# Core and Billing Manager 850 Configuration Management

This NTP contains the procedures used for configuration software applications that run on the core manager.

## What's new in Core and Billing Manager 850 Configuration Management in (I)SN09

### Feature changes

See the following section for information about the feature change.

**Geo OA&M Automatic Backup and Accelerated Restore**
Geo OA&M Automatic Backup and Accelerated Restore allows a standby system to be backed up automatically at regular intervals so that the standby system is ready to provide service if the primary system is unavailable for an extended period of time. Procedures associated with this feature are:

- Initiating a recovery back to the cluster
- Initiating a switch over to the remote backup server
- Installing the remote backup server

### Other changes

There are no other changes in this release.

# Configuring a virtual IP address on an SPFS-based server

## Application

Use this procedure to configure a virtual IP address on a Carrier Voice over IP Server Platform Foundation Software (SPFS)-based server. This procedure applies to simplex and high availability (HA) servers. An HA server refers to a Sun Netra 240 server pair.

## Prerequisites

You need the root user ID and password for the server on which you are configuring the virtual IP address.

## Action

Perform the following steps to complete this procedure.

**ATTENTION**
In a two-server configuration, perform the steps that follow on the Active server.

***At your workstation***

**1** Log in to server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**
is the IP address or host name of the SPFS-based server on which you are configuring the virtual IP address

***Note:*** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

**2** When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

***Note:*** In a two-server configuration, ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

**6** Enter the number that corresponds to the “Configuration” option in the menu.

*Example response*

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)

 X - exit


Select -
```

**7** Enter the number that corresponds to the “IP Configuration” option in the menu.

*Example response*

```
IP Configuration
 1 - config_router (Configure Default Router and
     Netmask)
 2 - config_data (Configure System Data IP
     Addresses)
 3 - ipsecike_config (Configure IPSec/IKE Rules)

 X - exit

select -
```

**8** Enter the number that corresponds to the “config_data” option in the menu.

*Example response*

```
===Executing “config_data”

WARNING: Changing the network settings will
effect all applications! Improper network
configuration will result in loss of service!
Applications may require restart or
reconfiguration after network changes

CAUTION: You are not accessing this tool via the
system console. Changing network configuration
may disrupt this session.

CAUTION: HTTPS Certificate is installed for web
services. Changing the hostname or ip may
require an updated certificate.

hostname:           <hostname>
ip address:           <ip address>

Enter the hostname for this system [hostname]
```

**9** When prompted, enter the hostname for this SPFS-based server, or press the Enter key to accept the default value if one is specified.

*Example response*

```
Enter ip address for <hostname> [00.00.00.00]
```

**10** When prompted, enter the IP address for this SPFS-based server, or press the Enter key to accept the default value if one is specified.

*Example response*

```
Configure additional ip address? [yes]
```

**11** When prompted, indicate whether you want to configure an additional IP address.

| If you enter | Do |
|---|---|
| yes | step 12 |
| no | step 15 |

**12** When prompted, enter the virtual IP address you want to configure on this server, or press the Enter key to accept the default value if one is specified.

*Example response*

```
Enter application for ip address <ip address>
```

**13** When prompted, enter the application name for the additional IP address you just specified, or press the Enter key to accept the default value if one is specified.

***Note 1:*** When configuring a virtual IP address for APS, the application name is APS. When configuring a virtual IP address for IEMS, the application name is IEMS.

***Note 2:*** The system allocates a hostname for each virtual IP address that is configured. The hostname is in the form of <spfs_primary_hostname-application>, for example, “wxe0s00j-iems” when the virtual IP address is set up for IEMS. Hostnames are stored in file” /etc/hosts” on the system.

*Example response*

```
Configure additional ip address? [no]
```

**14** Repeat step 11.

**15** When prompted, confirm the settings by typing

**ok**

and pressing the Enter key.

*Example response on an **HA system***

```
The network changes have been made, however the
cluster requires a restart of both units. The
units must be restarted in the below order.

1) Login as root on the console of the standby
   unit and shut it down with the command:
   “shutdown -i 0 -y”.
2) After the standby unit has shutdown, restart
   the active unit with the command: “shutdown
   -i 6 -y”.
3)After the restart is complete, the new network
  settings are in effect.
4) Boot the standby unit with the command
   “boot”.

===”config_data” completed successfully
```

*Example response on a **simplex system***

```
The network changes have been made, however a
restart is required to use the new network
settings. Reboot to ensure all applications are
restarted. Exit this "cli" tool and reboot using
the Solaris command "shutdown -i 6 -y".

===”config_data” completed successfully
```

**16** Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

| If you have | Do |
|---|---|
| a simplex system | step 17 only |
| an HA system | step 18 |

**17** Reboot the server by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

You have completed this procedure.

***At the console of the Inactive node***

**18** Log in to the inactive node through the console (port A) using the root user ID and password.

> ***Note:*** Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

**19** Shutdown the inactive node by typing

```
# shutdown -i 0 -y
```

and pressing the Enter key.

### *At the console of the active node*

**20** Log in to the active node through the console (port A) using the root user ID and password.

***Note:*** Ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

**21** Restart the active node by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

### *At the console of the Inactive node*

**22** Boot the inactive node by typing

```
# boot
```

and pressing the Enter key.

You have completed this procedure.

# Configuring log delivery destinations

## Purpose

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

## Application

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

- a TCP device (a host IP and port on the network)
- a TCP-IN device (a remote IP and core manager port number)
- a file device (a file on the core manager)

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

- change any aspect of an existing device, including log routing entries, refer to the procedure Modifying a log device using logroute on page 19.
- delete an existing device, refer to the procedure Deleting a device using logroute on page 26.
- modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters on page 81.

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

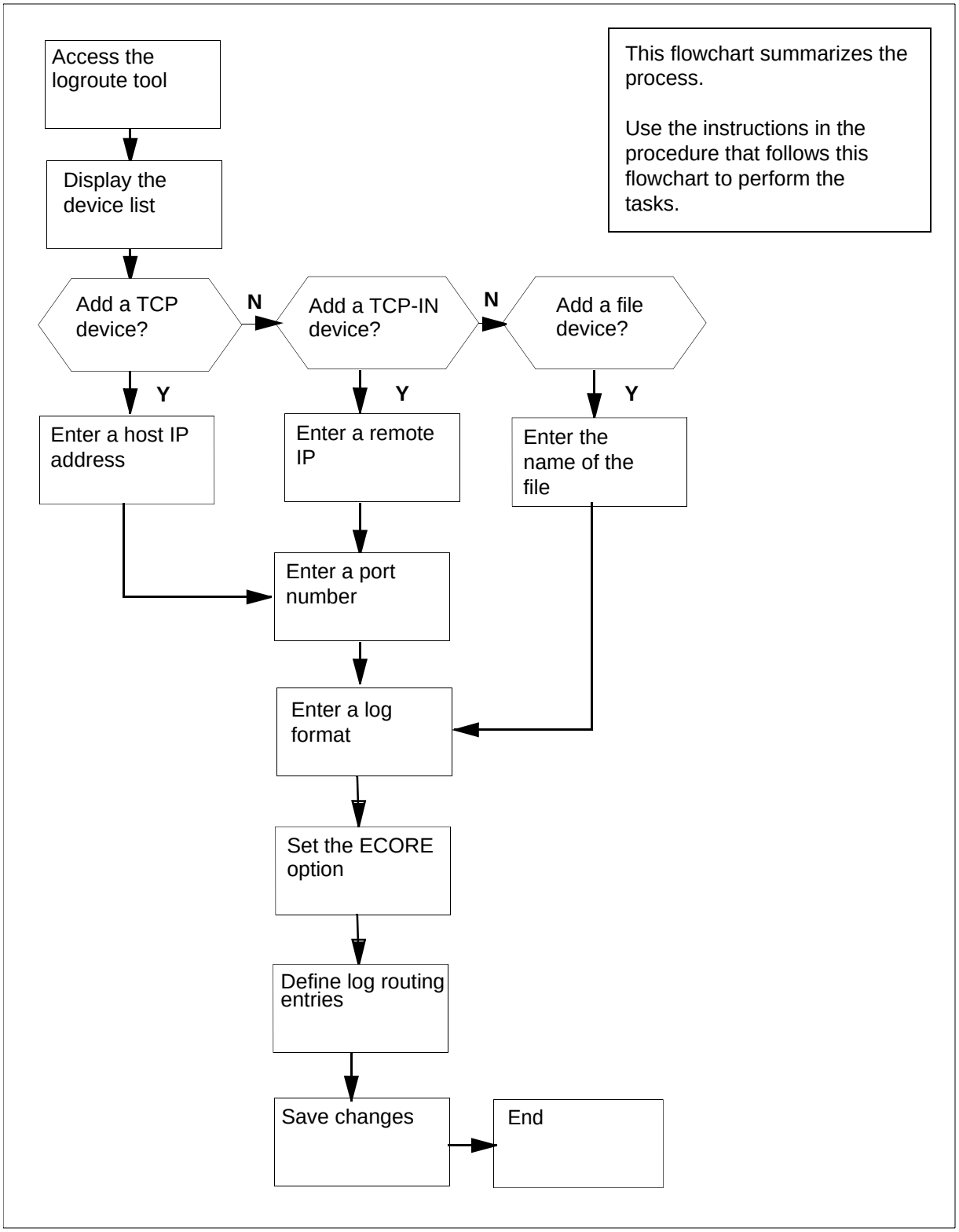
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

## Task flow for Configuring log delivery destinations



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

## Configuring log delivery destinations

### *At any workstation or console*

**1** Log into the core manager. Refer to Prerequisites on page 9 for details.

**2** Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                  Logroute Main Menu


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



Enter Option ==>
```

**3** Display the device list:

**1**

The Device List Menu screen appears.

```
                    Device List Menu


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




 Enter Option ==>
```

**4** Begin to add a new log device:

**2**

The Add Device screen appears.

```
                      Add Device


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




 Enter Option ==>
```

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

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

**6** Start adding a TCP device:

**1**

*Example response:*

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

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




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

**7** Enter a host IP address.

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

Continue with step 14.

**9** Start adding a TCP-IN device:

**2**

*Example response:*

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

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




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

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

**11** When prompted, enter the core manager port number.

Continue with step 14.

