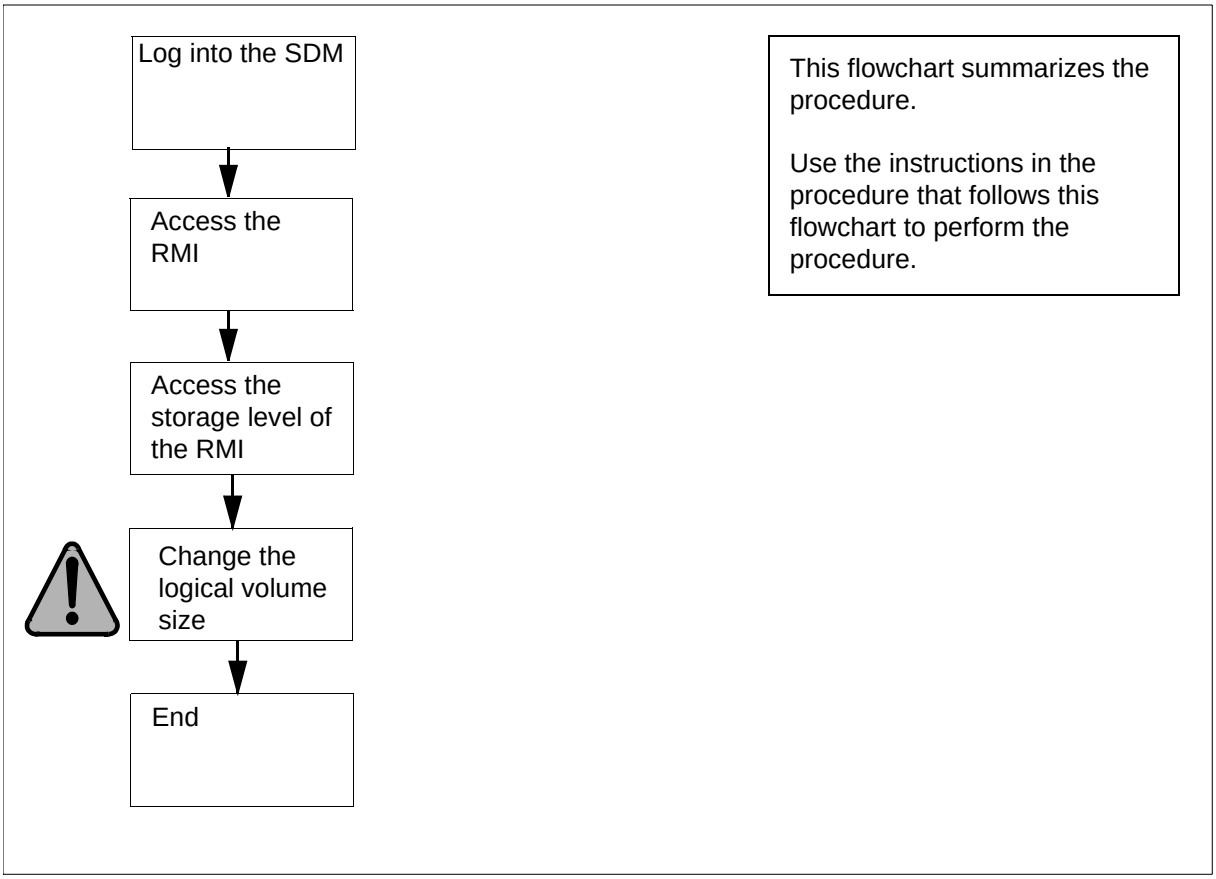
DANGER
Increasing the size of a logical volume can limit future software upgrade capability
SDM logical volumes are pre-engineered to sizes that are adequate for Nortel Networks customers. Do not increase the size of a logical volume unless absolutely necessary.

If you need to change the size of a logical volume, do so only with the assistance of Nortel Networks Technical Assistance and Support. Failure to follow this warning may jeopardize future software upgrade capability.

