297-5051-906

DMS-100 Family

SuperNode Data Manager

Fault-tolerant User Guide

SDMN0009 Standard 03.04 October 1998

NORTEL

NORTHERN TELECOM

DMS-100 Family

SuperNode Data Manager

Fault-tolerant User Guide

Publication number: 297-5051-906
Product release: SDMN0009
Document release: Standard 03.04
Date: October 1998

Printed in the United States of America

Publication history

May 1998

SDMN0009 Standard 03.03 document upissued to include changes for software release SDMNM009.3

February 1998

SDMN0009 Standard 03.02 document upissued for editorial changes

February 1998

SDMN0009 Standard 03.01 document upissued to standard

August 1997

SDMN0004 Standard 02.01 document upissued to include changes for the SDMN004 release

August 1997

SDMN0003 Standard 01.03 editorial changes made

August 1997

SDMN0003 Standard 01.02 document upissued to standard

May 1997

SDMN0003 Preliminary 01.01 first release of this document

Contents

Figures

Tables

About this document

When to use this document

This document contains information for administering and maintaining the fault-tolerant SuperNode Data Manager (SDM). It is intended for SDM system administration and maintenance personnel.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers, for example, 01.01.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the *next* software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time the document is revised but rereleased in the *same* software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

To determine which version of this document applies to the software in your office and how documentation for your product is organized, check the release information in *DMS-100 Family Guide to Northern Telecom Publications*, 297-1001-001.

References in this document

The following documents are referred to in this document:

- *DMS-100 Family Guide to Northern Telecom Publications*, 297-1001-001
- *DMS-100 Family Trouble Locating and Clearing Procedures*, 297-xxxx-544
- *DMS-100 Routine Maintenance Procedures*, 297-xxxx-546
- *SuperNode Data Manager Enhanced Terminal Access User Guide*, 297-5051-904

- *SuperNode Data Manager Exception Reporting User Guide*, 297-5051-912
- *SuperNode Data Manager Secure File Transfer User Guide*, 297-5051-913
- *SuperNode Data Manager SuperNode Billing Application Application Guide*, 297-5051-300
- *OSF DCE Command Reference*, ISBN 0-13-185844-0, Release 1.1 (1995) Open Software Foundation, Inc., 11 Cambridge Center, Cambridge, MA 02142.

What precautionary messages mean

The types of precautionary messages used in Nortel documents include attention boxes and danger, warning, and caution messages.

An attention box identifies information that is necessary for the proper performance of a procedure or task, or the correct interpretation of information or data. Danger, warning, and caution messages indicate possible risks.

Examples of the precautionary messages follow.

ATTENTION Information needed to perform a task

ATTENTION

If the unused DS-3 ports are not deprovisioned before a DS-1/VT Mapper is installed, the DS-1 traffic will not be carried through the DS-1/VT Mapper, even though the DS-1/VT Mapper is properly provisioned.

DANGER Possibility of personal injury

DANGER

Risk of electrocution

Do not open the front panel of the inverter unless fuses F1, F2, and F3 have been removed. The inverter contains high-voltage lines. Until the fuses are removed, the high-voltage lines are active, and you risk being electrocuted.

WARNING Possibility of equipment damage

WARNING
Damage to the backplane connector pins
Align the card before seating it, to avoid bending the backplane connector pins. Use light thumb pressure to align the card with the connectors. Next, use the levers on the card to seat the card into the connectors.

CAUTION Possibility of service interruption or degradation

CAUTION
Possible loss of service
Before continuing, confirm that you are removing the card from the inactive unit of the peripheral module. Subscriber service will be lost if you remove a card from the active unit.

How commands, parameters, and responses are presented

Commands, parameters, and responses in this document conform to the following conventions.

Input prompt (>)

An input prompt (> or #) indicates that the information that follows is a command or other required input:

```
>BSY
```

Commands and fixed parameters

Commands and fixed parameters that are entered at the MAP display are shown in uppercase letters:

```
>BSY  LINK
```

UNIX commands and fixed parameters that are entered at the SDM are shown in lowercase and uppercase letters, depending on the UNIX syntax:

```
>echo  $TERM
```

Variables

Variables that are entered at the MAP display are shown in lowercase letters:

>BSY LINK ps_link

UNIX variables that are entered at the SDM are shown in italicized lowercase letters:

>setenv TERM *term_type*

The letters or numbers that the variable represents must be entered. Each variable is explained in a list that follows the command string.

Multiple keystrokes

Multiple keystrokes, such as control character sequences, are shown enclosed in angle brackets and separated by a dash. The following example indicates that you hold down the control key while pressing b:

<CTRL-b>

Responses

Responses generated by the MAP display and the SDM are shown in a different type:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed.
```

The following excerpt from a procedure shows the command syntax used in this document:

1 Manually busy the CTRL on the inactive plane by typing

>BSY CTRL ctrl_no
and pressing the Enter key.

where

ctrl_no is the number of the CTRL (0 or 1)

Example of a MAP response:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed.
```

Understanding the fault-tolerant SDM

This chapter describes the SuperNode Data Manager (SDM) fault-tolerant platform, as follows:

- ”SDM overview” on page 1-1 summarizes the SDM characteristics and capabilities.
- ”SDM hardware” on page 1-4 describes the hardware of the SDM fault-tolerant platform.
- ”SDM software” on page 1-22 describes the base, service, and application software provided with the SDM fault-tolerant platform, and the maintenance and administration user interfaces.
- ”LAN-based I/O interface capabilities” on page 1-25 summarizes equipment configuration capabilities and requirements for connecting the SDM to the operating company local area network (LAN).
- ”SDM Log Delivery” on page 1-27 describes the SDM Log Delivery application.

SDM overview

The fault-tolerant SDM is a high-performance UNIX-based processing platform that supports DMS SuperNode operations, administration, maintenance, and provisioning applications.

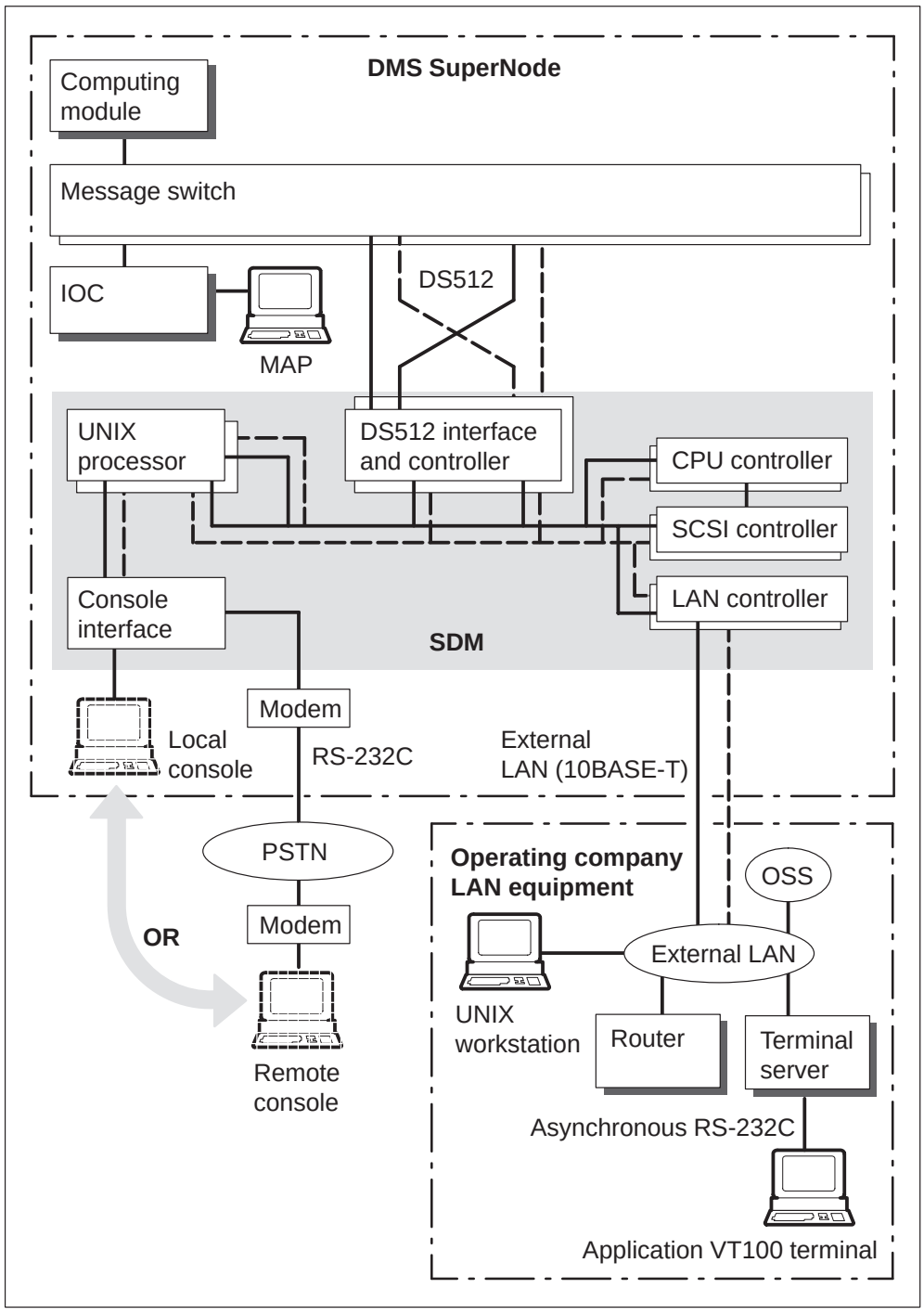
In conjunction with the SDM-resident base and application software developed by Nortel (Northern Telecom), and corresponding DMS-based hardware and software elements, the SDM fault-tolerant platform uses Motorola technology, and includes the following elements:

- PowerPC 604 microprocessor
- fault-tolerant (FT) hardware
- AIX 4.1.4 operating system

Figure 1-1 shows the position of the SDM within the DMS SuperNode system. The fault-tolerant SDM is connected to the message switch (MS) using four DS512 fiber links from two DS512 controller modules. Each DS512 controller module is equipped with two ports that connect over separate links to the two MS planes. These links maintain communication to

the MS if a link fails or if one side of the MS is unavailable. External hardware is connected to the SDM through modems using serial ports or through the operating company LAN using a built-in Ethernet interface.