**12** Start adding a file device:

**3**

*Example response*

```
                          File
Enter ABORT to return to Previous Screen

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









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

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

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

***Note 1:*** Enter STD or SCC2 if you want the following information to be displayed in all log reports (otherwise, enter STD_OLD or SCC2_OLD):

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

***Note 2:*** The default format is STD.

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

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

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

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

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

*Example response:*

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

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

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

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

***Note 3:*** You can also enter **`all`**, which will suppress or un-suppress all logs routed to this device.

*Example response:*

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

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

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

**y**

The new device will be added to the system.

*Example response:*

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

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

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

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

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

**5**

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

**6**

**20** Quit the logroute tool:

**6**

**21** You have completed this procedure.

# Modifying a log device using logroute

## Purpose

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

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

If you want to modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters on page 81.

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

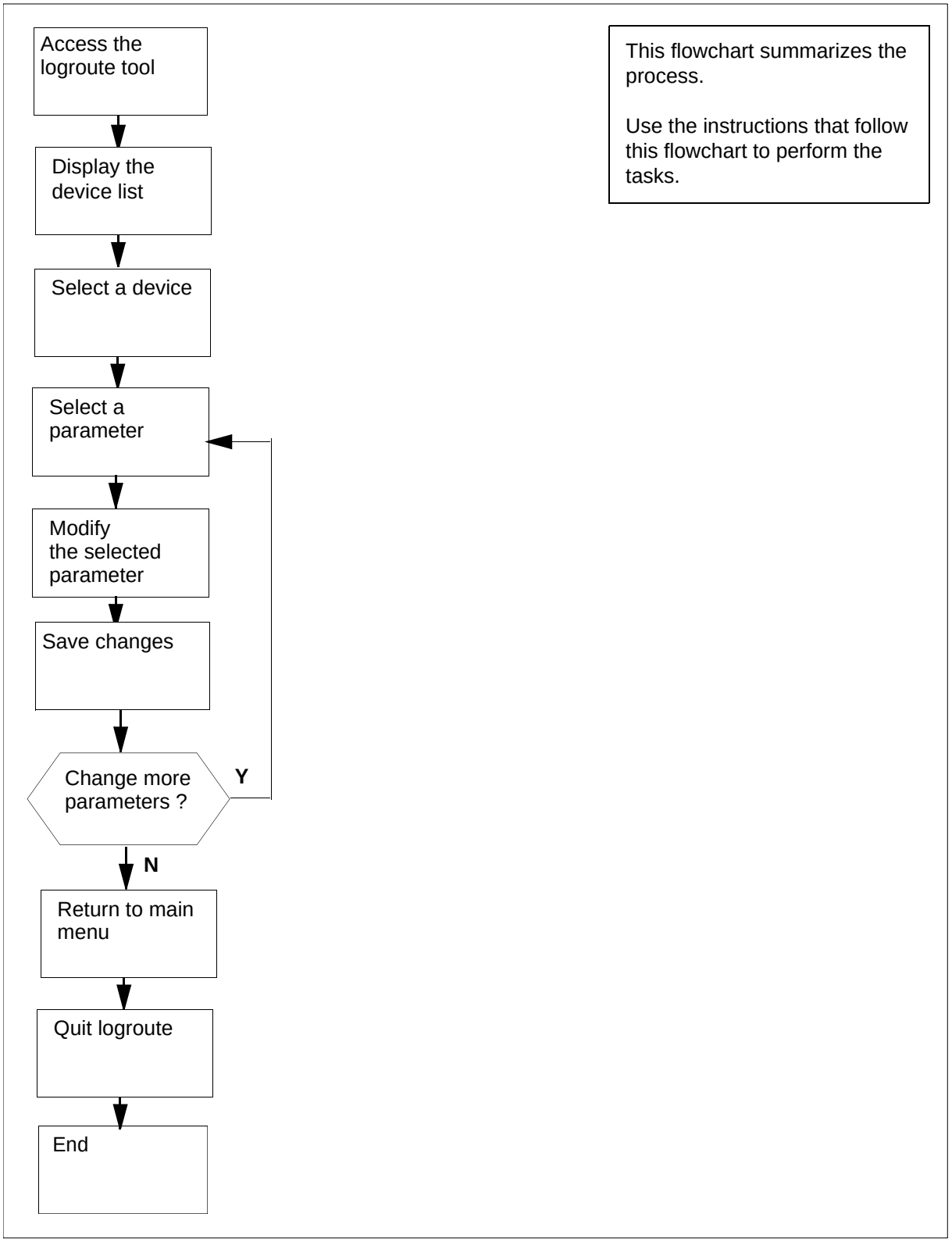
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

## Task flow for Modifying a log device using logroute



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

## Procedure

### Modifying a log device using logroute

#### *At the VT100 console*

**1** Log into the core manager. Refer to Prerequisites on page 19 for details.

**2** Access the logroute tool:

**`logroute`**

The Logroute Main Menu screen appears.

```
                Logroute Main Menu


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




 Enter Option ==>
```

**3** Display the device list:

**1**

The Device List Menu screen appears.

```
                    Device List Menu


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




 Enter Option ==>
```

**4** Access the Modify Device Menu screen:

**4**

The system displays all currently configured devices.

*Example response:*

```
                  Modify Device Menu

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









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

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

The screen for the selected device is displayed.

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

```
                TCP-IN Device

Enter ABORT to return to Modify Device Menu

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



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

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

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

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

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

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

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

Continue with step 16.

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

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

Continue with step 16.

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

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

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

- **a**
  if you want to un-suppress logs (cause them to be routed to the device)
- **d**
  if you want to suppress logs (cause them not to be routed to the device)

  *Response*

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

**12** Enter a log type or a combination of log type and log number (separated by a space). The new entry is added to the log routing list on the screen. For example, an entry of:

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

*Example response:*

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

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

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

*Example response:*

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

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

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

**16** When prompted, save your changes:

**y**

*Example response:*

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

**17** Confirm the save command:

**y**

*Example response:*

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

Press the Enter key to confirm the change.

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

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

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

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

**20** Exit the Modify Device Menu screen:

**abort**

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

**6**

**22** Quit the logroute tool:

**6**

**23** You have completed this procedure.

# Deleting a device using logroute

## Purpose

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

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

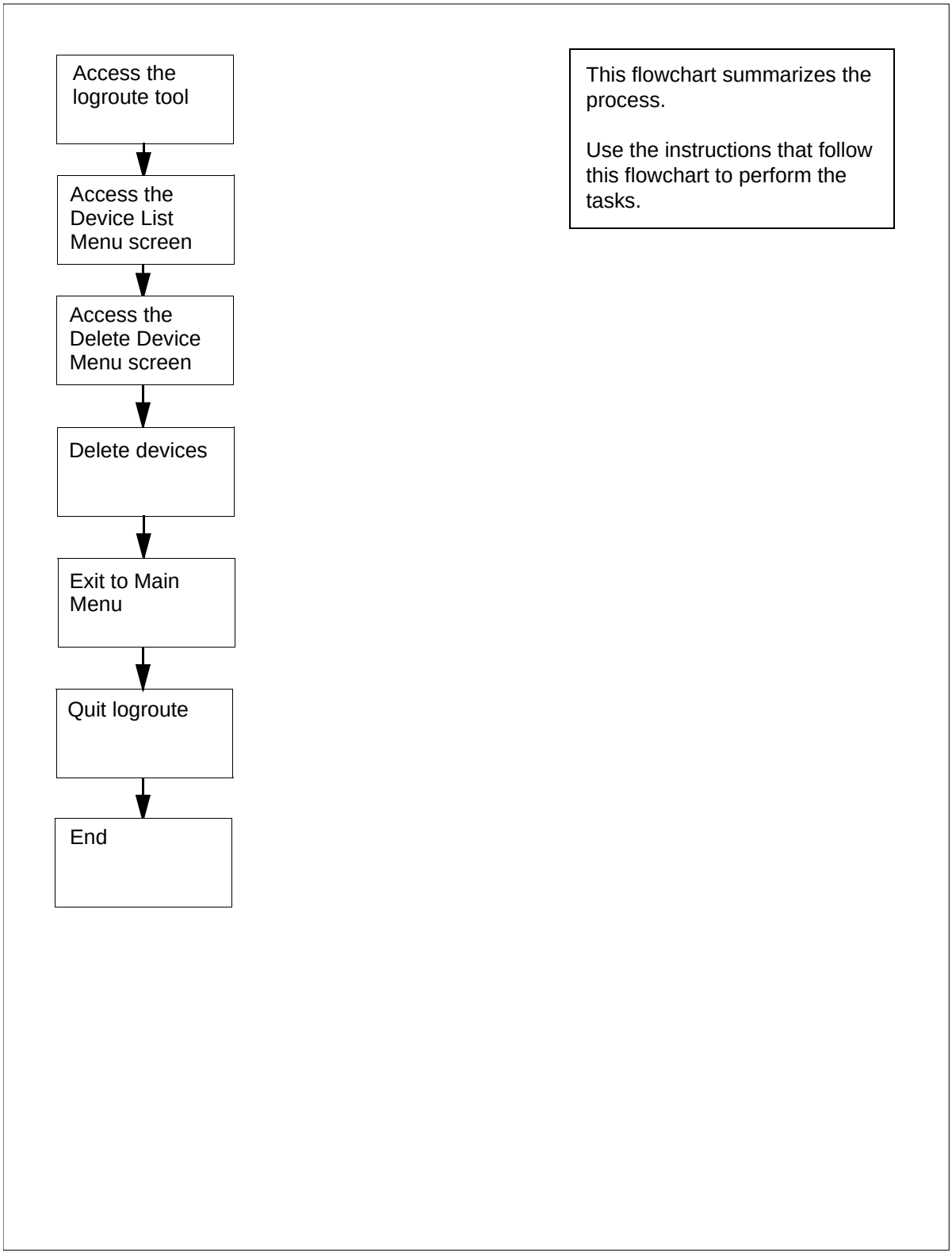
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

## Task flow for Deleting a device using logroute



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

## Procedure

### Deleting a device using logroute

***At the VT100 console***

**1** Log into the core manager. Refer to Prerequisites on page 26 for details.

**2** Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

**3** Display the device list:

```
1
```

The Device List Menu screen appears.

