Core and Billing Manager 800 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 800 for (I)SN09

Feature changes

There are no feature changes in this release.

Other changes

There are no other changes in this release.

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 12.
- delete an existing device, refer to the procedure Deleting a device using logroute on page 19.
- modify global parameters (parameters that apply to all devices), refer to the procedure Configuring Log Delivery global parameters on page 31.

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

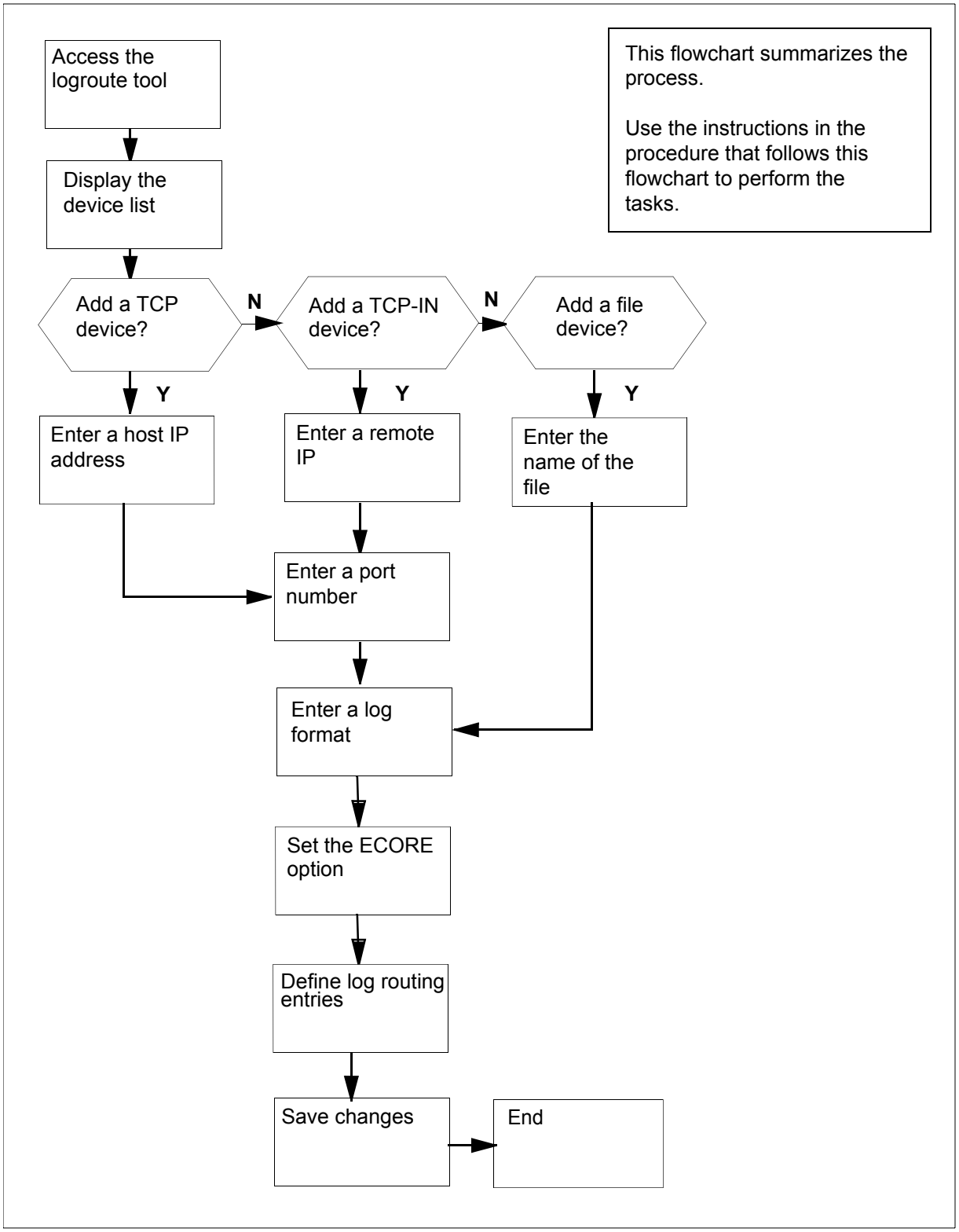
Logging on to the Core and Billing Manager 800

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 2 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 24. Logs suppressed at the CM cannot be unsuppressed for a specific device.

Example response:

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

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

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

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

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

Example response:

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

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

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

y

The new device will be added to the system.

Example response:

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

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

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

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

18 Return to the Device List Menu screen:

5

19 Return to the Logroute Main Menu screen:

6

20 Quit the logroute tool:

6

21 You have completed this procedure.

Modifying a log device using logroute

Purpose

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

The routing rules you enter for each device only accommodate the set of logs defined in the procedure Specifying the logs delivered from the CM to the core manager on page 24. 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 31.