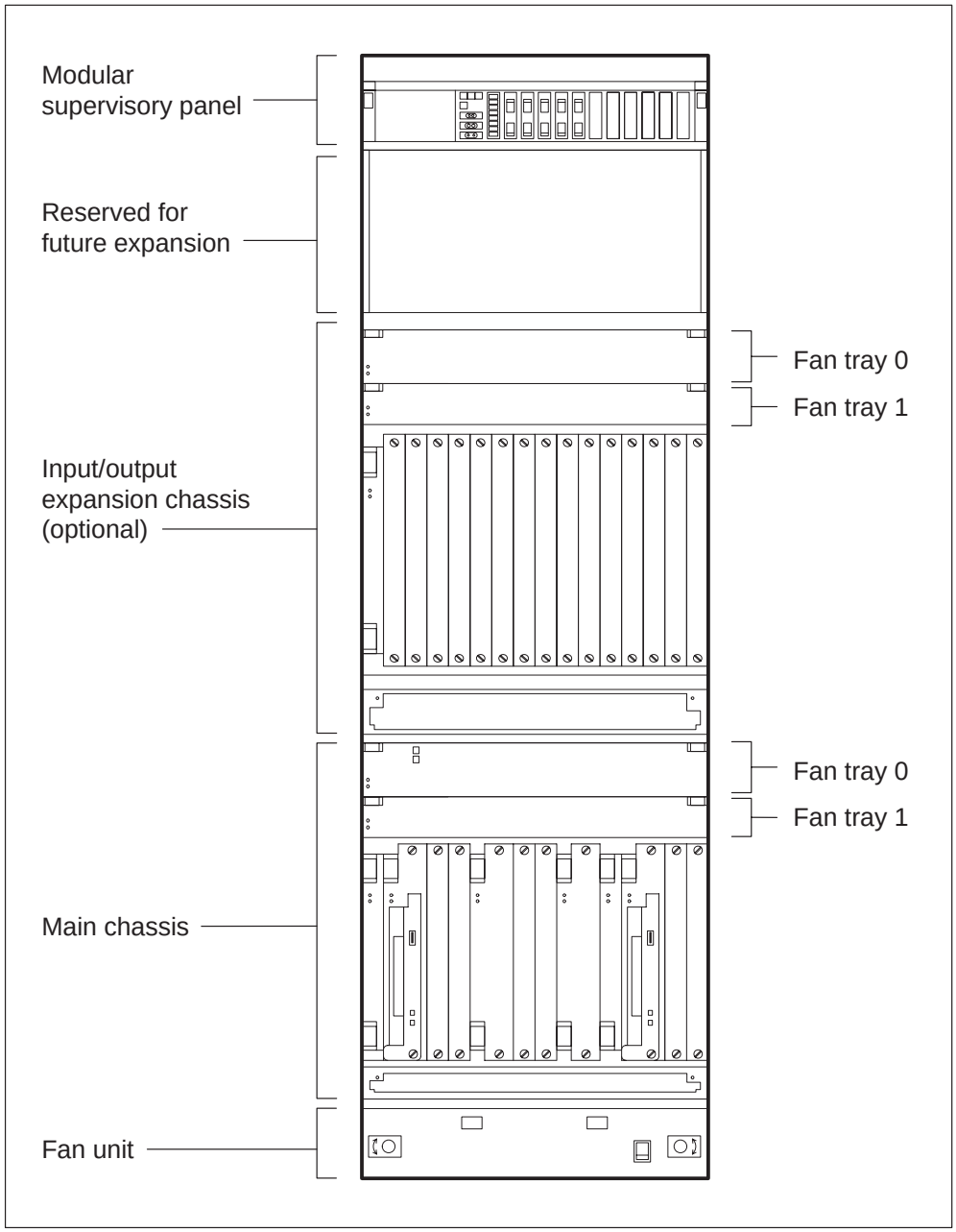
Figure 1-1
SDM position in the DMS SuperNode system



SDM hardware

This section is an overview of the hardware components that can make up the SDM fault-tolerant platform. The SDM chassis mounts in a Nortel C28 Model B (C28B) DMS Streamlined cabinet as shown in figure 1-2. The input/output expansion chassis shown in figure 1-2 is optional.

Figure 1-2
Front view of SDM cabinet



SDM cabinet

The SDM cabinet contains the modular supervisor panel (MSP), an optional I/O expansion chassis, the main chassis, and the fan unit. The I/O expansion chassis is located above the main chassis, and can be used for future expansion. Both chassis have 16 slots, each with front and rear sections.

Controller modules are located at the front of the main chassis and the I/O expansion chassis. Each controller module has a P1 and a P2 connector. All controller modules, except for the CPU controller module, use the P1 connector to plug directly into a mid-mounted backplane. The P2 connector bypasses the backplane and plugs directly into the corresponding personality module, located at the back of the SDM.

Note: Controller modules are described on pages 1-6 and 1-20.

Each chassis is divided into two domains: domain 0 and domain 1. In each chassis, slots 1 to 5 make up domain 0, and slots 12 to 16 make up domain 1. (Slots 6 to 11 make up the CPU core.) The two domains mirror (duplicate) each other's functionality to achieve fault-tolerant operation. The modules in each chassis must be provisioned in pairs and occupy the corresponding slot in each domain. If a module in domain 0 malfunctions, the corresponding module in domain 1 takes over operations, avoiding a service interruption, and vice versa.

Modular supervisory panel

The MSP provides power and alarm monitoring capabilities for the C28B cabinet. The SDM fault-tolerant platform is powered by A and B battery feeds (-48V dc). Each feed is supplied from a separate breaker in the MSP into interconnect modules (ICMs), located in the main and I/O expansion chassis.

The SDM computing hardware provides failure indications through volt-free relay contacts in the ICM. These contacts provide an interface to the MSP and to the central office alarm system. The status of the SDM is monitored at the remote maintenance interface (RMI) alarm banner and the MAP alarm banner. If a fan within the fan unit fails, or a power alarm occurs, the MSP also activates end-of-aisle lamps on the DMS switching equipment, and frame-fail lamps on the SDM cabinet.

Fan unit

The fan unit provides cooling in the SDM cabinet, in addition to the fan trays in the main and I/O expansion chassis. The fan trays provide horizontal cooling from the front to the rear of the SDM. The fan unit provides vertical cooling, forcing hot air up and out the top of the SDM.

Note: For information on replacing this fan unit or its cooling unit filter, refer to *DMS-100 Family Trouble Locating and Clearing Procedures* and *DMS-100 Family Routine Maintenance Procedures* included with your DMS switch.

Front-mounted SDM main chassis hardware

Figure 1-3 shows a front view of the main chassis of the SDM fault-tolerant platform. The front of the chassis is equipped with upper and lower fan trays, and provisionable controller modules. Minimally, the front of the main chassis must contain the following controller modules:

- two DS512 controller modules (NTRX50GA) that mount in slots 1 and 12
- two I/O controller modules (NTRX50FQ) that mount in slots 2 and 3, and in slots 13 and 14
- two CPU controller modules (NTRX50FK), with 128-Mybte memory, that mount in slots 6 and 7, and in slots 10 and 11