```
                  Device List Menu


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




 Enter Option ==>
```

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

**4** Access the Delete Device Menu screen:

**3**

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

*Example response*:

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




 Enter device number to delete ==>
```

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

*Response*

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

**6** Confirm that you want to delete the selected device:

**y**

*Example response*:

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

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

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

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

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

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

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

**`abort`**

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

**6**

**11** Quit the logroute tool:

**6**

**12** You have completed this procedure.

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

## Purpose

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

### Logging on to the Core and Billing Manager 850

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

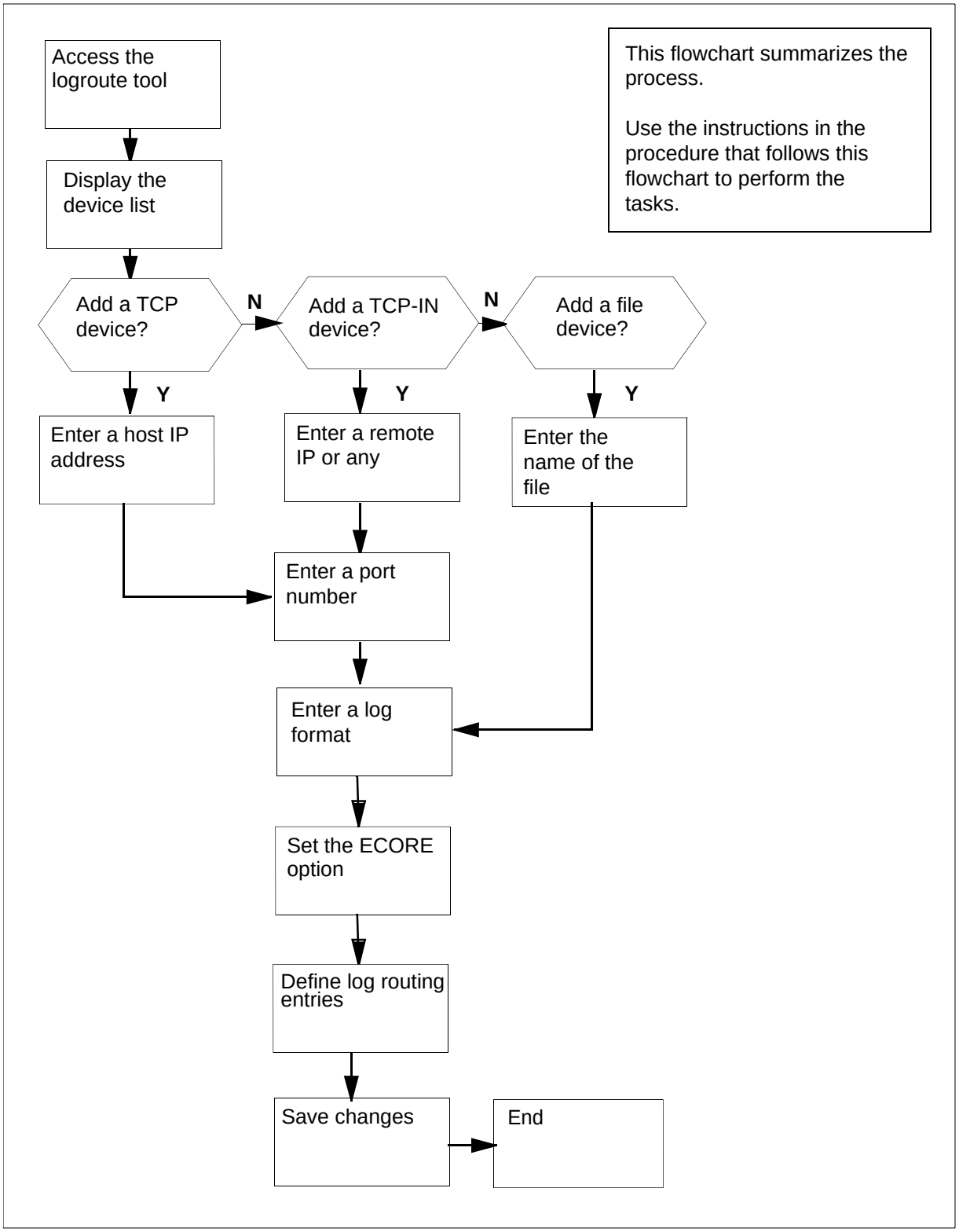
### System requirements

The Nortel Multiservice Switch Log Streamer application should be configured on the core manager to retrieve logs from the MDM. To configure the Nortel Multiservice Switch Log Streamer application on the CS 2000 Core Manager, use the procedure Installing and configuring the log delivery application in NN10104-511, *CS 2000 Core Manager Configuration Management*. To configure the Nortel Multiservice Switch Log Streamer application on the Core and Billing Manager 850, use the procedure Installing optional software on a CBM 850 in *Upgrading the Core and Billing Manager 850*, NN10347-461.

## Task flow diagram

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

## Task flow for Configuring log delivery destinations



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

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

### *At any workstation or console*

1 Log into the core manager. Refer to Prerequisites on page 31 for details.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                Logroute Main Menu

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



Enter Option ==>
```

**3** Enter “1” to display the device list.

The Device List Menu screen appears.

```
                Device List Menu


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




 Enter Option ==>
```

**4** Enter “2” to add a new log device.

The Add Device screen appears.

```
                    Add Device


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




 Enter Option ==>
```

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

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

**6** Enter “1” to add a TCP device.

*Example response:*

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

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




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

**7** Enter a host IP address.

*Example response:*

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

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




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

**8** Enter a port number from the range displayed.

*Example response:*

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

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




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

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

*Example response:*

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

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




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

**10** Set the ECORE option to ON or OFF.

*Example response:*

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

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




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

**11** Enter “a” to add report.

*Example response:*

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

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




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

**12** Enter log identifier as “MDM 601”

*Example response:*

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

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




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

**13** Enter “Y” to add more logrouting details.

*Example response:*

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

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




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

**14** Enter “a” to add report.

*Example response:*

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

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




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

**15** Enter log identifier as “PPEM 601”

*Example response:*

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

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



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

**16** Enter “N” to indicate you don’t want to add more logrouting details.

*Example response:*

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

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



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

**17** Enter “Y” to save device details.

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

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

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

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

**18** Enter “2” to add a TCP_IN device.

*Example response:*

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

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




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

**19** Enter a remote IP address or “a” for any IP address.

*Example response:*

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

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




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

**20** Enter a port number from the range displayed.

*Example response:*

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

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




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

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

*Example response:*

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

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




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

**22** Set the ECORE option to ON or OFF.

*Example response:*

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

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




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

**23** Enter “a” to add report.

*Example response:*

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

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




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

**24** Enter log identifier as “MDM 601”.

*Example response:*

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

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




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

**25** Enter “Y” to add more logrouting details.

*Example response:*

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

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




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

**26** Enter “a” to add report.

*Example response:*

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

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




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

**27** Enter log identifier as “PPEM 601”.

*Example response:*

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

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



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

**28** Enter “N” to indicate you don’t want to add more logrouting details.

*Example response:*

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

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



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

**29** Enter “Y” to save device details.

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

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

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

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

**30** Enter “3” to add file device.

*Example response:*

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

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




Enter file name ==>
```

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

*Example response:*

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

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




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

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

*Example response:*

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

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




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

**33** Set the ECORE option to ON or OFF.

*Example response:*

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

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









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

**34** Enter “a” to add report.

*Example response:*

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

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









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

**35** Enter log identifier as “MDM 601”.

*Example response:*

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

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




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

**36** Enter “Y” to add more logrouting details.

*Example response:*

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

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




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

**37** Enter “a” to add report.

*Example response:*

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

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




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

**38** Enter log identifier as “PPEM 601”.

*Example response:*

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

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




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

**39** Enter “N” to indicate you don’t want to add more logrouting details.

*Example response:*

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

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




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

**40** Enter “Y” to save device details.

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

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

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

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

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

`enter` **5**

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

`enter` **6**

**43** Quit the logroute tool:

`enter` **6**

**44** You have completed this procedure.

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

## Purpose

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

### Logging on to the Core and Billing Manager 850

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

### System requirements

The Nortel Multiservice Switch Log Streamer application should be configured on the core manager to retrieve logs from the MDM. To configure the Nortel Multiservice Switch Log Streamer application on the CS 2000 Core Manager, use the procedure Installing and configuring the log delivery application in NN10104-511, *CS 2000 Core Manager Configuration Management*. To configure the Nortel Multiservice Switch Log Streamer application on the Core and Billing Manager 850, use the procedure Installing optional software on a CBM 850 in *Upgrading the Core and Billing Manager 850*, NN10347-461.

## Procedure

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

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

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

***At the VT100 console***

1 Log into the core manager. Refer to Prerequisites on page 54 for details.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                Logroute Main Menu

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



Enter Option ==>
```

**3** Enter “1” to display the device list.

The Device List Menu screen appears.

```
                    Device List Menu


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




 Enter Option ==>
```

**4** Enter “1” to view the configured devices.

The Device List screen appears.

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

```
                    Device List Screen


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









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

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

*Example response*

```
                    TCP Device


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



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

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

| If the device | |
|---|---|
| is configured for ALL logs | step 23 |
| is configured for “MDM 601” and “PEM 601” logs | step 7 |

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

The Device List Menu screen appears.

```
                    Device List Menu

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



  Enter Option ==>
```

**8** Enter “4” to modify a device.

The Device List screen appears.