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

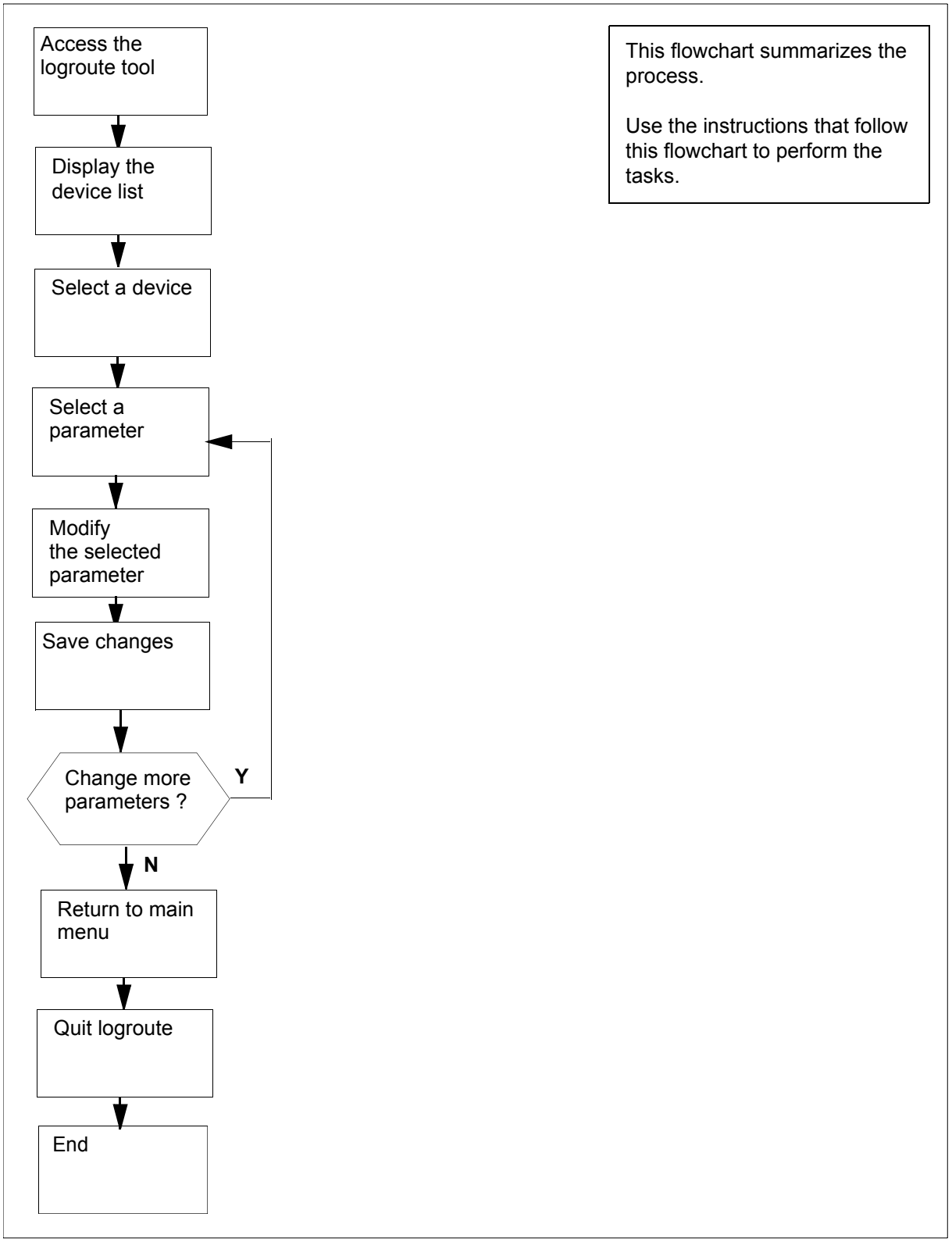
Logging on to the Core and Billing Manager 800

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 12 for details.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                Logroute Main Menu


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




 Enter Option ==>
```

3 Display the device list:

1

The Device List Menu screen appears.