Action

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

Summary of increasing the size of a logical volume



Increasing the size of a logical volume

At the local VT100 console

1 Log into the SDM as the root user.

2 Access the top menu level of the remote maintenance interface (RMI):

 # sdmmtc

3 Access the system (Sys) menu level of the RMI:

> sys

4 Access the storage menu level of the RMI:

> storage

Example response:

```
Volume Group      Status      Free (MB)
rootvg            mirrored    1932
datavg            mirrored    7760

Logical Volume    Location     Size (MB) %
full/threshold 1 /         rootvg       88
11/ 80
2 /usr           rootvg      600          28/ 90
3 /var           rootvg      200           7/ 70
4 /tmp           rootvg      24            5/ 90
5 /home          rootvg      304          11/ 90
6 /sdm           rootvg      504          23/ 90
7 /data            datavg       208
   6/ 80
                Logical volumes showing: 1 to 7 of 7
```

Note: The example response only shows part of the information displayed at the storage menu level of the RMI.

5 Determine if there is un-allocated disk space that can be used to increase a logical volume.

If there is	Do
enough disk space	step 6
not enough disk space	step 10

6 Identify the logical volume to increase in size. Record the volume name of the logical volume on the left of the System menu of the RMI.

7

ATTENTION
A logical volume on the SDM must never reach 100% full. System behavior cannot be predicted when a logical volume reaches 100% full.

Change the size of the logical volume:

> change lv /<logical_vol> <Mbyte>

where

<logical_vol>
is the name of the logical volume

<Mbyte>
is the size in Mbytes to be added to the logical volume. The size must be less than the amount of un-allocated disk space.

Example input:

> change lv /home 48

Example response:

```
Expanding Volume /home
Expanding Volume /home - Command complete
```

Note: The SDM can round the new size to the nearest 8-, or 16-Mbyte increment.

8 For a 4 Gbyte disk, add 8- or 16-Mbyte multiples. When the logical volume is created, the operating system determines the multiple that has to be used.

9 If the occupancy level of the specified logical volume has exceeded its alarm threshold, contact your system administrator to assess the current condition of the logical volume.

10 You have completed this procedure.

Managing ETA extended registry attributes

ATA and ETA client principal account information is stored on the DCE security server and managed by the DCE admin user. Users can change the CM password that belongs to their principal account.

You can access one MAP/CI session with each CM userID and password. To bypass this limitation, an ATA or ETA client user can access a pool of CM user accounts (userIDs and passwords) to establish multiple MAP/CI sessions.

Depending on the user profile, an ATA or ETA client user may have one SDM userID assigned to a principal account. The SDM userID is used to access one or more SDM sessions.

ATA and ETA clients can share SDM user accounts with each other because the SDM has a limited and restricted list of user accounts, typically root and maint.

The SDM userID, CM userID and CM password information are stored in the extended registry attributes (ERA) of the DCE principal. ERA is administered by the DCE administrator user.

Displaying the CLLI from the command line

Use the following procedure to display the Common Language Location Identifier (CLLI) of the Core from the command line.

Prerequisites

This procedure requires access to the SuperNode Data Manager (SDM) through telnet, Enhanced Terminal Access (ETA) or ASCII Terminal Access (ATA). This procedure does not support access to the SDM through SDMRLOGIN.

Procedure

From any workstation or console

1 Access the SDM.

From the command line

2 Display the CLLI of the Core by typing

```
# clli
```

and pressing the Enter key.

Response

The system displays the CLLI of the core.

Example

```
EAST_CS01
```

3 You have completed this procedure.

Displaying the CLLI from BILLMTC

Use the following procedure to display the Common Language Location Identifier (CLLI) of the Core from the Billing Maintenance (billmtc) interface.

Prerequisites

This procedure requires access to the SuperNode Data Manager (SDM) through telnet, Enhanced Terminal Access (ETA) or ASCII Terminal Access (ATA). This procedure does not support access to the SDM through SDMRLOGIN.

Procedure

From any workstation or console

1 Access the SDM.

2 Access the billing maintenance by typing

```
# billmtc
```

and pressing the Enter key.