```
                    Device List Screen

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









  Enter device number to delete ==>
```

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

*Example response*

```
                    TCP Device

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



 Enter number of device parameter to change:
```

**10** Enter “5” to change the Log Routing device parameter.

*Example response*:

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









  Enter “a” to add report or “d” to delete report ==>
```

**11** Enter “d” to delete a report.

*Example response*:

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









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

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

*Example response*:

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

          1 - ADDREP PPEM 601









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

**13** Enter “Y” to indicate that you want to delete another Logrouting detail.

*Example response*:

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









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

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

*Example response*:

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









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

**15** Enter “N” to indicate that you don’t want to delete more Logrouting details.

**16** Enter “Y” to save the Logrouting details changes you have made.

*Example response*:

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









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

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

*Example response*:

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









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

**18** Press Enter to continue.

*Example response*

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

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




Enter number of device parameter to change:
```

**19** Enter “abort” to return to the Modify Device Menu.

*Example response*:

```
                  Modify Device Menu

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









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

**20** Enter “abort” to return to the Device List Menu.

The Device List Menu screen appears.

```
                  Device List Menu

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



 Enter Option ==>
```

**21** Enter “6” to return to the Logroute main menu screen.

The Logroute Main Menu screen appears.

```
                  Logroute Main Menu

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



 Enter Option ==>
```

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

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

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

The Device List Menu screen appears.

```
                  Device List Menu

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



 Enter Option ==>
```

**24** Enter “4” to modify a device.

The Device List screen appears.

```
                Device List Screen

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









Enter device number to delete ==>
```

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

*Example response*

```
                    TCP-IN Device

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




Enter number of device parameter to change:
```

**26** Enter “5” to change the Log Routing device parameter.

*Example response*:

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









 Enter “a” to add report or “d” to delete report ==>
```

**27** Enter “a” to add report.

*Example response*:

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









 Enter “a” to add report or “d” to delete report ==>
```

**28** Enter “d” to delete report.

*Example response*:

```
                  Logrouting of File
Enter ABORT to return to previous screen
Logrouting
          1 - ADDREP ALL









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

**29** Enter the log identifier, “MDM 601”.

*Example response*:

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









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

**30** Enter “Y” .

*Example response*:

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









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

**31** Enter “d” to delete report.

*Example response*:

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









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

**32** Enter the log identifier, “PPEM 601”.

*Example response*:

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




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

**33** Enter “N” to indicate that you don’t want to enter more Logrouting details.

**34** Enter “Y” to save the Logrouting details changes you have made.

*Example response*:

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









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

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

*Example response*:

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









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

**36** Press Enter to continue.

*Example response*

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

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




Enter number of device parameter to change:
```

**37** Enter “abort” to return to the Modify Device Menu.

*Example response*:

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









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

**38** Enter “abort” to return to the Device List Menu.

The Device List Menu screen appears.

```
                  Device List Menu


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




 Enter Option ==>
```

**39** Enter “6” to return to the Logroute main menu screen.

The Logroute Main Menu screen appears.

```
                  Logroute Main Menu


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




Enter Option ==>
```

**40** Enter “6” to exit from the Logroute tool.

**41** You have completed this procedure.

# Specifying the logs delivered from the CM to the core manager

## Purpose

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

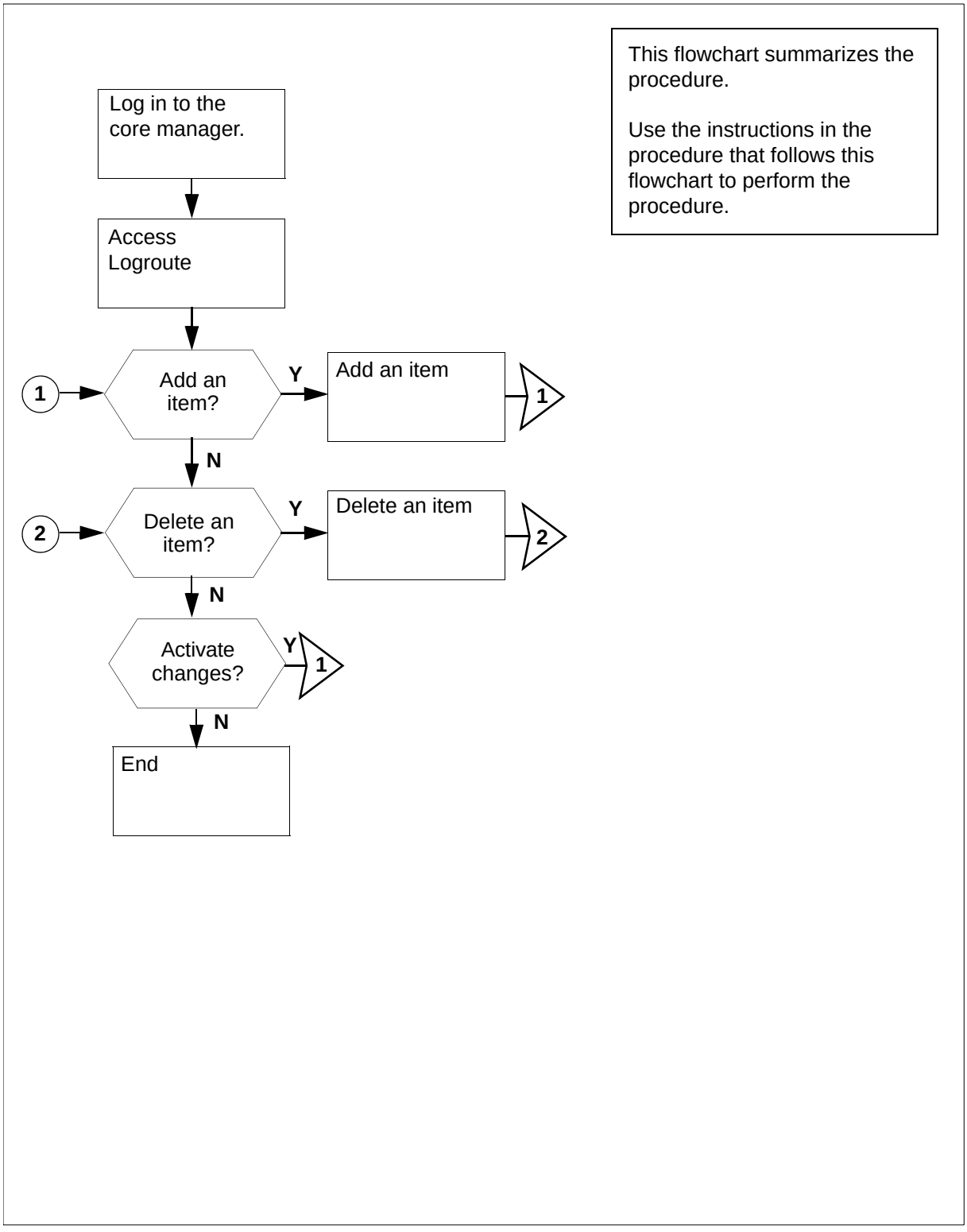
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

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



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

## Procedure

### Specifying the logs delivered from the CM to the core manager

***At the VT100 console***

**1** Log into the core manager. Refer to Prerequisites on page 74 for details.

**2** Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen is displayed.

```
                  Logroute Main Menu


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




 Enter Option ==>
```

**3** Access the CM Configuration File menu:

**3**

The CM Config File Menu screen is displayed.

```
                    CM Config File Menu


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




  Select Option ==>
```

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

**4** Access the CM - Add Report screen:

**2**

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

*Example response: response*

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

           1 - DEL IOAUD 107









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

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

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

*Response*

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

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

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

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

*Example response:*

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

**6** Save your changes:

**y**

The new item is added to the list.

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

**7** Access the CM - Delete Report screen:

**3**

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

*Example response:*

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

           1 - DEL IOAUD 107
           2 - ADD PM 181









     Select report to delete ==>
```

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

*Example response:*

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

**9** Confirm the delete command:

**y**

*Example response:*

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

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

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

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

**abort**

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

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

**5**

**12** Quit the logroute tool:

**6**

**13** You have completed this procedure.

# Configuring Log Delivery global parameters

## Purpose

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

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

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

- Configuring log delivery destinations on page 9
- Modifying a log device using logroute on page 19

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

- log_office_id (office name)

  ***Note:*** This parameter is valid only for devices that have log format set to STD or SCC2.

- buffer size (number of logs)
- reconnect time-out value (seconds)
- lost logs threshold (number of lost logs before the system generates a design log)

  ***Note:*** This parameter is for Nortel personnel only.

- incoming end of line character (ASCII code)
- outgoing end of line characters (ASCII code)
- start of log characters (ASCII code)
- end of logs characters (ASCII code)
- the number of days to keep log files

- maximum size of a log file (Mbyte)
- maximum size action

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

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

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

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

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

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

  — CORE-COMPAT, the core's LOG_OFFICE_ID defined in table OFCVAR will be used for all logs. Until the first log arrives from the core, the system CLLI is used.
- buffer size (number of logs): range is 50 to 300, default is 150
- reconnect time-out value (secs): range is 1 to 3600, default is 15
- lost logs threshold: range is 1 to 300, default is 100 (-1 turns this option off)
- number of days to keep log files: range is 1 to 45, default is 5
- maximum size of a log file (Mbytes): range is 5 to 300, default is 40
- maximum size action: values are STOPDEV, CIRCULATE, and ROTATE

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

  The ROTATE value tells the file device to save the data in separate files every 12 hours. When the file created at each 12-hour rotation is full, the system creates another file to continue saving any log

data. The system does not wait until the next 12-hour rotation to create a new file.

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

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

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

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

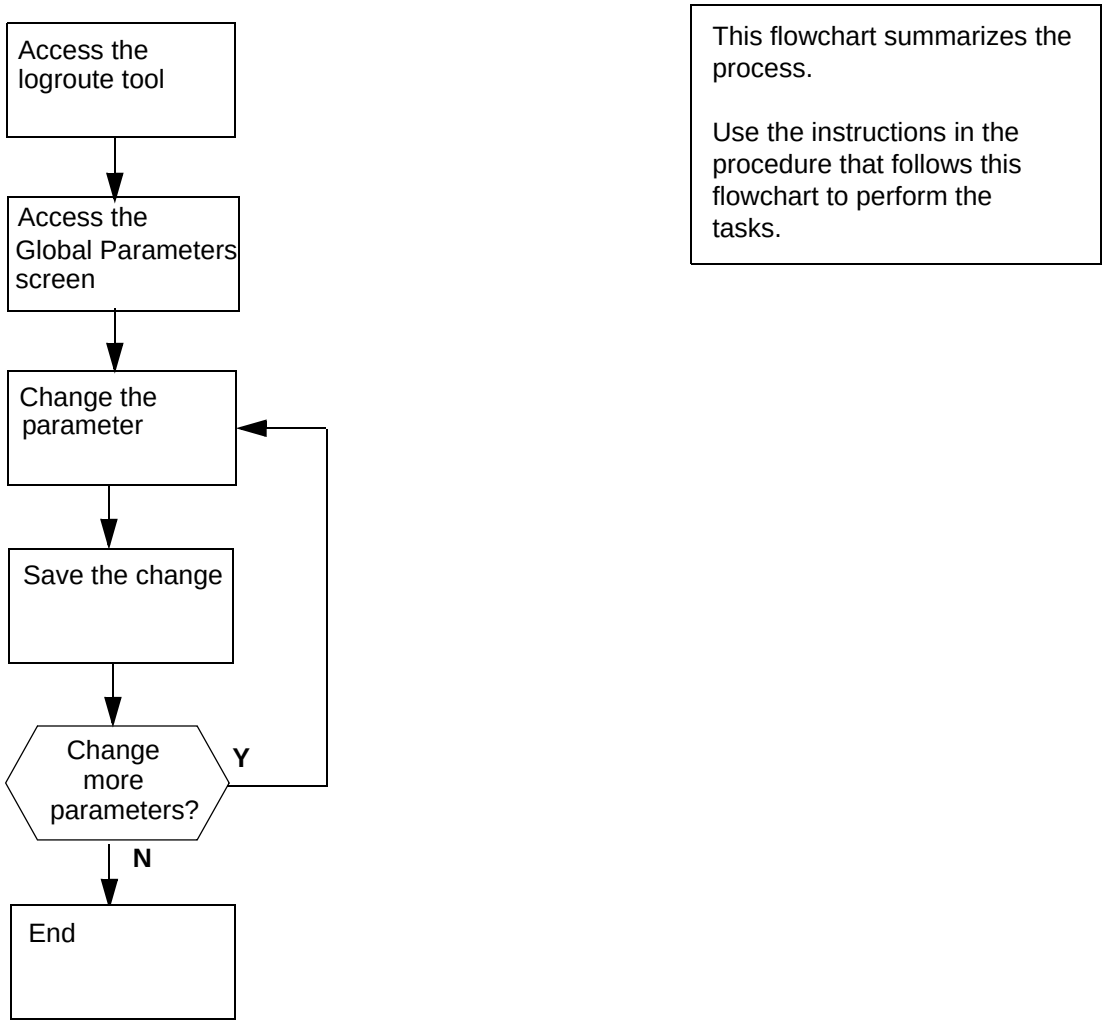
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

### Task flow for Configuring Log Delivery global parameters




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

## Procedure

### Configuring Log Delivery global parameters

***At the VT100 console***

**1** Log into the core manager. Refer to Prerequisites on page 83 for details

**2** Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

**3** Access the Global Parameters screen:

**2**

*Example response*:

```
          Global Parameters

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


Enter Option ==>
```

***Note:*** This display shows the default values for the Global Parameters menu.

**4** Select the parameter that you want to change:

***<n>***

*where*

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

*Example response for changing the buffer size:*

```
                    Global Parameters

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


Enter buffer size (range - 50 to 300) ==>
```

***Note 1:*** The log and line delimiters (incoming and outgoing end of line characters, and start and end of log characters) must be entered as decimal or hexadecimal ASCII code.

***Note 2:*** For a detailed description of each parameter, see the Help menu (option 12).

**5** Enter a new value for the selected parameter.

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

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

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

**7** The system displays the following warning:

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

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

**8** Enter **n**.

The unchanged value appears on the Global Parameter screen.

Continue with step 11.

**9** Enter **y**.

The system displays the following message:

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

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

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

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

**13**

**12** Quit the logroute tool:

**6**

**13** You have completed this procedure.

# Configuring the GDD parameter using logroute

## Purpose

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

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

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

***Note 2:*** When the configured number of days is reached (maximum 30 days), the logs are rotated, and the oldest log file is replaced by the newest.

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

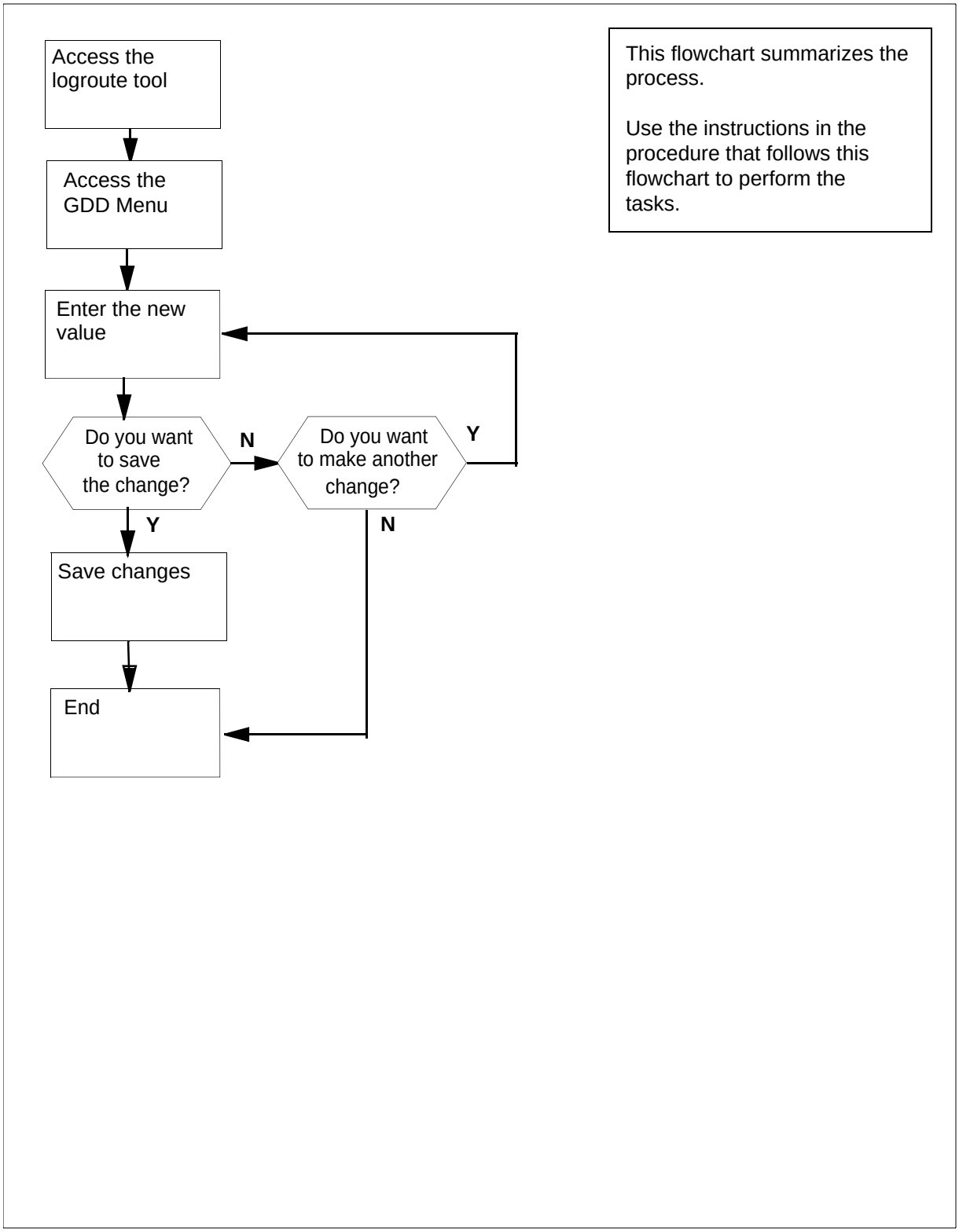
### Logging on to the Core and Billing Manager

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

## Task flow diagram

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

## Task flow for Configuring GDD parameter using logroute



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

### Configuring GDD parameter using logroute

#### *At the VT100 console*

1 Log into the core manager. Refer to Prerequisites on page 88 for details.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                  Logroute Main Menu


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



 Enter Option ==>
```

**3** Access the GDD Menu:

**4**

*Example response:*:

```
                        GDD Menu

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









 Enter Option ==>
```

**4** Select the GDD parameter:

**1**

*Example response:*

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

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

*Example response:*

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

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

**6** Cancel your change:

**n**

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

**7** Save the GDD value:

**y**

*Example response::*

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

**8** Press the Enter key to confirm the change.

*Example response:*

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

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

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

**3**

**11** Quit the logroute tool:

**6**

**12** You have completed this procedure.

# Configuring outbound connection security for OMDD

## Purpose

Secure outbound file transfer of OMs is provided through the OpenSSH SFTP (secure file transfer protocol) client. The SFTP client protects all data, including sensitive users' passwords, by encrypting the data before it leaves the core manager and decrypting the data after it arrives at the downstream OSS destination. The SFTP client also provides data integrity checking to ensure that the data has not been tampered with during the transfer.

## Prerequisites

The following prerequisites apply to the outbound connection security feature:

- An SSH sftp server (SFTP server subsystem) that is compatible with the OpenSSH sftp client must be running on the downstream Operations Support System (OSS) in order for the OMDD to transfer data with the OpenSSH sftp client.
- OpenSSH software, version 3.7.1p2 or later, and any dependent software must be installed on the core manager in order for SFTPW (Secure File Transfer Protocol wrapper) protocol for outbound file transfer to be used. There is no explicit check performed by the OMDD software to determine whether this package or fileset is installed when the SFTPW is being configured. Thus, if the OMDD SFTPW application fails to find the sftp program, an SFTPW alarm is raised and the application terminates any transfer event it is attempting to perform.
- For the CBM, this secure outbound transfer capability depends on the OpenSSH packages as well as NTutil.
- For the SDM and CS 2000 Core Manager, the secure outbound transfer capability depends on the SDM_OpenSSH.base fileset, which must be installed manually, and the SDM_BASE.util fileset.
- The initial host key acceptance of the downstream processor should be performed manually in order for the SFTPW to be used for file transfer from the core manager. The .ssh/known_hosts file in the maint home directory is edited by SSH software to include the host key. After this is completed, sftp can be used to send files to the downstream OSS. This step must be performed for each downstream destination prior to schedule tuple configuration for SFTPW.

### Limitations and restrictions

The following limitations and restrictions apply to the secure outbound file transfer capability:

- Secure outbound file transfer (SFTPW) cannot re-send ClosedSent files when ClosedSent files already exist on the target directory in the downstream system. Therefore, it is important that existing ClosedSent (or processed) files at the downstream system be either moved to another directory or re-named before an attempt is made to re-send ClosedSent files from the core manager to the downstream system.

## Procedure

To configure secure data transfer to a downstream OSS destination, it is necessary to first accept the known host key for the downstream OSS destination. Steps 1 through 10 of this procedure enable you to perform this task. This task must be performed whenever the destination downstream OSS is rebooted or whenever the SFTPD server on the OSS is restarted.