```
                    Device List Menu


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




 Enter Option ==>
```

4 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

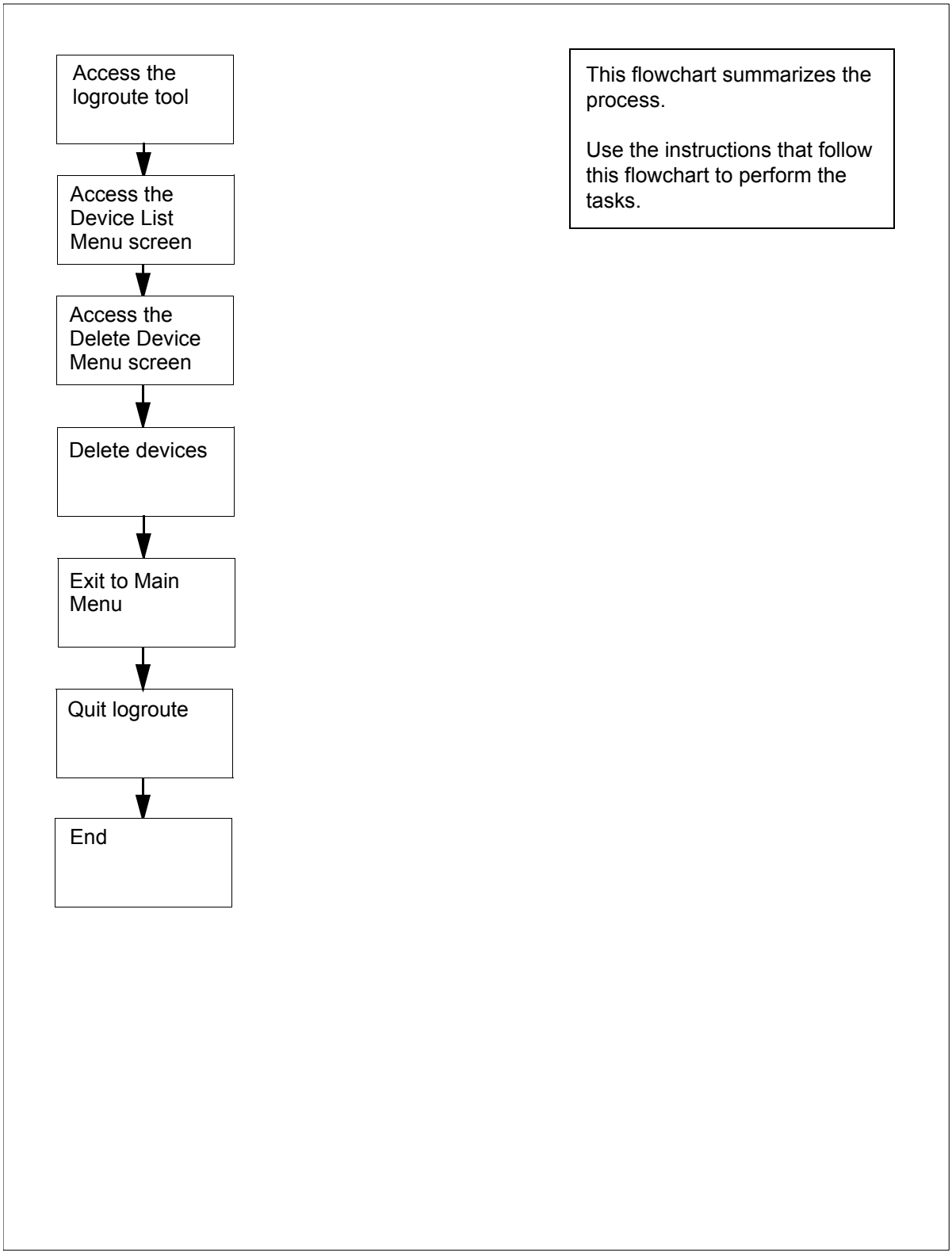
Logging on to the Core and Billing Manager 800

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 19 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.

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