Figure 1-3
Front view of the main chassis

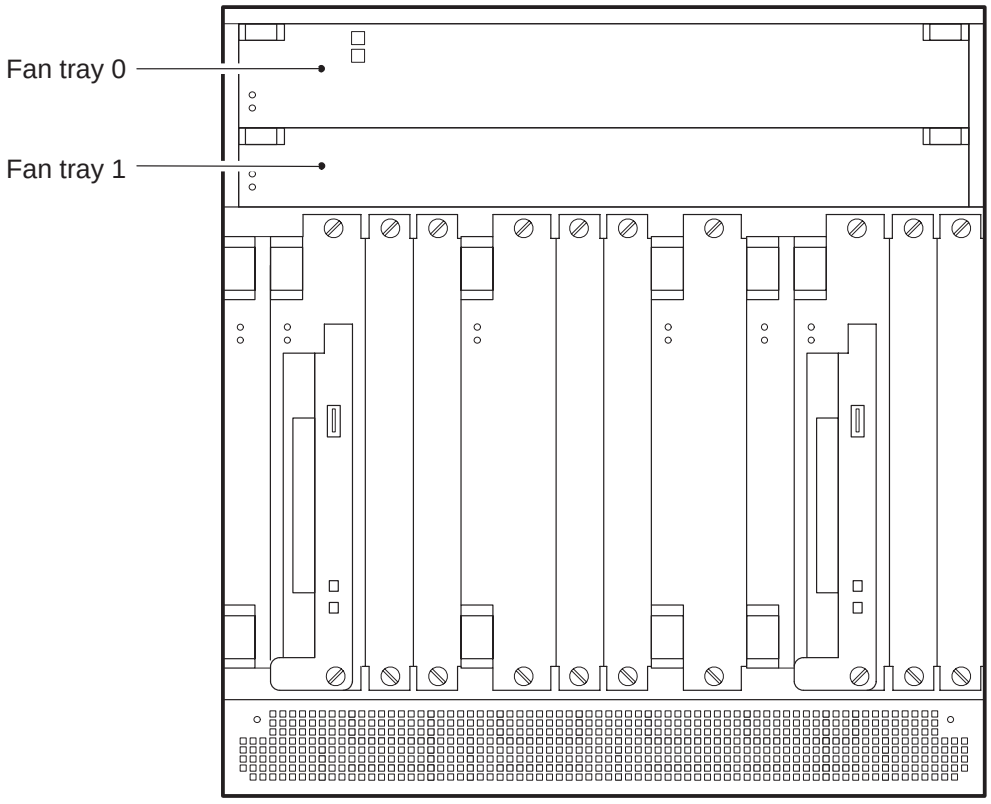
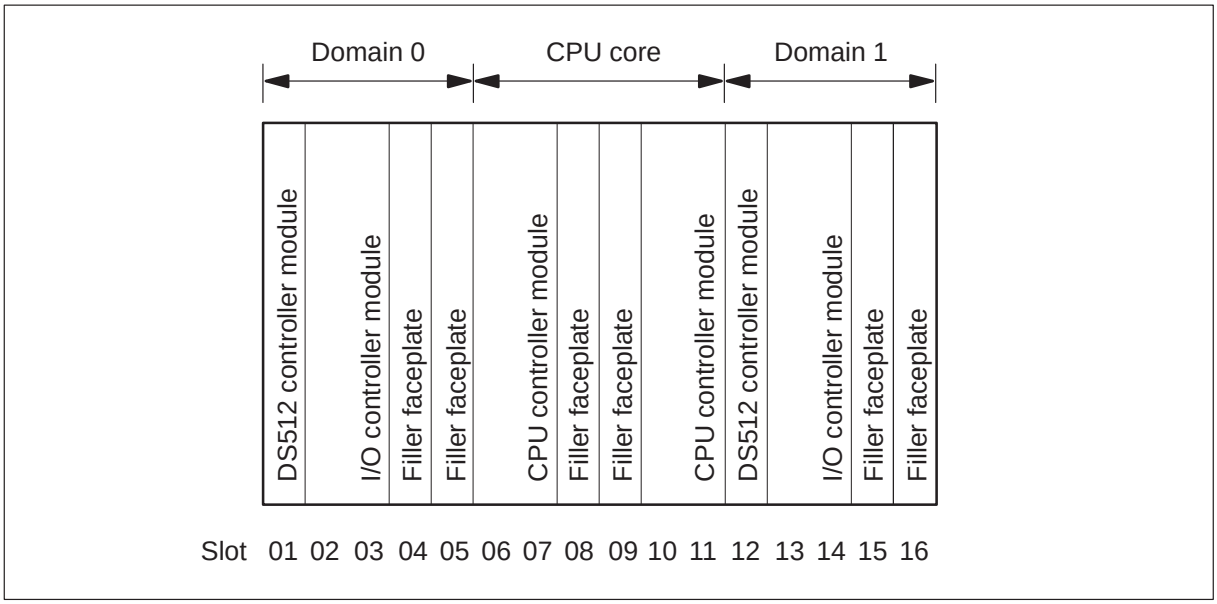


Figure 1-4 shows the slot numbers contained in domain 0, domain 1, and the CPU core. It also identifies the required provisionable controller modules shown in the main chassis in figure 1-3. All other slots are available for provisioning optional controller modules.

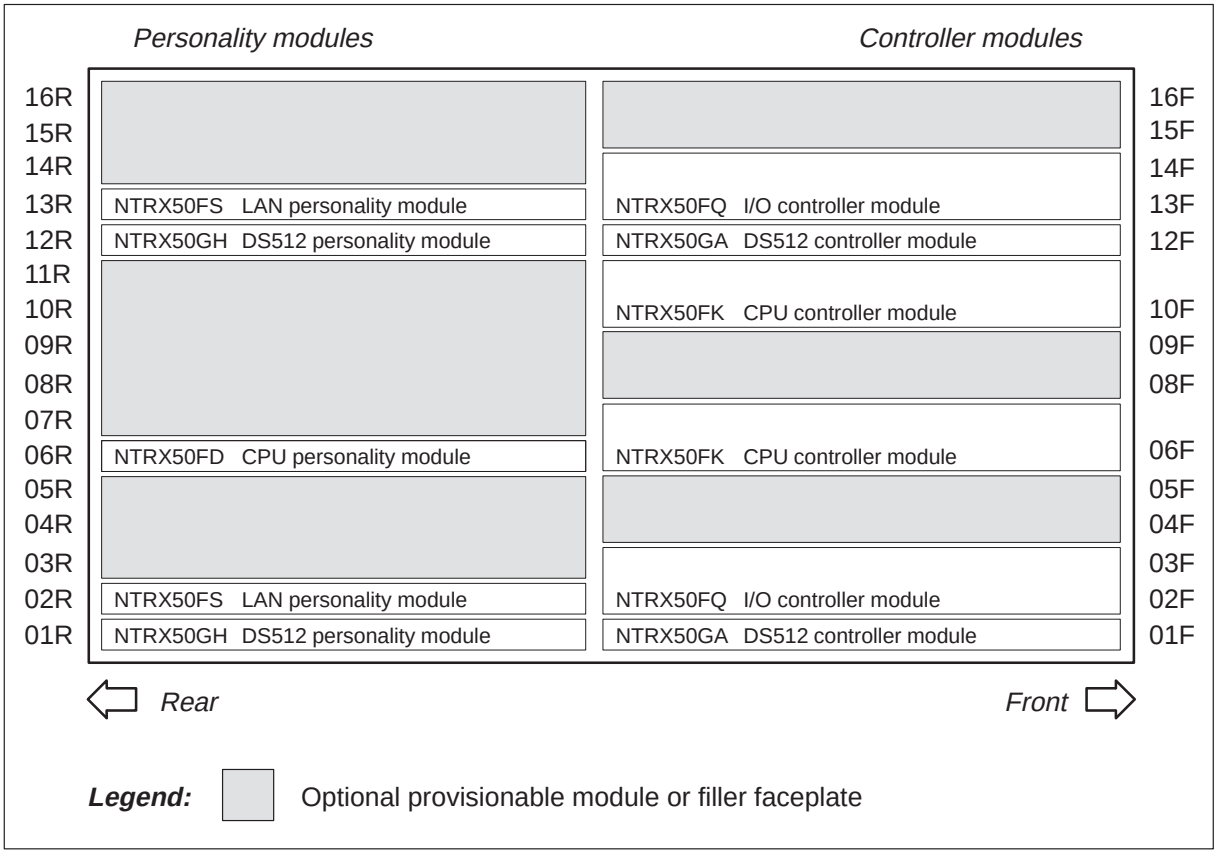
Figure 1-4
Front view of the main chassis by slot number



Module slot placement

Figure 1-5 shows the dedicated slot numbers for required modules mounted at the front and back of the main chassis of the fault-tolerant SDM. These slot numbers must be used for these modules. Unless noted otherwise, other provisionable equipment can be mounted in any other slot number in either the main or I/O expansion chassis. The corresponding slot number for controller and personality modules must, however, be used for each domain. For example, a provisionable controller module that is mounted in slot 4 (domain 0) must also be mounted in slot 15 (domain 1) to achieve fault-tolerant operation for both domains. The required personality module also mounts in slot 4 and 15 at the back of the SDM. When a controller module occupies two slots, its personality module occupies the lower slot number. For example, if a controller module occupies slots 4 and 5, and 15 and 16 at the front of the SDM, its personality module occupies slots 4 and 15 at the back of the SDM.

Figure 1-5
Module slot number layout



CPU controller module (NTRX50FK)

The CPU controller module is a provisionable item that must mount in slots 6 and 7, and in slots 10 and 11, at the front of the main chassis of the SDM. The minimum memory option of this module is 128-Mbyte (NTRX50FK), however, it is also available in memory options of 256-Mbyte (NTRX50FL) or 512-Mbyte (NTRX50FM).

The CPU controller module contains the main processing power and memory capacity of the SDM. Each CPU controller module plugs into the backplane of the main chassis through P1 and P2 connectors. The CPU controller module is used in conjunction with the CPU personality module (NTRX50FD), which is located in slot 6 at the back of the main chassis of the SDM. The CPU personality module provides console port connections to the CPU controllers.

DS512 controller module (NTRX50GA)

The DS512 controller module is a provisionable item that must mount in slots 1 and 12 at the front of the main chassis of the SDM. Each module

supports two DS512 fiber links that connect to the two MS planes. These four links are normally all operating. If one module fails, the other module takes over, ensuring that communication to the computing module (CM) continues.

The DS512 controller module is used in conjunction with the DS512 personality module (NTRX50GH), which is located in slot 1 and 12 at the back of the main chassis of the SDM. The DS512 controller module connects to its DS512 personality module using a P2 connector.