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

### Configuring outbound connection security for OMDD

***At the PC or UNIX workstation***

**1** Establish a telnet connection to the core manager by completing the following substeps.

**a** Open a terminal window that is VT100 compatible.

**b** Log onto the core manager from the terminal window prompt:

```
telnet <ip_address>
```

*where*:

**<ip_address>**
is the IP address of the core manager

**c** When prompted, enter the login ID and password for the root user.

**2** Change directory to the maint home directory:

```
cd ~maint
```

**3** Look in the maint directory for the ".ssh" directory:

```
ls -lad .ssh
```

| If | Do |
|---|---|
| the .ssh file does not exist | step 4 |
| the .ssh file does exist | step 10 |

**4** Create the .ssh directory:

```
mkdir .ssh
```

**5** Change the .ssh directory ownership:

```
chown maint:maint .ssh
```

**6** Change the permissions associated with the .ssh directory:

```
chmod u+rwx .ssh
```

**7** Change to the maint user:

```
su maint
```

**8** Run the ssh client to the downstream OSS destination by providing a "maint" user name and IP address for the ssh client, by performing the following steps:

**a** Type

```
ssh -l maint <nn.nn.nn.nn>
```

*where*

<nn.nn.nn.nn> is the IP address of the ssh client

*Example of response*

The authenticity of host '10.10.10.10' can't be established.

RSA key fingerprint is 3a:d5:d7:6e:ee:6b:45:fc:b9:0b:92:a7:1c:d8:f1:be.

Are you sure you want to continue connecting (yes/no)?

**b** Type

```
yes
```

*Example of response*

Warning: Permanently added '10.10.10.10' (RSA) to the list of known hosts.

**9** Press ctrl + C to terminate the program.

**10** Exit the telnet session:

```
exit
```

**11** You have completed this procedure.

## Troubleshooting

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

- Connection refused

  This error causes a “Down” status for the SSH Collector Status parameter.

  **Example**
  Error : ssh; connect to host <hostname/hostip> port 22: Connection refused
  Connection closed.

  To resolve this problem:

  — Verify that the host machine is on the network.

  — Verify that the SSH server on the host machine is running and that the configuration is correct (such as, the port number and fingerprint).

- SSH not found

  This error is caused by the ssh not being installed on the core manager.

  **Example**
  Error: /bin/ksh: ssh: not found.

  To resolve this problem:

  — Verify that the OpenSSH package is installed on the system.

  ***Note:*** If your core manager is an AIX-based SDM or CS 2000 Core Manager, you can verify whether the OpenSSH package

is installed by checking for the package at the SWIM level of the sdmmtc user interface.

If the package is not installed, contact your Nortel service representative for assistance in installing the OpenSSH package provided by Nortel.

***Note:*** You should not install the OpenSSH package downloaded from the web unless you are instructed to do so by your Nortel service representative.

- known_hosts file cannot be datafilled

  This error is caused by the non-existence of, or incorrect permissions for, the /home/maint/.ssh (AIX-based SDM) or /cbmdata/users/maint/.ssh (CBM) directory.

  To resolve this problem:

  — Verify that you are logged in as the root user and that you switched user (su) to the maint user.

  — Verify that the directory /home/maint/.ssh (AIX-based SDM) or /cbmdata/users/maint/.ssh (CBM) is present and has read/write permissions set for the maint user. If the directory doesn't exist, create it.

  — Verify that the correct IP address is used for host key acceptance.

- SSH server's host key has changed

  If the server's host key has changed, the client will notify you that the connection cannot proceed until the server's host key is deleted from the known_hosts file using a text editor. Before performing this task, you must contact the system administrator of the SSH server to ensure that the server operation will not be compromised.

  To resolve this problem:

  — Try to create an ssh connection to a different machine. If you receive an error message about a changed or incorrect public key, it is probably due to the host changing its public key. Edit the

file /home/maint/.ssh/known_hosts using a text editor and delete any line containing the name of that host.

— Try to create an ssh connection to that host again and then accept a new public key for the host.

- SSH warns about “man-in-the-middle attack”

  This problem is caused either by someone eavesdropping on your connection or by the host key having been changed.

  To resolve this problem:

  — Contact your system administrator to determine whether the host key has been changed or whether the ip address of the client has been changed.

  — Edit the file /home/maint/.ssh/known_hosts using a text editor and delete any line containing the name of that host.

  — Datafill the known_host keys with new information.

# Configuring core access for SBRM through the CBM 850

## Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

***Note 1:*** Perform the procedure, Creating the backup user ID on the core for SBRM on page 102 before you perform this procedure for the first time.

***Note 2:*** This procedure should be performed whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

## Procedure

### Configuring core access for SBRM

***At your workstation***

1 Log into the Core and Billing Manager 850 (CBM 850).

2 Change to the root user:

```
su - root
```

3 When prompted, enter the root password.

4 Change directory to the directory containing appropriate configuration script:

```
cd /opt/nortel/bkresmgr/cbm/scripts
```

5 Run the configuration script:

```
./bkmgr_config.sh
```

6 As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, Creating the backup user ID on the core for SBRM on page 102

7 As the script continues to run, you are then prompted for the user you entered (in step 6). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, Creating the backup user ID on the core for SBRM on page 102

8 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.

9 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.

10 You have completed this procedure.

# Creating the backup user ID on the core for SBRM

## Purpose

This procedure enables you to create the user ID on the core to enable the operation of the Synchronous Backup Restore Manager (SBRM). The types of operations that can be performed by this user are:

- set dump_restore_in_progress field in ofcstd table
- start image dump
- ability to run itocci command set
- ability to perform diskut commands

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

***Note 2:*** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or $, displayed by the system through a GUI or on a command line.

## Procedure

### Creating the backup user ID on the core for SBRM

***At the CI prompt on the core***

1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000
english all
```

where

**<backupuser>**
is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

**<backupuser_pswd>**
is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

**4**
is the priority

**10000**
is the stack size

**english**
the language setting

**all**
is the privilege setting

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

***Note 2:*** If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log into the core manually with this user first. The core will prompt you to change the password at the first login after the login is permitted. Change the password and then perform the procedure, “Configuring core access for SBRM” using the <backupuser> user you have created and the changed password.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in “Configuring core access for SBRM” to ensure that the password for the <backupuser> user

**2** You have completed this procedure.

# Commissioning or decommissioning Network Time Protocol (NTP)

## Purpose

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

***Note:*** After CBM 850 HA system installation, if no external NTP server is configured the ntp level of cbmmtc will display an NTP peer server, which is the unit mate. This is for cluster internal synchronization purposes only. During this time, the overall NTP state is “unequipped” (-) and NTP info is “No NTP servers or peers defined.” After the external NTP server is added, the NTP info will change, and the NTP state will change from (-) to (.), to reflect the presence of an external source.

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

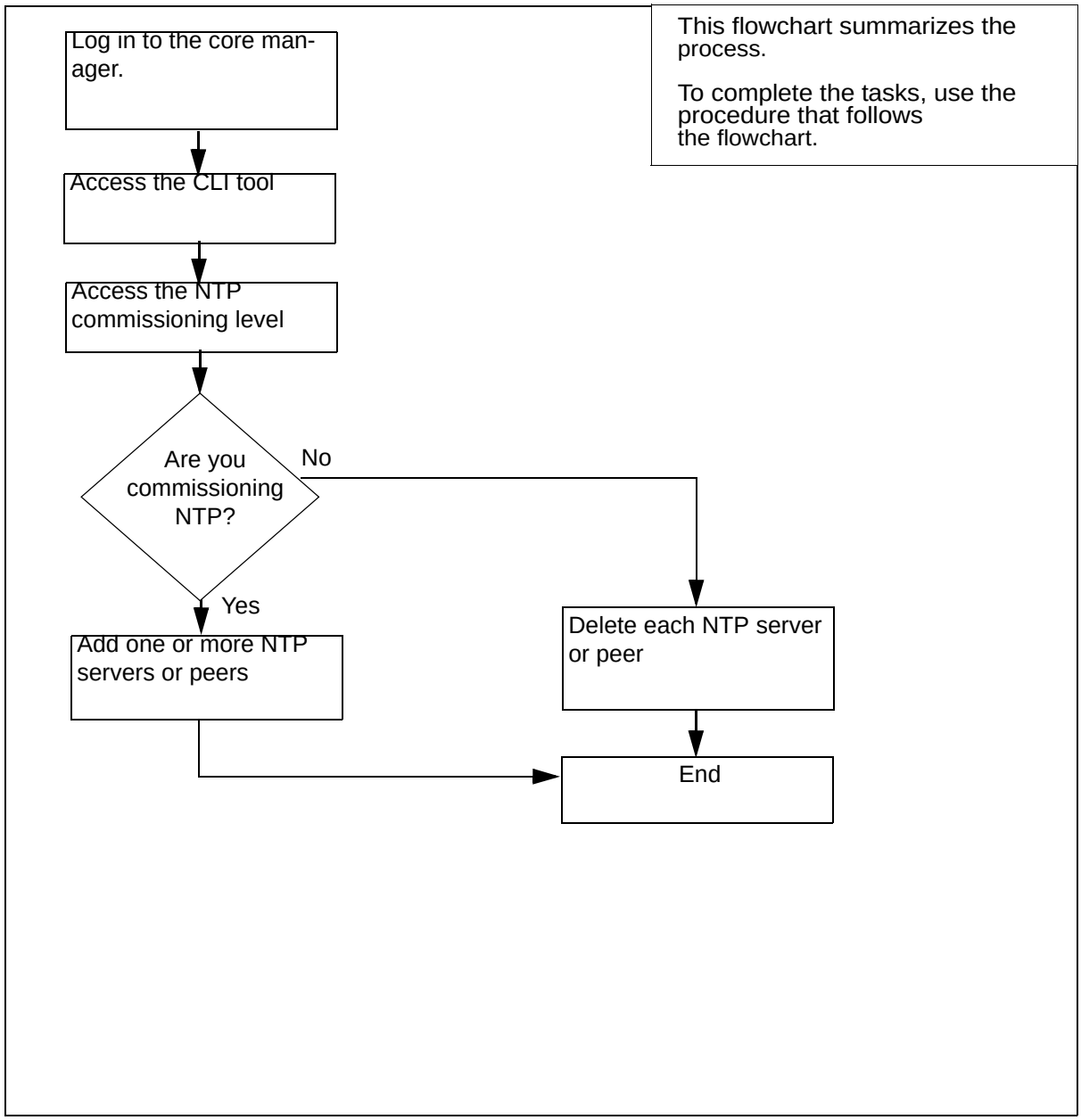
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

## Task flow for Commissioning or decommissioning NTP



## Procedure

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

### Commissioning or decommissioning NTP

#### *At the local VT100 console*

1 Log into the core manager as the root user.

2 Access the CLI tool:

```
cli
```

3 Access the CLI configuration level:

**<#>**

*where*

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

4 Access the NTP configuration level:

**<#>**

*where*

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

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

5 Add an NTP server or peer:

**<#>**

*where*

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

6 Enter the IP address of the server or peer.

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

***Note 2:*** You can add a maximum of three NTP servers or peers. If you attempt to add more than three, then the system

will only recognize the three most recent NTP servers or peers.

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

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

**8** Remove all NTP servers

**<#>**

*where*

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

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

**10** Remove only selected NTP servers or peers

**<#>**

*where*

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

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

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

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

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

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

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

15 Access the RMI level to see the response.