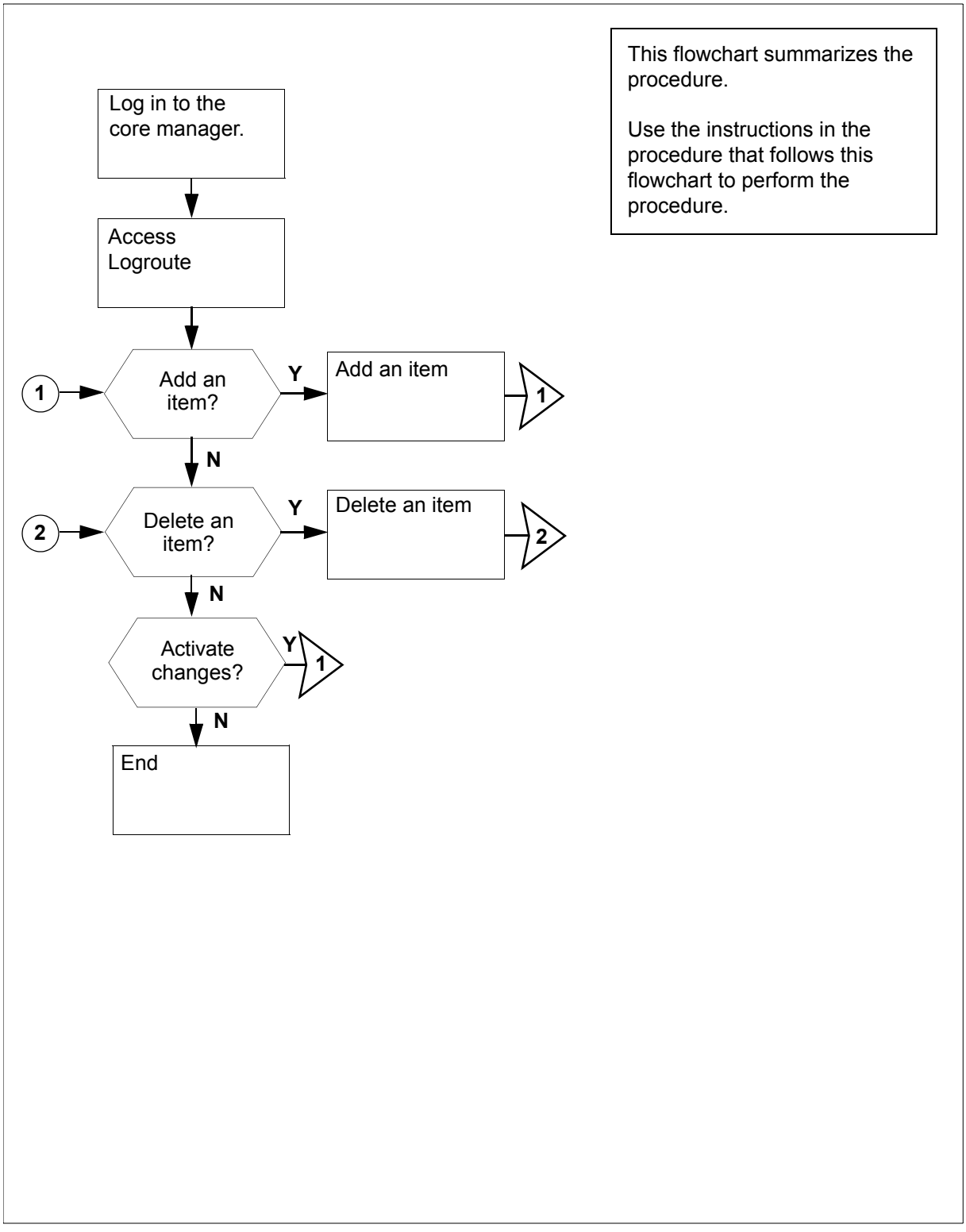
Logging on to the Core and Billing Manager 800

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 24 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 2
- Modifying a log device using logroute on page 12

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

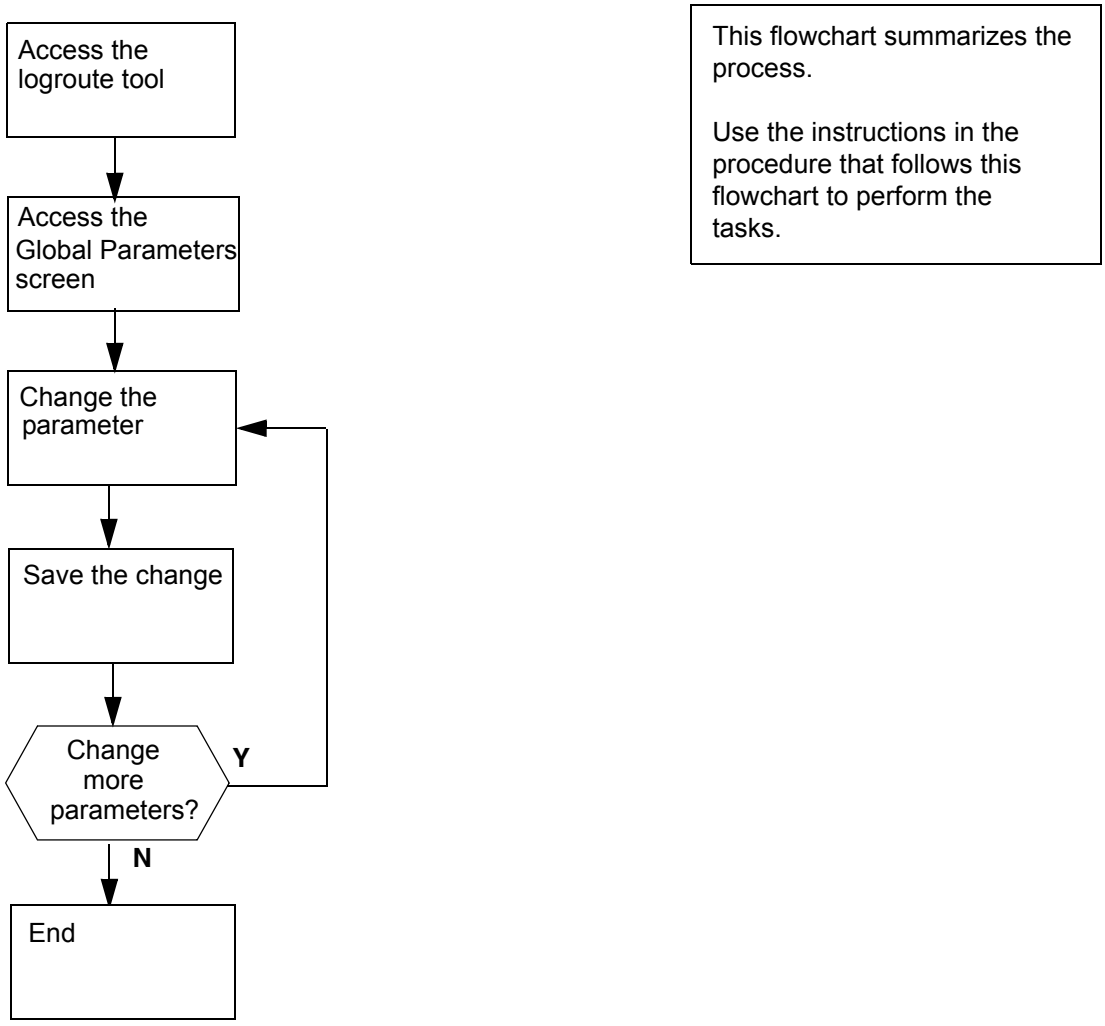
Logging on to the Core and Billing Manager 800