I/O controller module (NTRX50FQ)

The I/O controller module is a provisionable item that must mount in slots 2 and 3, and in slots 13 and 14, at the front of the main chassis of the SDM. The I/O controller module provides a 3.5-in. 2-Gbyte disk drive unit (DDU), a digital audio tape (DAT) drive, and an Ethernet interface. The disk drive is used for storage of the AIX operating system, the SDM base, service and application software, and data. The DAT drive is used for installation of SDM software, for software restore in the event of corruption or disk drive failure, and for performing software and data backups.

For information on performing software backups and restores, refer to the "SDM system administration overview" and "SDM system administration procedures" chapters of this document.

The NTRX50FQ I/O controller module is recommended for systems with limited application storage requirements of less than 1 Gbyte. Application data is stored in the root volume group (rootvg). Rootvg cannot be upgraded to 4 Gbyte (I/O controller module NTRX50GN). To upgrade to an I/O controller module with the data volume group (datavg), manual transfer of data is required, and application service is interrupted.

The I/O controller module is used in conjunction with the LAN personality module (NTRX50FS) to provide connectivity using a 10BASE-T port from the SDM to the operating company LAN. The LAN personality module mounts in slots 2 and 13 at the back of the main chassis. The module is connected to its I/O controller module using a P2 connector.

Note: The NTRX50FU and NTRX50GP I/O controller modules are provisionable and can be used in addition to the NTRX50FQ I/O controller module. For more information on these modules, including their use with the NTRX50FQ I/O controller module, refer to "I/O controller module (NTRX50FU)" on page 1-20, and "I/O controller module (NTRX50GP)" on page 1-21.

Optional slots at the front of main chassis

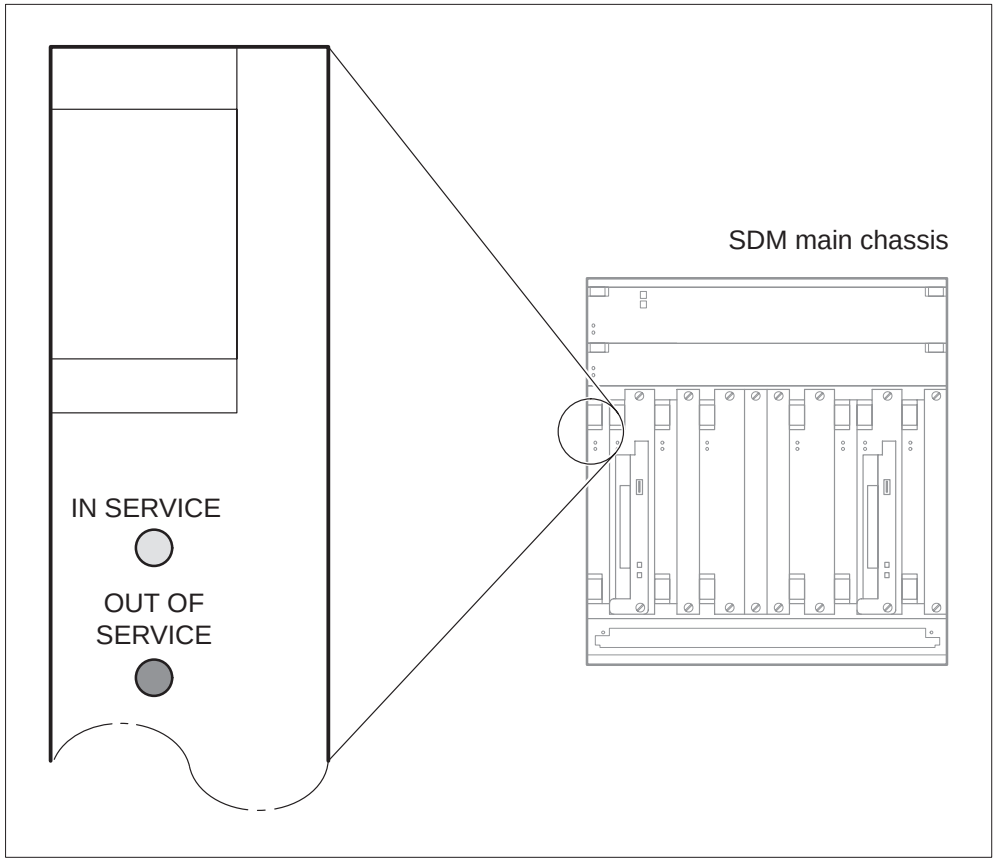
Slots 4, 5, 8, 9, 15 and 16 at the front of the main chassis of the SDM are not used, unless your SDM contains additional provisionable equipment. All

unused slots at the front must be equipped with filler panels to ensure electromagnetic interference (EMI) compliance, and to distribute cooling air evenly.

Controller module LEDs

Figure 1-6 shows the LEDs on the controller modules at the front of the main chassis of the SDM. These LEDs are visible on all controller modules in the main or the optional I/O expansion chassis. These LEDs are described in further detail on page 2-95.

Figure 1-6
Controller module LEDs



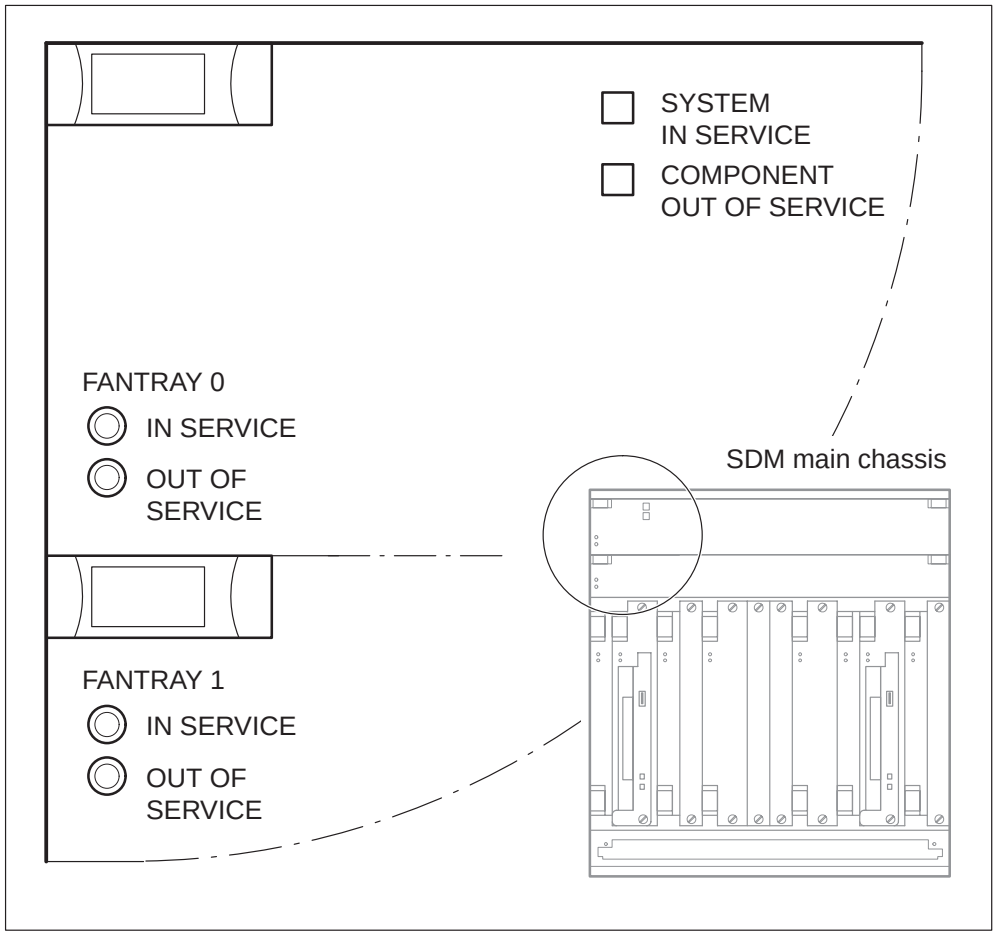
Fan trays

The main chassis is equipped with two removable fan trays (NTRX50FE and NTRX50FF) that provide uninterrupted cooling to the main chassis. Each fan tray has three fans. The fan trays are powered by separate battery feeds. This ensures uninterrupted cooling during servicing to a fan tray. Fan trays (NTRX50KD and NTRX50FF) are also located in the I/O expansion chassis.

Fan tray LEDs

Figure 1-7 shows the LEDs on the fan trays in the main chassis. Both fan trays in the main and I/O expansion chassis contain In Service and Out of Service LEDs. The top fan tray (NTRX50FE) in the main chassis also contains system status LEDs. There are no system status LEDs on the fan trays in the I/O expansion chassis. Fan tray LEDs are described in further detail on page 2-95.

Figure 1-7
Fan tray LEDs on the main chassis



Rear-mounted SDM main chassis hardware

Figure 1-8 shows a rear view of the main chassis of the SDM fault-tolerant platform. The rear of the main chassis is equipped with two DS512 personality modules (NTRX50GH) mounted in slots 1 and 12. The chassis also contains two interconnect modules (ICMs) (NTRX50FG and NTRX50FH) that supply power to the SDM. Other optional personality modules may also be mounted in this chassis.