```
# cbmmtc ntp
```

16 You have completed this procedure.

# Adding or removing an NTP server or peer

## Purpose

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

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

***Note 2:*** If you have Distributed Computing Environment (DCE) installed on your system and are deleting the last NTP server or peer, you will be prompted to set up the DCE's DTS. For this, you will need a DCE administrator password.

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

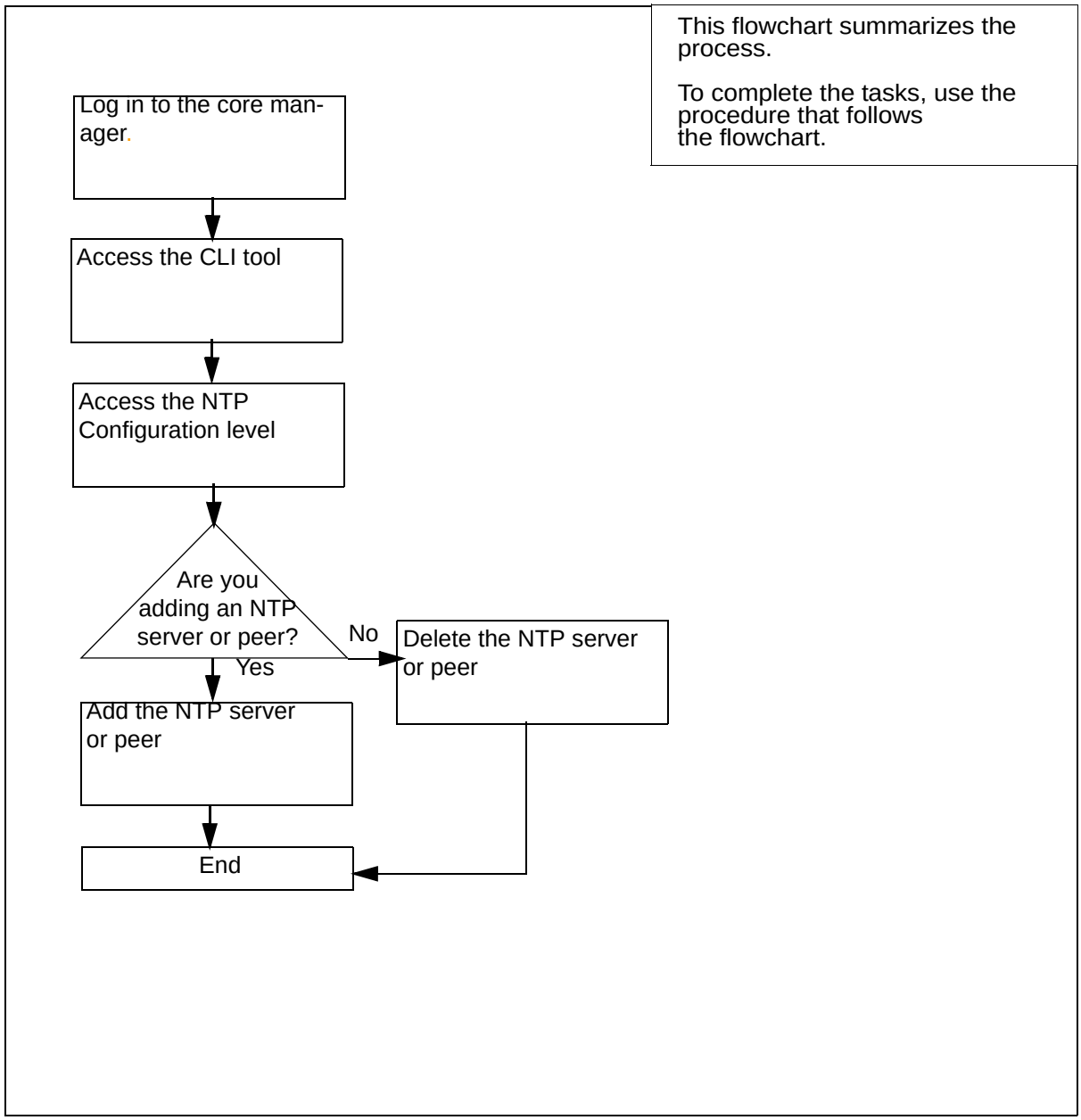
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

## Task flow for adding or removing an NTP server or peer




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

## Procedure

### Adding or removing an NTP server or peer

***At the local VT100 console***

**1** Log into the core manager. Refer to Prerequisites on page 109 for details.

**2** Access the CLI tool

**`cli`**

**3** Access the CLI configuration level:

**<#>**

*where*

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

**4** Access the NTP configuration level:

**<#>**

*where*

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

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

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

**<#>**

*where*

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

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

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

***Note 1:*** You can add a maximum of three NTP servers or peers. If you attempt to add more than three, then the system will only recognize the three most recent NTP servers or peers.

***Note 2:*** A peer can act as a server.

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

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

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

8 Remove all NTP servers

**<#>**

*where*

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

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

10 Remove only selected NTP servers or peers

**<#>**

*where*

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

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

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

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

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

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

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

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

```
sbmcbmmtc ntp
```

**16** You have completed this procedure.

# Installing the logreceiver tool on a client workstation

## Application

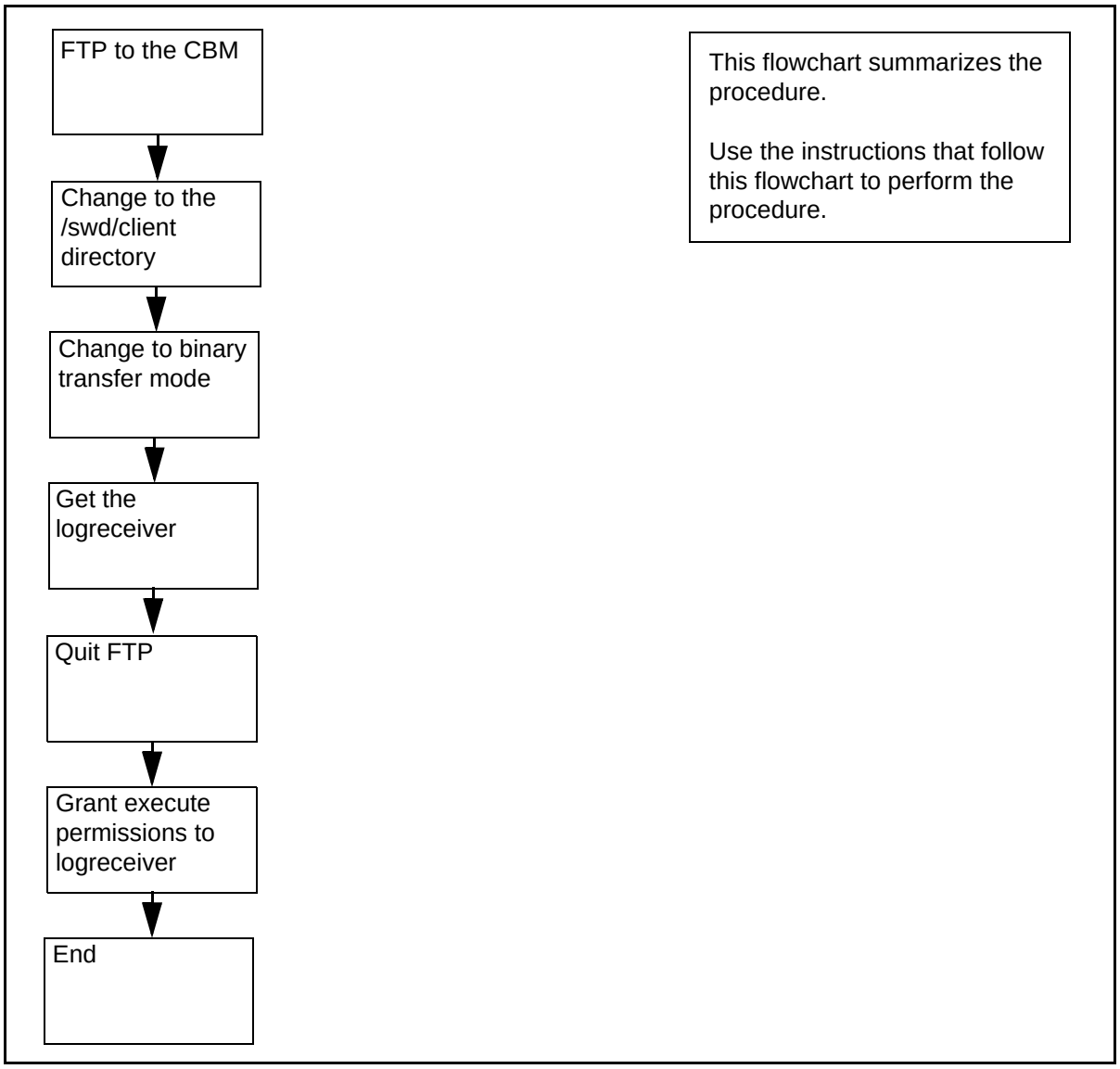
Use this procedure to install the logreceiver tool on a client workstation. The procedure accesses the logreceiver software stored on the CBM to which the workstation can connect, and installs it in a specific directory on the workstation.

***Note:*** The logreceiver tool is supported only on clients running Solaris 7, Solaris 8, or Solaris 9.

## 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 Installing the logreceiver tool on a client workstation




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

### Installing the logreceiver tool on a client workstation

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

**1** FTP to the CBM

```
ftp <CBM_IP_address>
```

*where*

**<CBM_IP_address>**
is the IP address or node name of the CBM

2 Change the directory to /swd/client