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 33 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

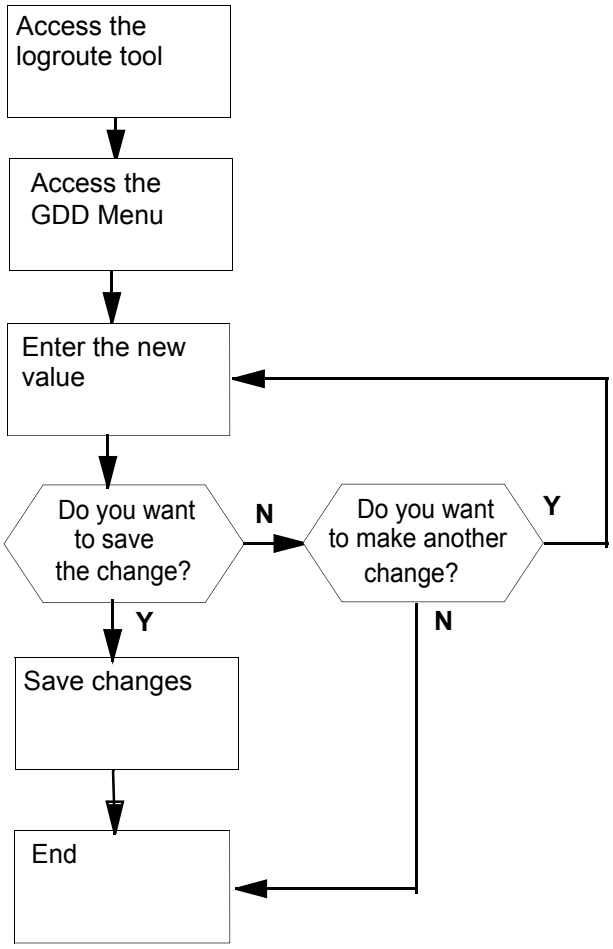
Logging on to the Core and Billing Manager

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



This flowchart summarizes the process.

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

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 38 for details.

2 Access the logroute tool:

```
logroute
```

The Logroute Main Menu screen appears.

```
                    Logroute Main Menu


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



 Enter Option ==>
```

3 Access the GDD Menu:

4

Example response::

```
                        GDD Menu


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









Enter Option ==>
```

4 Select the GDD parameter:

1

Example response:

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

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

Example response:

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

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

6 Cancel your change:

n

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

7 Save the GDD value:

y

Example response::

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

8 Press the Enter key to confirm the change.

Example response:

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

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

10 Return to the Logroute Main Menu screen:

3

11 Quit the logroute tool:

6

12 You have completed this procedure.

Commissioning or decommissioning Network Time Protocol (NTP)

Purpose

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

Note: After CBM 800 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

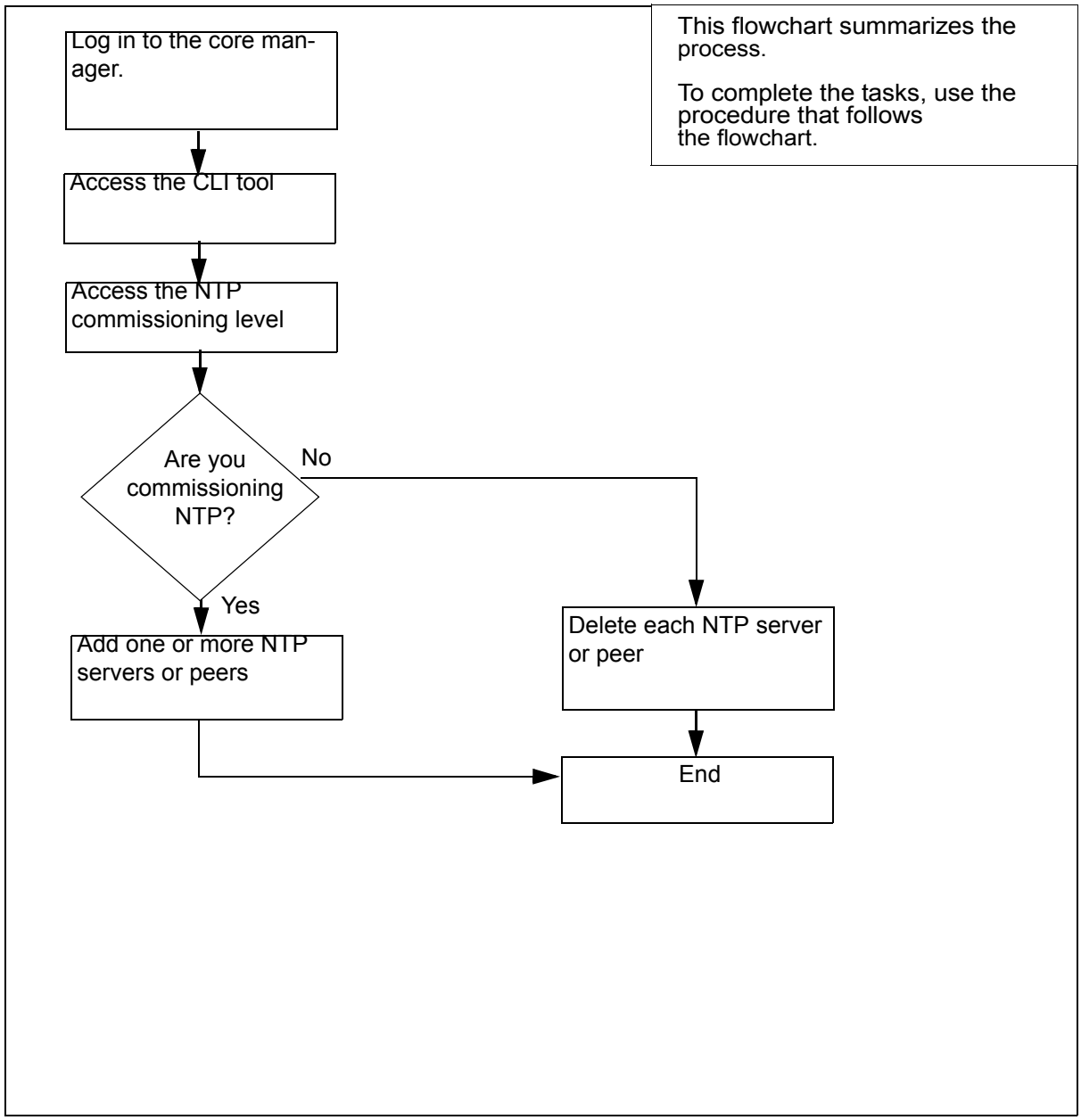
Logging on to the Core and Billing Manager 800

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

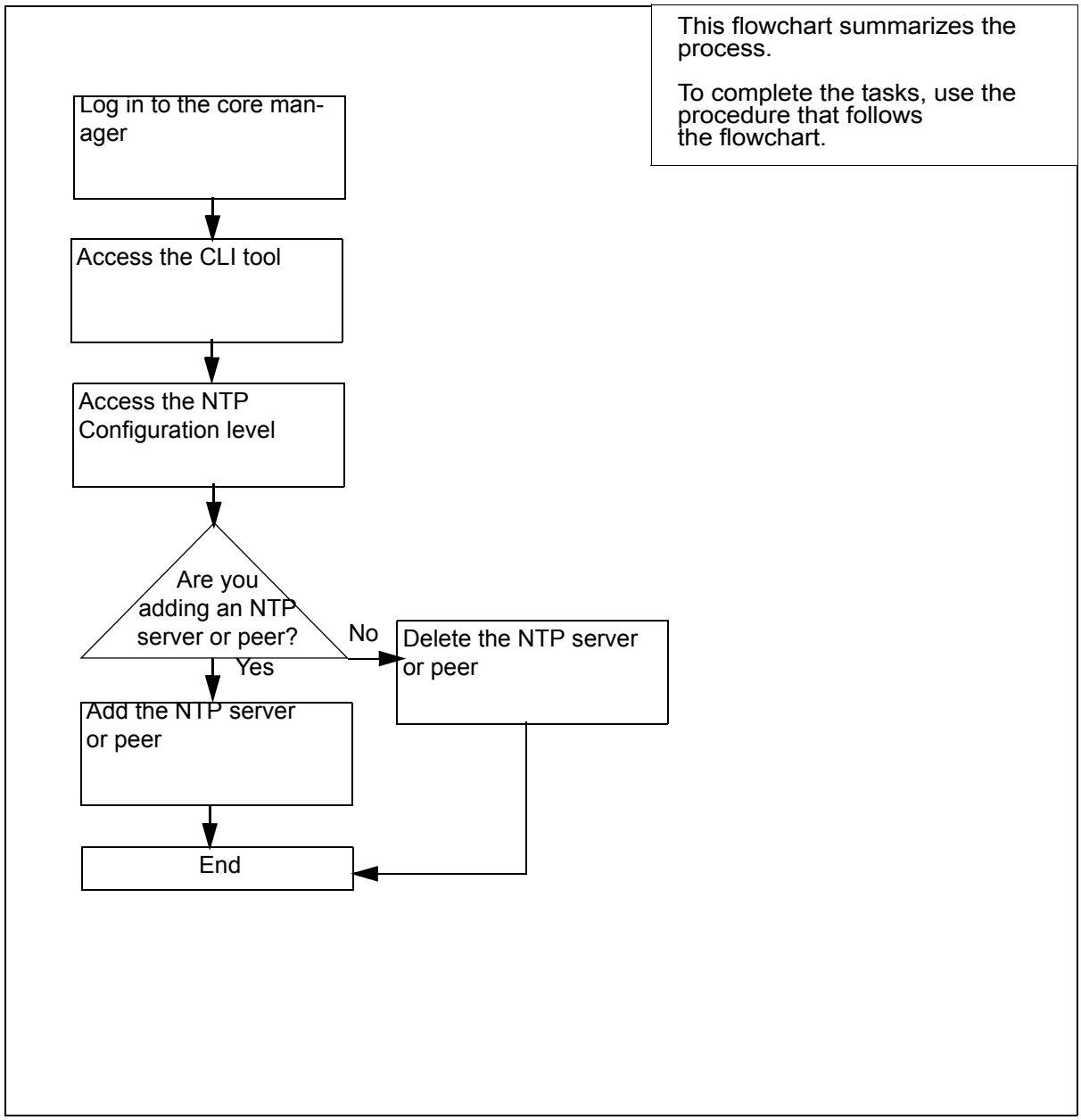
Logging on to the Core and Billing Manager 800

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 49 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.