The rear of the main chassis must also contain the following:

- two LAN personality modules (NTRX50FS) that mount in slots 2 and 13
- one CPU personality module (NTRX50FD) that mounts in slot 6

Figure 1-8
Rear view of the main chassis

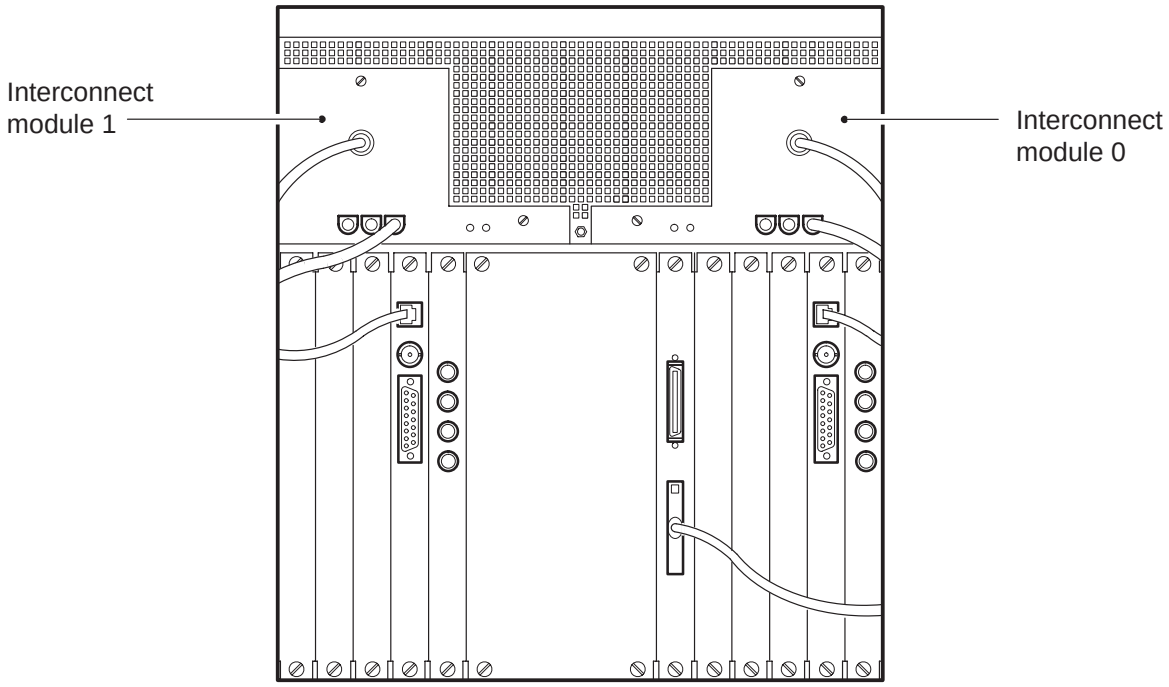
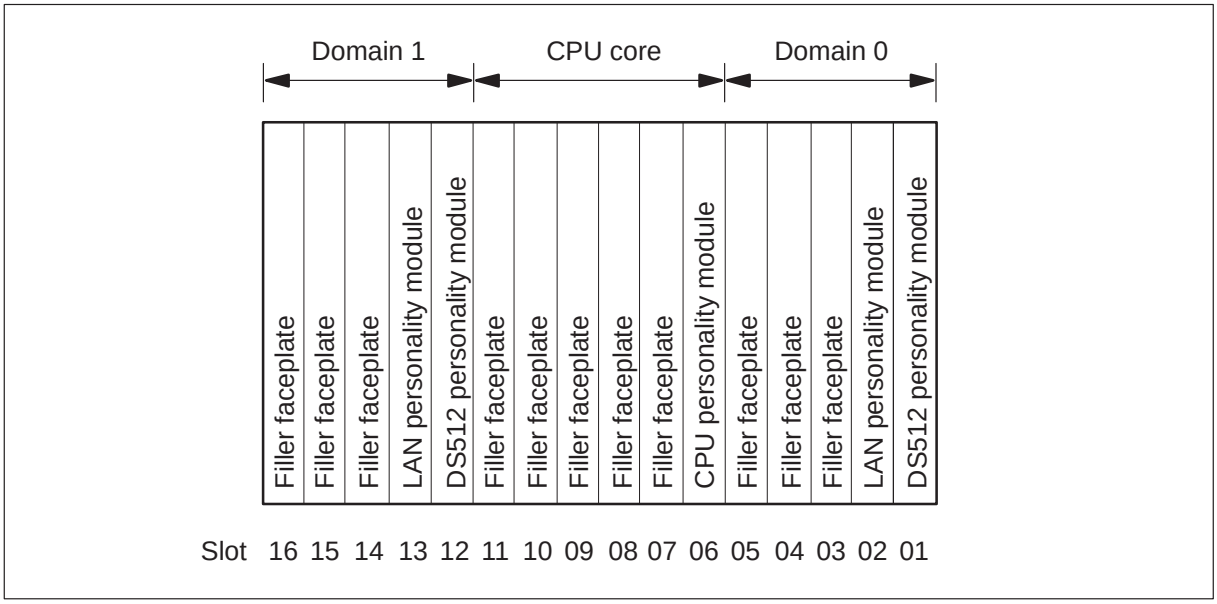


Figure 1-9 shows the slot numbers contained in domain 0, domain 1, and the CPU core. It also identifies the required provisionable personality modules in each slot number shown in figure 1-8. All other slots are available for provisioning optional personality modules.

Figure 1-9
Rear view of the main chassis by slot number



DS512 personality module (NTRX50GH)

The DS512 personality module must be mounted in slots 1 and 12 at the back of the main chassis. The DS512 personality module is connected to the DS512 controller module (NTRX50GA) located in slots 1 and 12 at the front of the main chassis.

LAN personality module (NTRX50FS)

The LAN personality module must be mounted in slots 2 and 13 at the back of the main chassis of the SDM. A LAN personality module is connected to each I/O controller module (NTRX50FQ), in slots 2 and 3, and 13 and 14 at the front of the main chassis. The LAN personality module allows for 10BASE–T port connection to the operating company LAN.

CPU personality module (NTRX50FD)

The CPU personality module must mount in slot 6 at the back of the main chassis of the SDM. The CPU controller module (NTRX50FK) connects to the CPU personality module, which provides console and modem port connection to the CPU controller module. For remote console access, port SP0 on the CPU personality module must be connected to a modem by a NTRX5093 cable. Port SP0 can be connected to a VT100 terminal by a NTRX5094 cable for local console access.

Optional slots at the back of main chassis

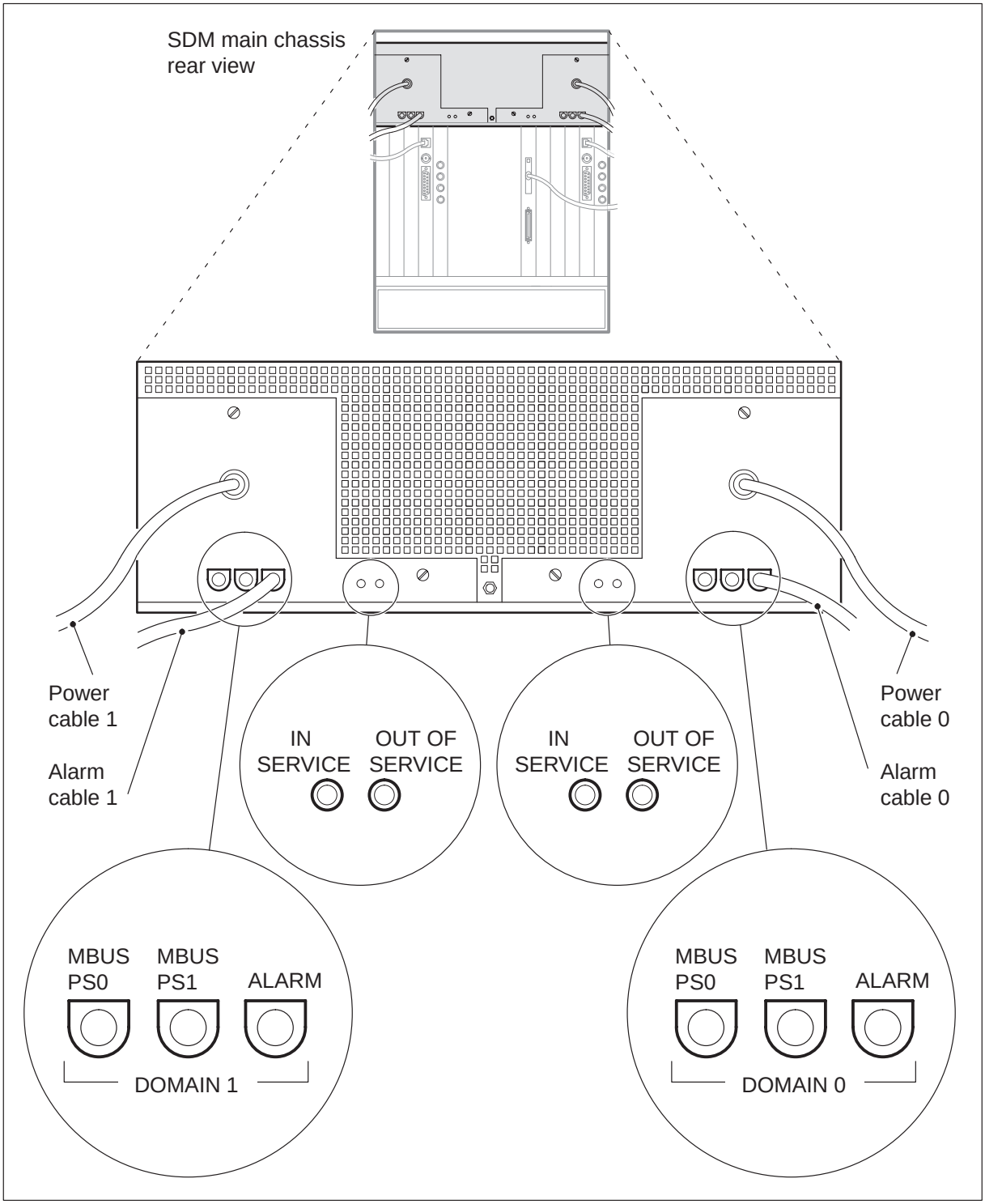
Slots 3 to 5, 7 to 11, and 14 to 16 at the back of the main chassis of the SDM are normally not used, unless your SDM contains optional equipment. All unused slots at the back must be equipped with filler panels to ensure EMI compliance, and to distribute cooling air evenly.