Response

The billing maintenance interface opens.

From any level of BILLMTC

3 Display the CLLI of the Core by typing

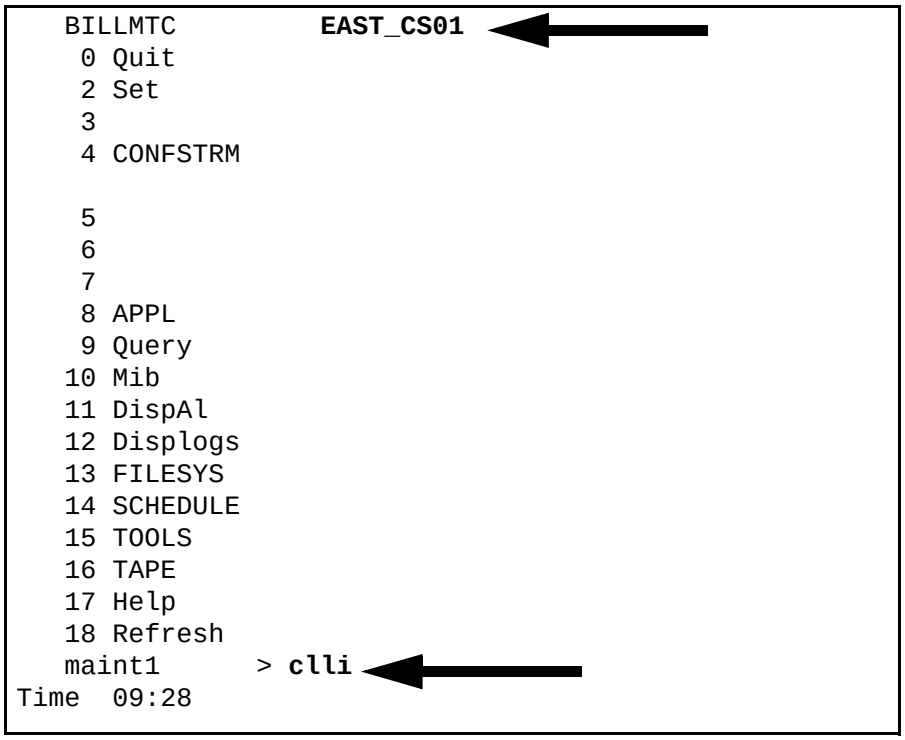
> clli

and pressing the Enter key.

Response

BILLMTC interface displays the CLLI at the top of the screen.

Example



4 You have completed this procedure.

Configuring secure outbound transfer of OMs

Application

Use this procedure configure secure outbound transfer of Operational Measurements (OM).