```
ftp> cd /swd/client
```

3 Change the files transfer mode to binary

```
ftp> binary
```

4 Get the logreceiver tool

```
ftp> get logreceiver
```

5 Quit FTP

```
ftp> bye
```

6 Grant execute permissions to the logreceiver

```
chmod +x logreceiver
```

7 You have completed this procedure.

# Installing the CMFT on a client workstation

## Purpose

Use this procedure to install the Command Module File Transfer script (CMFT) on a client workstation.

## Application

This procedure copies the CMFT from the Command Module (CM) to a specified directory on the client workstation, typically /sdm/bin. The CMFT script allows you to use SCFT (SSH Core File Transfer) to transfer files to and from the CM.

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

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

## Prerequisites

### Logging on to the CS 2000 Core Manager

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

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

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

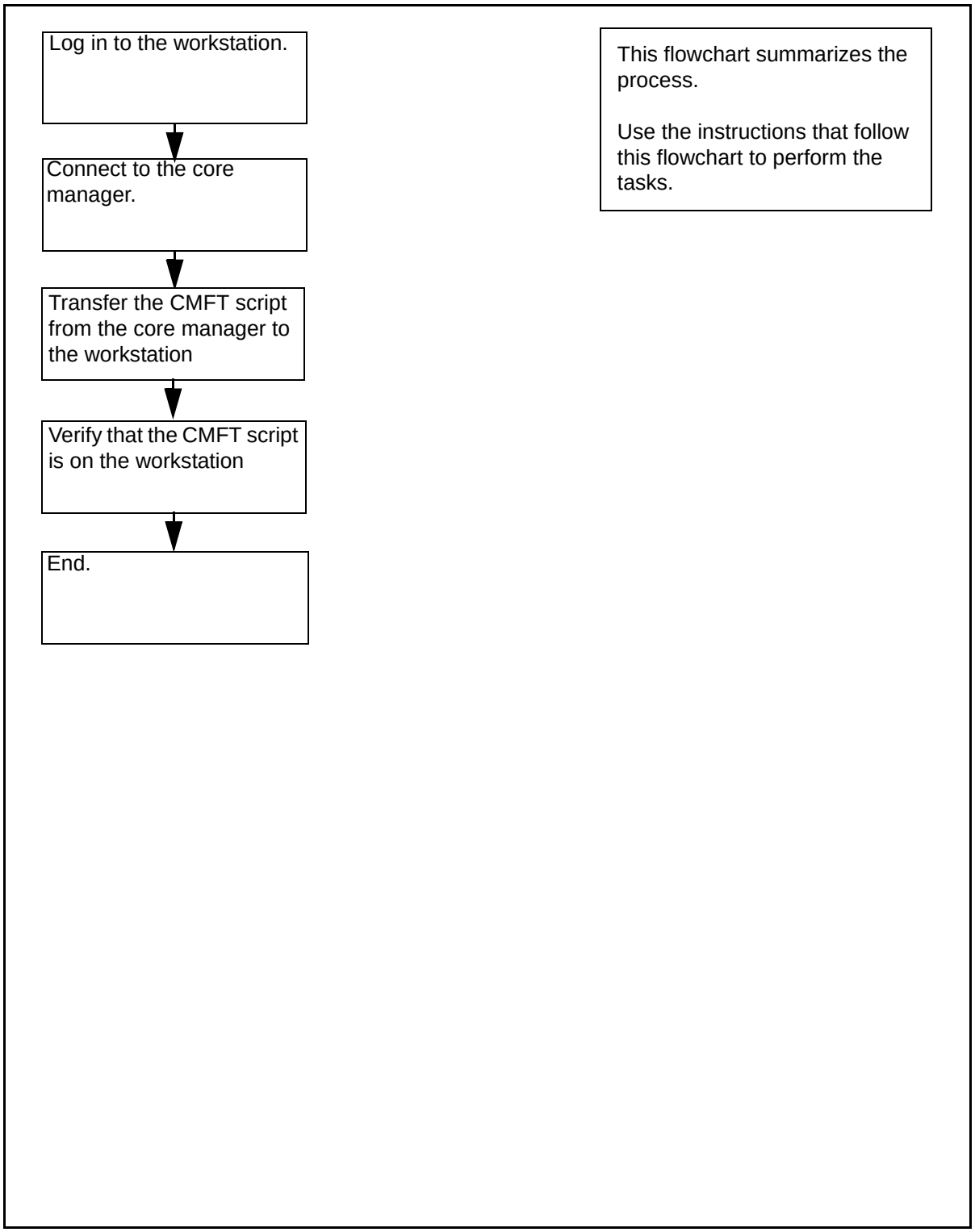
### Logging on to the Core and Billing Manager 850

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

## Task flow diagram

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

## Task flow for installing the CMFT on a client workstation



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

## Procedure

### Installing the CMFT on a client workstation

### At the local or remote VT100 console

1 Log in to the client workstation.

2 Get the CMFT script from the core manager:

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

where

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

3 Verify that you have successfully transferred the CMFT script

```
ls -l cmft
```

The client workstation displays the CMFT script.

4 Set the ownership and permissions of the CMFT script to 755:

```
chmod 755 cfmt
```

5 You have completed this procedure.

# Initiating a recovery back to the cluster

## Prerequisites

It is expected that the primary server is in the shut-down mode.

If the box was previously a CBM HA cluster, any billing files not already sent to a down-stream billing server should be removed prior to performing ‘Installing the remote backup server.

## Target

When completed, this procedure will reboot unit 0 of the cluster (configured as a remote backup server in step 1) after a remote backup of the original remote server located on the opposite side of the ring. Unit 0 will become the cluster and Unit 1 will clone Unit 0 and the HA Cluster (Primary Server) will then be completely recovered.

## Action

**Initiating a recovery back to the cluster**

***At your workstation***

**1** Follow the ‘Installing the remote backup server’ procedure.

***Note:*** In his case, the unit0 server of the cluster is used as a remote backup server. Use the same hostname and IP address that was used to configure the remote backup server in the first place

**2** Follow the ‘Scheduling automatic backup of the remote server’ procedure.

***Note:*** Use only one automated schedule and make sure to select a time that will not be invoked shortly.

**3** Follow the ‘Performing a manual backup of the remote server’ procedure.

**4** Bring down the machine currently active by following the procedure ‘Two-server (cluster) configuration’ in chapter ‘Shutting down an SPFS-based server’ of the document ATM/IP Solution-level Fault Management NN10408-900.

**5** Follow the ‘Initiating a switch over to the remote backup server’ procedure to bring the services back to unit0 of the cluster.

**6** Follow the ‘Cloning the image of one server in a cluster to the other server’ procedure of the document ATM/IP Solution-level Security and Administration NN10402-600.

7 You **MUST** remove any outstanding billing records, not already sent to a downstream billing server, from the remote server (if that is a CBM) before continuing otherwise the billing records on that box will be lost.

8 Reinstall the backup server following the (Installing the remote backup server' procedure.

9 Reconfigure the backup server following the 'Scheduling automatic backups of the remote server' procedure.

10 The procedure is complete.

# Initiating a switch over to the remote backup server

## Prerequisites

Prior to starting this procedure the Cluster machine must be shut down.

To carry this out, refer to section ‘Two-server (cluster) configuration’ in chapter ‘Shutting down an SPFS-based server’, of the document *ATM/IP Solution-level Fault Management* NN10408-900.

The user must be logged in as the root user in order to initiate the switch command.

## Target

When completed, this procedure will reboot the remote backup server as the unit0 of the cluster.

## Action

**Initiating a switch over to the remote backup server**

***At your workstation***

**1** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**<server>**
is the IP address or host name of the SPFS-based remote backup server

**2** When prompted, enter your user ID and password.

**3** Invoke the switch by typing

```
$ /opt/sspfs/rbks/switch
```

and pressing the Enter key.

**4** When ready, indicate you want to proceed by typing

```
OK
```

and pressing the Enter key.

**5** The procedure is complete.

# Installing the remote backup server

## Target

Use this procedure to perform a manual backup of the remote server. Backing up the remote server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with system configuration data and files accurate to the last synchronization.

## Action

### Installing the remote backup server

***At your workstation or the remote server console***

**1** Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server

| If you want to log in by means of | Do |
|---|---|
| ssh | Type ssh -1 root <server> and press the Enter key. Go to step 2 |
| telnet | Type telnet <server> and press the Enter key. Go to step 2 |
| the remote server console | step 2 |

where

**<server>**
is the name of the N240 server.

**2** Log in to the server through the console (port A) and when prompted, enter the root user ID and password.

**3** Bring the system to the OK prompt by typing:

```
# init 0
```

and pressing the Enter key.

**4** Insert SPFS CD disk#1 into the drive.

**5** At the OK prompt, restore the system by typing:

```
OK boot cdrom - rbackup
```

and pressing the Enter key.

6 When prompted, accept the software license restrictions by typing:

**OK**

and pressing the Enter key.

7 When prompted for the profile, press the Enter key.

8 The system will prompt:

```
Enter the hostname for this system
```

Enter the hostname.

9 The system will prompt:

```
Enter ip address for <hostname>
```

Enter the IP address.

10 The system will prompt:

```
Enter the subnet mask for this network
[255.255.255.0]
```

Enter the subnet mask.

11 The system will prompt:

```
Enter ip address for this networks router
```

Enter the router's IP address.

12 The system will prompt:

```
Enter the timezone for this system
```

Enter your timezone.

***Note:*** The default is 'US/Eastern'. Enter'?' for a list of supported time zones.

13 The system will prompt:

```
Will this system use DNS?
```

Enter 'yes' or 'no'. If you answer 'yes' you will be prompted for the DNS domain name, name server IP addresses, and the search domains. You may enter several name servers and search domains, to stop entry enter a blank line.

***At the server***

1 Remove SPFS Disk 1 from the CDROM drive, and insert SPFS Disk 2.

***At the server console***

1 When ready, indicate you want to proceed by typing:

**OK**

and pressing the Enter key.

2 Once Disk 2 is installed successfully press the Enter key twice to reboot the system and apply OS patches.

***At the server***

1 Remove SPFS Disk 2 from the CDROM drive, and insert SPFS Disk 3.

***At the server console***

1 When ready, indicate you want to proceed by typing:

**OK**

and pressing the Enter key.

2 Once Disk 2 is installed successfully press the Enter key twice to reboot the system and apply OS patches.

3 The procedure is complete.