Interconnect modules (NTRX50FG, NTRX50FH)

Two interconnect modules (ICMs) are located at the rear of the main chassis and the I/O expansion chassis of the SDM. These modules are plugged directly into the backplane. Each ICM supplies -48V dc to its corresponding domain through separate battery feeds. Each ICM has two LEDS that indicate when it is in service, or out of service.

Figure 1-10 shows a rear view of the interconnect modules.

Figure 1-10
Rear view of the interconnect modules



Power supply

The fault-tolerant hardware on the SDM is powered by A and B battery feeds. Hardware in domain 0 is powered by battery feed A. Battery feed B powers hardware in domain 1. Both battery feeds are normally operational. During a single feed failure, the unaffected domain continues to provide all services. The A and B battery feeds from the MSP connect to the chassis through the ICMs at the back of each chassis.

Front-mounted SDM I/O expansion chassis hardware

Figure 1-11 shows a front view of the I/O expansion chassis of the SDM fault-tolerant platform. This chassis is used for optional controller modules that are not restricted to a designated slot number on the main chassis. In the example shown in figure 1-11, the I/O expansion chassis is equipped with an I/O controller module (NTRX50FU) to expand disk capacity.

Fan trays (NTRX50KD, NTRX50FF)

The I/O expansion chassis is equipped with two removable fan trays that provide uninterrupted cooling to the expansion chassis. Each fan tray has three fans. The fan trays are powered by separate battery feeds. This ensures uninterrupted cooling during servicing to a fan tray. Fan trays (NTRX50FE, NTRX50FF) are also located in the main chassis.

Note: There are no system status LEDs on the fan trays located in the I/O expansion chassis. These LEDs are only seen on the upper fan tray (NTRX50FE) in the main chassis. See figure 1-7 for more information.

Figure 1-11
Front view of the I/O expansion chassis

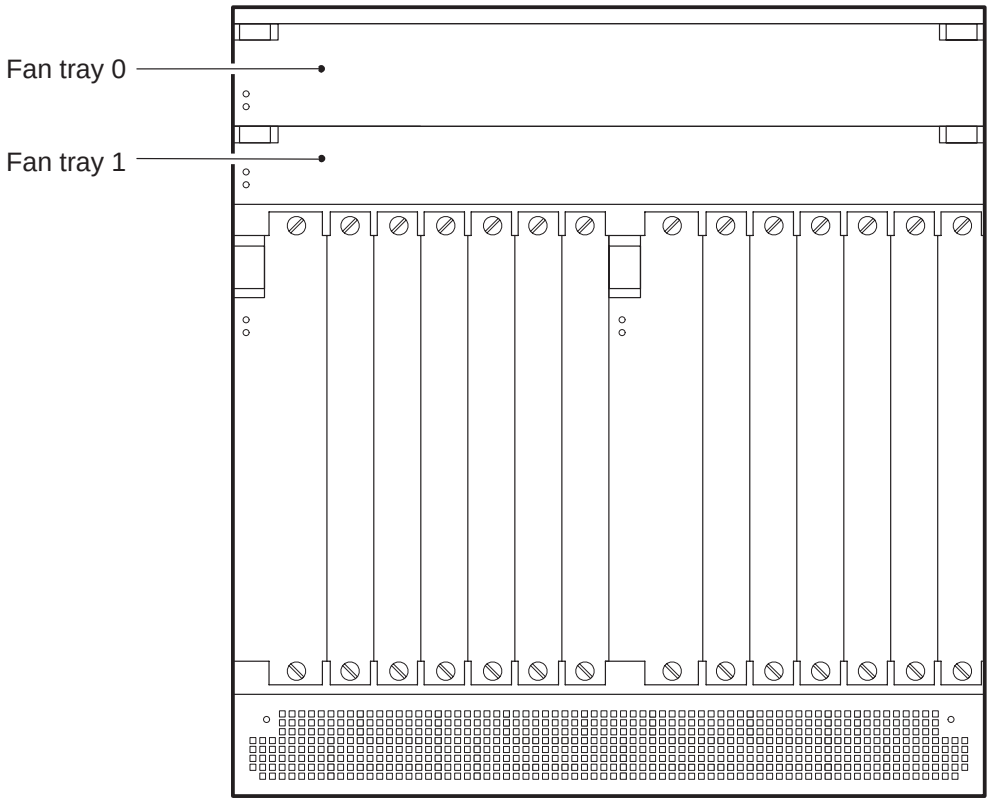
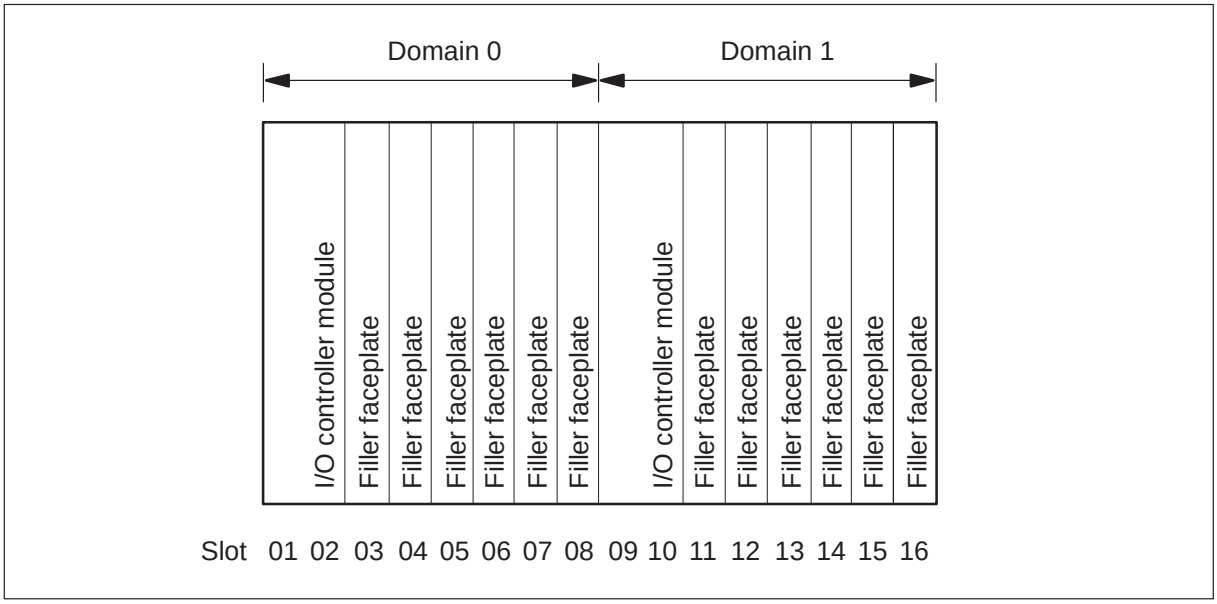


Figure 1-12 identifies the slot numbers contained in domain 0 and domain 1, and the optional I/O controller modules shown in figure 1-11.

Note: Provisionable controller modules in the I/O expansion chassis are not restricted to specific slot numbers. The I/O controller module shown in figure 1-11 can be mounted in any two slots, providing the slot numbers correspond in each domain (see page 1-7), and the corresponding personality modules are mounted in the appropriate slot at the back of the I/O expansion chassis.

Figure 1-12
Front view of the I/O expansion chassis by slot number



Rear-mounted SDM I/O expansion chassis hardware

Figure 1-13 shows a rear view of the I/O expansion chassis of the SDM fault-tolerant platform. This chassis also contains two ICMs that supply power to the SDM through separate battery feeds. The I/O expansion chassis is used for provisionable equipment that is not restricted to a designated slot number on the main chassis (see page 1-7 for more information on slot numbers).

In the example shown in figure 1-13, the I/O expansion chassis is equipped with a LAN personality module (NTRX50FS) in slot 9. This module is used in conjunction with the I/O controller module (NTRX50FU) that mounts at the front of the I/O expansion chassis.

Note: There is no alarm cable for the ICMs located in the I/O expansion chassis. The ICMs located in the main chassis each have an alarm cable (see figure 1-8.