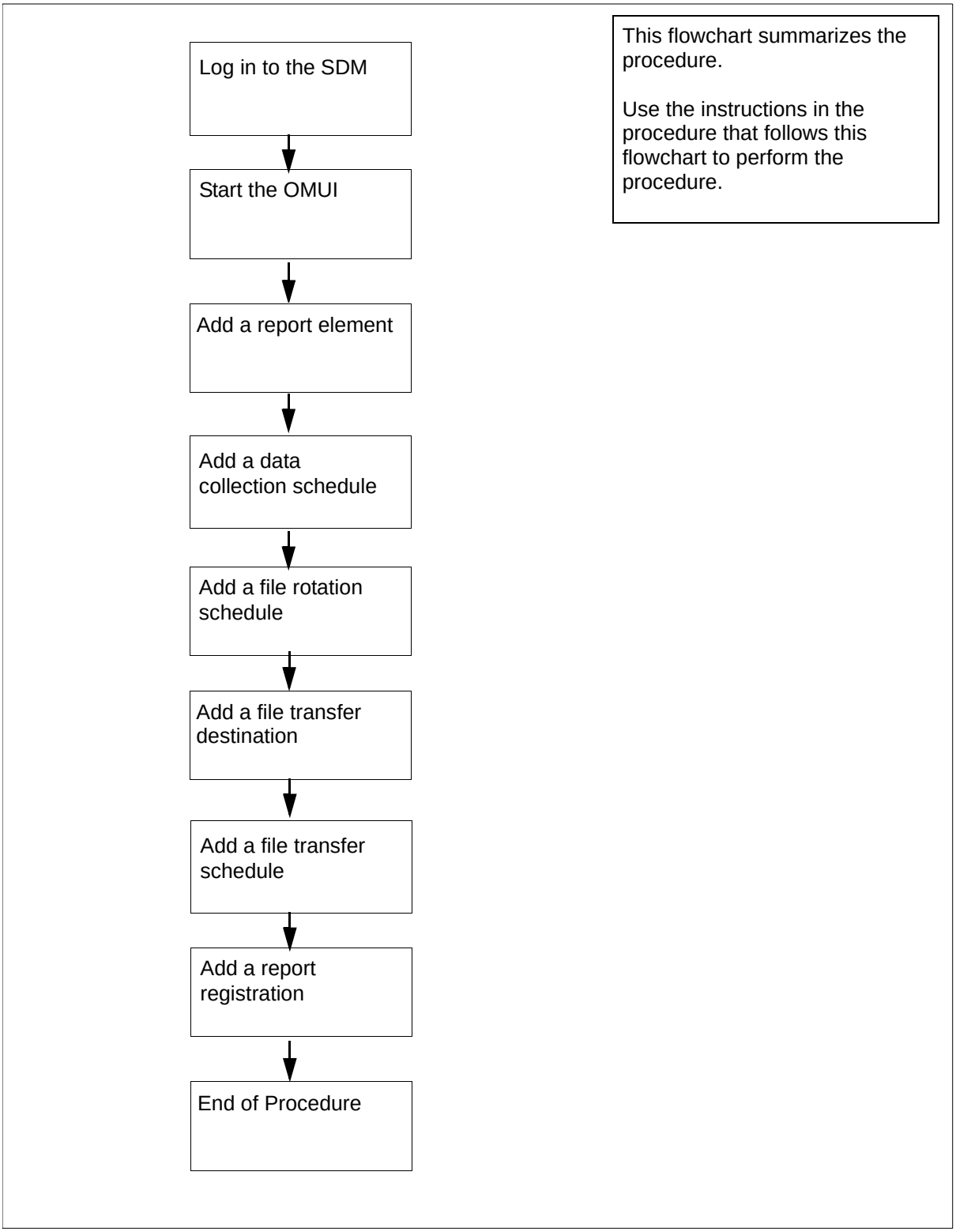
Note: To use secure file transfer, you must install the OpenSSH fileset.

This procedure provides the high level steps. For information on how to use the Operational Measurements User Interface (OMUI) and for details for each step, refer to NN10147-711, SDM Performance Management.

Action

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

Summary of configuring secure outbound transfer of OMs



Configuring secure outbound transfer of OMs

At the workstation UNIX prompt or VT-100 terminal prompt:

1 Log in to the SDM.

2 Start the OMUI.

Refer to Starting the OMUI in NN10147-711, SDM Performance Management.

3 Add a report element.

Refer to Adding a report element in NN10147-711, SDM Performance Management.

4 Add a data collection schedule.

Refer to Adding a data collection schedule in NN10147-711, SDM Performance Management.

5 Add a file rotation schedule.

Refer to Adding a file rotation schedule in NN10147-711, SDM Performance Management.

6 Add a file transfer destination. When prompted, enter the file type by typing

`secure`

and pressing the Enter key.

Note: If you choose standard, the outbound OM CSV files will be transferred using standard unencrypted FTP.

Refer to Adding a file transfer destination in NN10147-711, SDM Performance Management.

7 Using the file transfer destination in step 6, add a file transfer schedule.

Refer to Adding a file transfer schedule in NN10147-711, SDM Performance Management.

8 Using the report registration from step 3, the data collection schedule from step 4, file rotation schedule from step 5, and the file transfer schedule from step 7, add a report registration.

Refer to Adding a report registration in NN10147-711, SDM Performance Management.

9 You have completed this procedure.