```
mtc ntp
```

16 You have completed this procedure.

Installing the logreceiver tool on a client workstation

Application

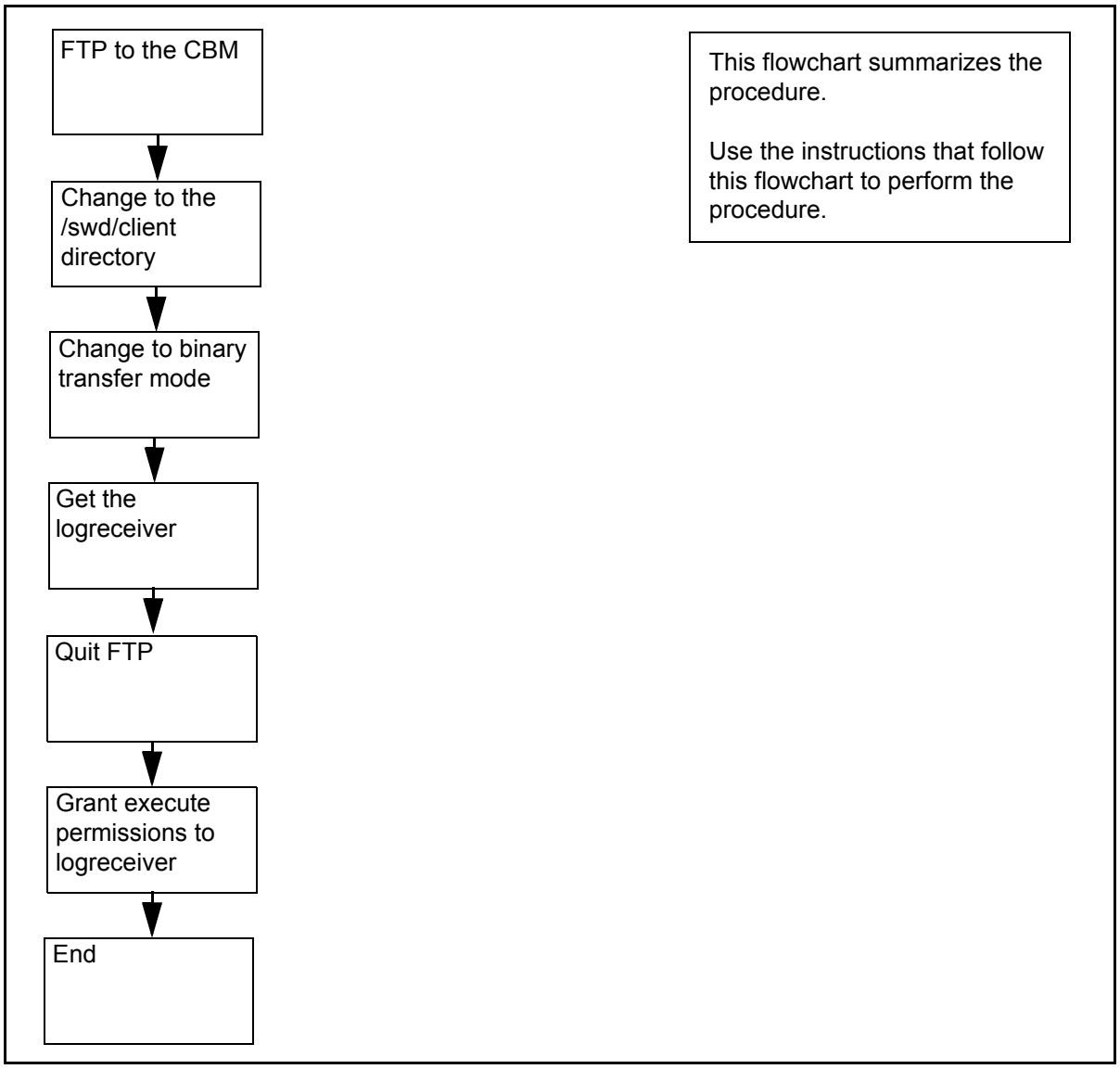
Use this procedure to install the logreceiver tool on a client workstation. The procedure accesses the logreceiver software stored on the CBM to which the workstation can connect, and installs it in a specific directory on the workstation.

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

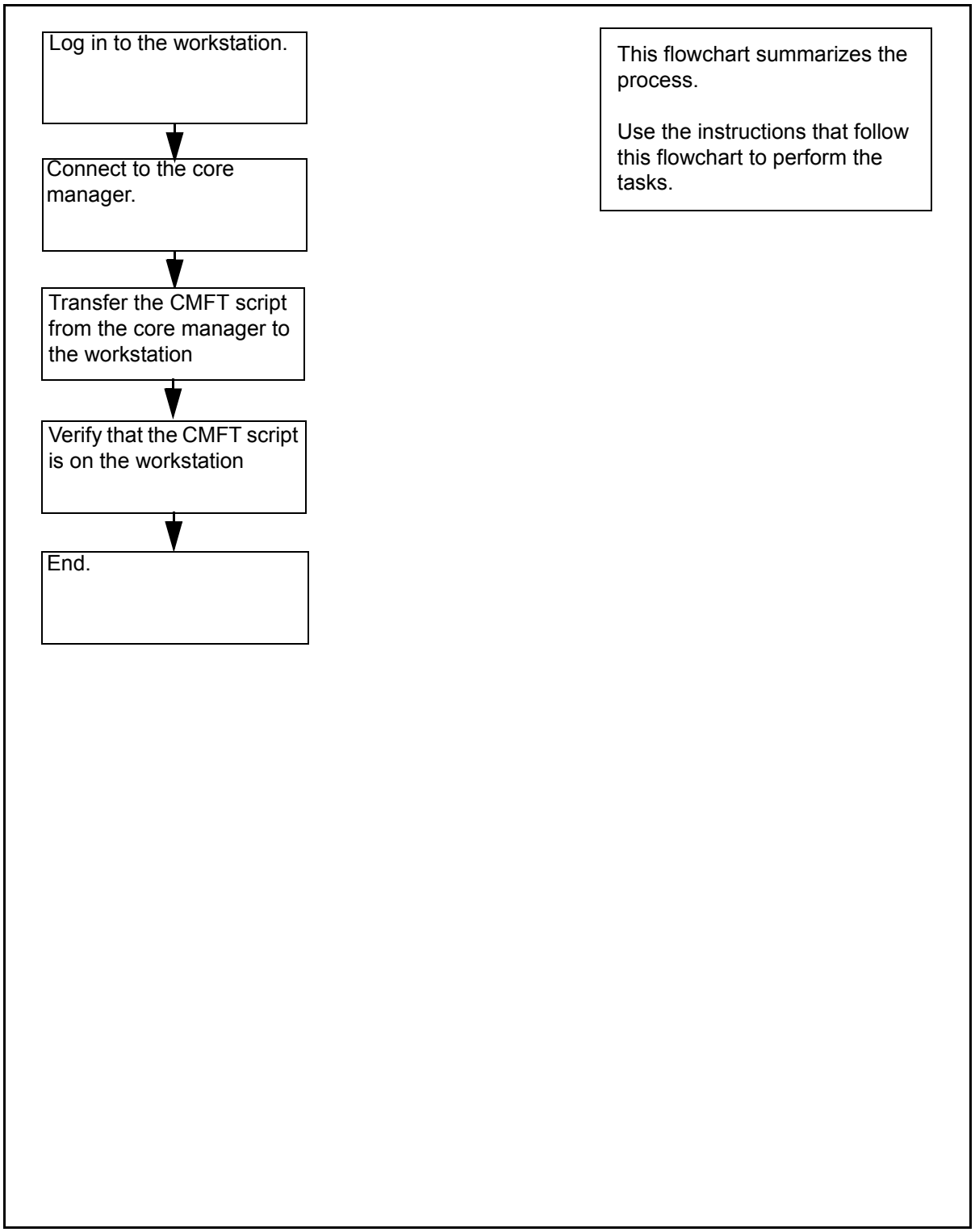
Logging on to the Core and Billing Manager 800

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.