Figure 1-13
Rear view of the I/O expansion chassis

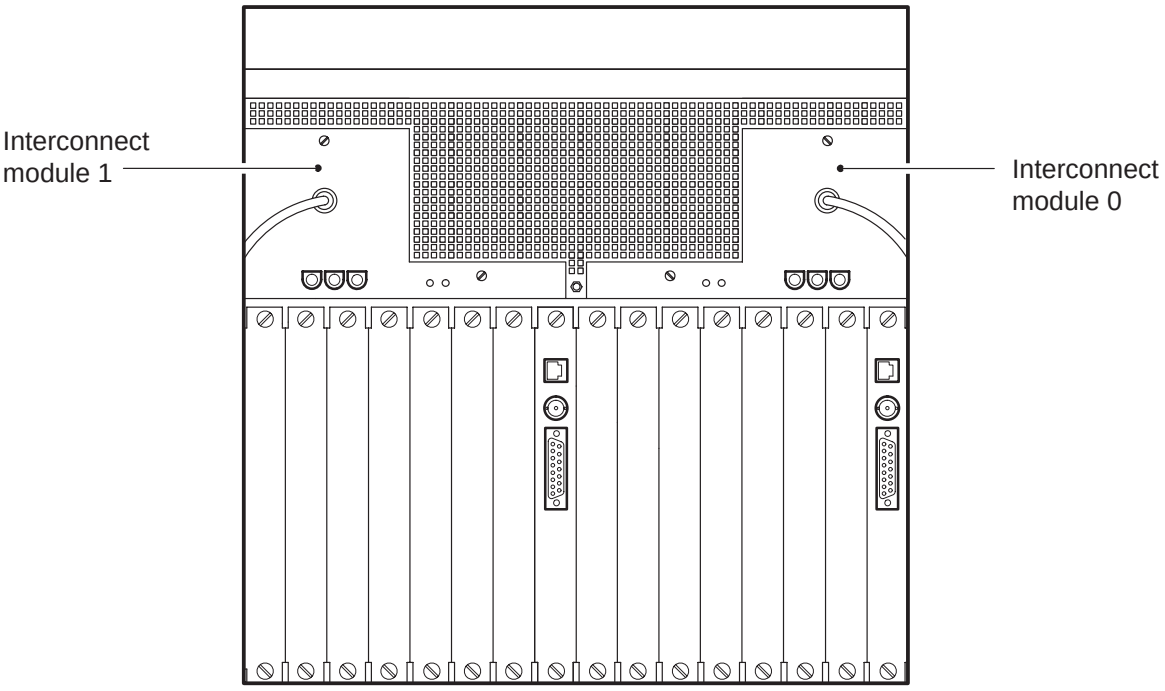
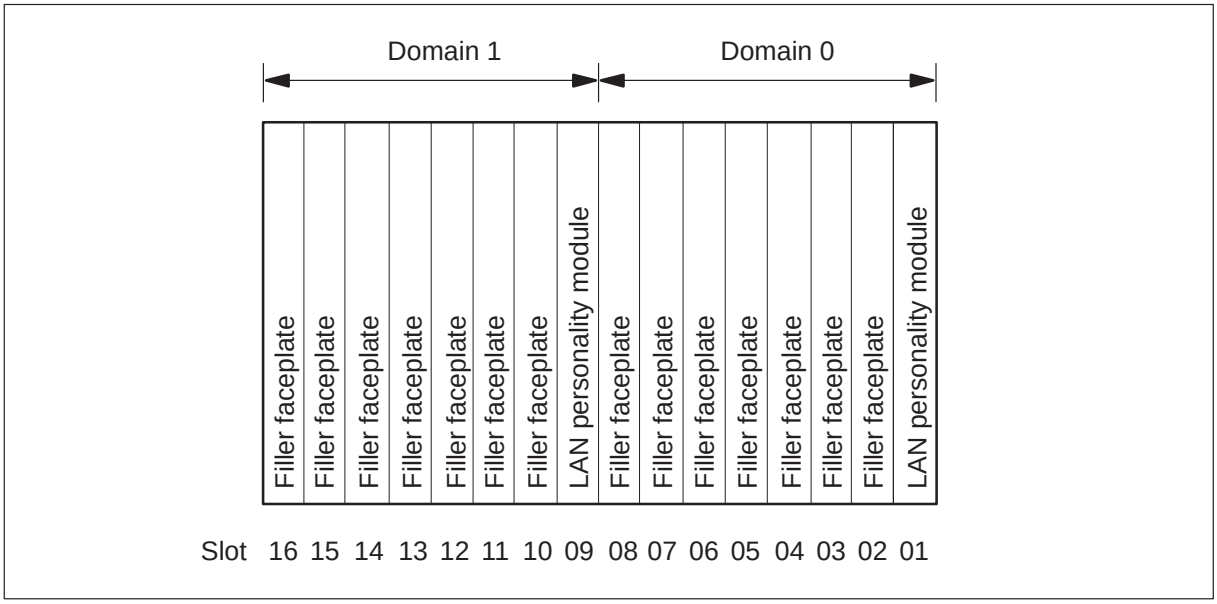


Figure 1-14 identifies the slot numbers contained in domain 0 and domain 1, and the provisionable LAN personality modules in each slot number, as shown in figure 1-13.

Note: Provisionable personalty modules in the I/O expansion chassis are not restricted to specific slot numbers. The LAN personality module shown in figure 1-13 can be mounted in any two slots, providing the slot numbers correspond in each domain, and match the slot numbers of the corresponding controller module that mounts at the front of the I/O expansion chassis. (For more information on slot numbers, see page 1-7.)

Figure 1-14
Rear view of the I/O expansion chassis by slot number



Additional provisionable hardware

This section describes additional provisionable hardware that can be mounted at the front of the main chassis or the I/O expansion chassis. These controller modules are not restricted to designated slot numbers, however, corresponding slot numbers must be used for each domain to achieve fault-tolerant operation.

Note: The SDM must be equipped with a pair of NTRX50GN or NTRX50FQ I/O controller modules. The capacity of rootvg may be extended by replacing NTRX50FQ modules with NTRX50GN modules. Rootvg cannot be extended by adding more modules.

I/O controller module (NTRX50FU)

The NTRX50FU I/O controller module provides two 2-Gbyte DDUs with Ethernet interfaces and 4 Gbyte of mirrored datavg capacity. To operate the NTRX50FU module, a LAN personality module (NTRX50FS) must be mounted in the corresponding slot number at the back of the chassis.

The NTRX50FU module can be used in addition to the NTRX50FQ and NTRX50GP modules. Datavg may be expanded by up to 16 Gbyte without service interruption, by adding NTRX50FU modules in pairs. The NTRX50FU modules may be mounted in any two corresponding slots in each domain of the main or I/O expansion chassis.

Note: The Ethernet interface on NTRX50FU I/O controller modules is not supported in this release.

I/O controller module (NTRX50GN)

The NTRX50GN I/O controller module provides a 3.5 in. 4-Gbyte DDU, a DAT drive, and an Ethernet interface. The disk drive is assigned to rootvg at installation. The AIX operating system, the SDM base, service and application software, and data are stored in rootvg.

The DAT drive is used for the following:

- installation of SDM software
- software restore in the event of corruption or disk failure
- performing software backups of rootvg

The NTRX50GN module mounts in slots 2 and 3, and 13 and 14, of the main chassis. To operate this module, a LAN personality module (NTRX50FS) must be mounted in slots 2 and 13 at the back of the main chassis.

Note: Nortel does not recommend using the NTRX50GN module when additional modules (NTRX50FU or NTRX50GP) are provisioned for datavg. Use the NTRX50FQ I/O controller module if the system is equipped with additional datavg modules.

I/O controller module (NTRX50GP)

The NTRX50GP I/O controller module provides two 4-Gbyte DDUs with Ethernet interfaces. The DDU is used for application data. The I/O controller module is always provisioned in pairs and occupies two slots in each I/O domain to extend the mirrored datavg capacity by 8-Gbyte. To operate the NTRX50GP module, a LAN personality module (NTRX50FS) must be mounted in the corresponding slot number at the back of the chassis.

Note: The Ethernet interface on NTRX50GP I/O controller modules is not supported in this release.

The NTRX50GP module can be used in addition to the NTRX50FQ module, depending on system requirements. The following examples outline different provisioning scenarios:

- Use a pair of NTRX50FQ modules with a pair of NTRX50GP modules to provide 2 Gbyte of rootvg and 8 Gbyte of datavg.

- Use a pair of both the NTRX50GP and NTRX50FU I/O controller modules with a pair of the NTRX50FQ modules to provide 12 Gbyte of datavg and 2 Gbyte of rootvg. (The NTRX50FQ modules mount in slots 2 and 3, and 13 and 14, at the front of the main chassis. The NTRX50FU or the NTRX50GP modules can mount in the main chassis in any two corresponding slots in each domain. An I/O expansion chassis is required to house the remaining pair of I/O controller modules. These modules must mount in the corresponding slot number in each domain.)
- Use two pairs of NTRX50GP I/O modules with a pair of NTRX50FQ modules to provide 16 Gbyte of datavg and 2 Gbyte of rootvg. This configuration is the maximum capacity for datavg. (An I/O expansion chassis is required for one pair of NTRX50GP I/O controller modules.)

CPU controller module (NTRX50FL, NTRX50FM)

The CPU controller module consists of a 256-Mbyte (NTRX50FL) or a 512-Mbyte memory option (NTRX50FM). It contains the main processing power and memory capacity of the SDM. Minimally, the SDM requires a 128-Mbyte CPU controller module (NTRX50FK). If a memory upgrade is required, the module with increased memory replaces the old one.

The CPU controller module mounts in slots 6 and 7, and 10 and 11, at the front of the main chassis. Each module plugs into the backplane of the main chassis through P1 and P2 connectors. The CPU controller module is used in conjunction with the CPU personality module (NTRX50FD), which is located in slot 6 at the back of the main chassis of the SDM. The CPU personality module provides console port connections to the CPU controllers.

SDM software

SDM software has a three-layer architecture composed of separate base, service, and application layers. This organization permits parallel development in each stream, allowing independent delivery of new services and applications, as well as interim delivery of any maintenance release software.

The SDM base software layer is responsible for the maintenance and operation of the SDM. The service layer provides common software utilities and functions that can be used by multiple SDM applications. The application software layer provides applications that address DMS switch operations, administration, maintenance and provisioning (OAM&P).

SDM base software layer

The SDM base software layer consists of the following:

- the AIX 4.1.4 operating system (the proprietary IBM implementation of UNIX) and server software
- node and process control services
- maintenance and administration services

SDM service software layer

The service software layer provides internal application support software for use by current and future SDM application packages. The service software layer consists of the following:

- table access utilities allowing SDM applications to manipulate tables maintained on the CM
- remote procedure calls (RPC) allowing CM software to raise RPCs to SDM software. RPCs allow a program running on one host to request and receive a message containing results of a service on another host.
- Open Software Foundation (OSF) Distributed Computing Environment (DCE) to provide authentication and authorization mechanisms to ensure network security
- operational measurement (OM) collection and application programming interface (API) allowing SDM applications to receive OM data from the CM

SDM application software layer

The application software layer contains operations, administration, and maintenance software application packages. This layer contains all SDM application software installed on your system, including the Log Delivery application, and the optional Exception Reporting (ER), Enhanced Terminal Access (ETA) and SuperNode Billing Application (SBA) applications.

For information on the Log Delivery application, see page 1-27. For information on optional SDM applications, refer to the following Northern Telecom Publications (NTPs):

- *SuperNode Data Manager Exception Reporting User Guide*
- *SuperNode Data Manager Enhanced Terminal Access User Guide*
- *SuperNode Data Manager SuperNode Billing Application Application Guide*

Maintenance interfaces

There are two maintenance interfaces for the SDM:

- the MAP, accessed from the CM

- the RMI, accessed from the SDM

The MAP is the primary access point for maintenance activities. The RMI is the secondary access point for maintenance activities. Maintenance activities must be initially performed at the MAP interface. When connectivity to the CM is not available, the RMI provides access to all maintenance activities that would normally be performed at the MAP interface.

MAP-based SDM maintenance

A dedicated SDM maintenance subsystem is provided at the MTC PM level of the MAP display which allows you to do the following:

- determine the node state and operating condition of the SDM
- alter the state of the SDM for maintenance purposes
- determine the status of connectivity to the SDM
- reboot or halt the SDM
- determine the status of SDM applications, including any faults currently affecting applications, by using the QuerySDM command (See the "SDM maintenance overview" chapter for more information.)
- determine the status of the SDM operating system, including any faults currently affecting system software resources, by using the QuerySDM command. (See the "SDM maintenance overview" chapter for more information.)

The MAP display is used to maintain the SDM if the CM is communicating successfully with the SDM. If the SDM and the CM are unable to communicate due to a fault on the SDM, the RMI must be used to diagnose and clear the problem.

See "Maintaining the SDM using the MAP interface" on page 2-2 for an overview of MAP-based maintenance capabilities.

RMI-based SDM maintenance

The RMI can be accessed by the following methods:

- using a remote or local VT100 terminal console port
- telneting from the operating company LAN (telnet must be enabled)
- using the optional ETA application from a remote workstation (telnet must be disabled)

The RMI provides the following maintenance capabilities:

- access to all maintenance capabilities which would normally be available through the MAP interface, including state change and monitoring capabilities, when connectivity to the CM is not available
- control of individual SDM application software packages
- control and maintenance of hardware

For full details on the capabilities provided on the RMI, see ”Maintaining the SDM using the remote maintenance interface” on page 2-34.

Administration functions

SDM administration is performed by root and maintenance (maint) users, primarily using UNIX-based utilities at a local or remote VT100 console, and tools available at the RMI. Administration capabilities supported through this interface include commissioning of the SDM fault-tolerant platform, commissioning of the Log Delivery application, setup of user groups (root and maint) and passwords, monitoring system resources, and performing software backup and restore functions.

Disk partitioning

The AIX operating system provides disk partitioning capability into logical volumes. Logical volume partitioning provides protection against disk occupancy errors (full disk), allowing the system to read from and write to the remaining disks without interruption.

On the SDM, logical volumes are equivalent to file systems. The SDM file system structure is provisioned by Nortel. The root user can only monitor file system partitioning and usage using the RMI or the MAP display at the local or remote VT100 terminal. The root user cannot modify logical volumes.

For additional information on administering the SDM, see the “System administration overview” and the “System administration procedures” chapters of this document.

LAN-based I/O interface capabilities

LAN-based I/O interfaces are supported on the SDM to the following types of equipment:

- workstations
- hubs
- routers
- terminal servers

Each of these interface types is discussed in the following subsections.

Workstations

UNIX workstations can be configured as remote user interface (UI) clients to provide the UI for the SDM applications. For this product release, UI clients are supported on the following workstations with the appropriate DCE client software (OSF DCE version 1.01):

- HP-700 series workstations running the HP-UX 9.05 operating system (or higher)
- Sun SPARC workstations running Solaris 2.4 or later

UI client performance depends on workstation performance.

Hubs

Hubs are required when 10BASE-T or unshielded twisted pair (UTP) LANs are used. The minimum requirements for a customer-supplied hub connected to the SDM are as follows:

- compliance with IEEE 802.3/Ethernet 10BASE-T specifications
- internal self-test, diagnostics, and configuration available from a locally attached terminal or through the Simple Network Management Protocol (SNMP) over the LAN
- compliance with the Address Resolution Protocol (ARP) broadcast refinement
- auto segmentation to prevent babbling or erroneous ports from affecting the operation of the LAN
- support for cascading hubs to expand the LAN
- visual indicators of the LAN status

Routers

Routers perform wide area networking for SDM graphical user interfaces (GUIs) over other networks, and provide gateway (or protocol translator) functions.

The minimum requirements for a customer-supplied router used in a configuration connected to the SDM are as follows:

- compliance with IEEE 802.3/Ethernet 10BASE-T specifications
- internal self-test, diagnostics, and configuration available from a locally attached terminal or through the SNMP over the LAN
- compliance with the ARP broadcast refinement
- support for a variety of WAN communication facilities (asynchronous transfer mode [ATM], and channel service unit [CSU]/data service unit [DSU])
- visual indicators of LAN and port status and connectivity

Terminal servers

A terminal server can be used to provide asynchronous access to the SDM. Terminal server ports can either be used instead of integrated asynchronous application ports or can be provisioned in addition to the integrated ports. The number of required asynchronous ports is determined by the engineering rules associated with each application.

The minimum requirements for a terminal server used with the SDM are as follows:

- compliance with IEEE 802.3/Ethernet 10BASE-T specifications
- telnet and TCP/IP support
- internal self-test, diagnostics, and configuration available from a locally attached terminal or through the SNMP over the LAN
- compliance with the ARP broadcast refinement
- visual indicators of LAN and port status
- capability to configure terminal servers through a locally attached terminal (preferred)
- full modem support for dial-up applications
- port speeds of up to 64 kbit/s
- point-to-point protocol availability

SDM Log Delivery

The Log Delivery application, included as part of the base software platform on the SDM, delivers user-defined streams of DMS SuperNode logs and SDM fault-tolerant platform and application logs to one or more of the following:

- up to 10 operations support systems (OSS), by TCP/IP links from the SDM to the operating company LAN

- up to 10 UNIX files stored on the SDM

A maximum of 10 Log Delivery output devices can be commissioned (the sum total of TCP/IP links and UNIX files cannot exceed 10).

The Log Delivery application cannot be used to deliver logs generated by DMS SuperNode processors other than the CM and the SDM. Logs from other processor types may continue to be delivered by the standard input output controller (IOC) log devices by datafilling a valid IOC log device name for each required processor type in table RLOGDEV. Currently defined processor types unsupported by SDM Log Delivery are as follows:

- message switch (MS)
- CCS7 link interface unit (LIU7)
- frame relay interface unit (FRIU)
- Ethernet interface unit (EIU)
- link interface module (LIM)
- enhanced network (ENET)
- application processor (AP)
- file processor (FP)
- X.25, X.75 link interface unit (XLIU)
- auxiliary processing unit (APU)
- GSM (global system for mobile communications) processor (GSMP)
- voice processing unit (VPU)
- high-speed link interface unit (HLIU)
- network interface unit (NIU)
- high-speed link router (HSLR)
- Ethernet link interface unit (ELIU)
- CDMA (code division multiple access) application unit (CAU)
- CDMA interface unit (CIU)
- cellular authentication and voice privacy unit (CAVU)
- A-interface control element (ACE)

Logreceiver tool

The logreceiver tool is a client application, included with the Log Delivery application, which runs on a remote workstation and receive logs sent to the workstation from an SDM by the operating company LAN. The logreceiver tool can either store these logs in a file, or display them on the screen. Only

HP 700/800 workstations running HP-UX 9.05 or later can be used to run logreceiver in this release.

To route logs from an SDM to a workstation, the SDM must be configured to send logs to a TCP device whose IP address is the IP address of the workstation using the logroute commissioning tool. (For more information, see ”Commissioning TCP client devices for Log Delivery” on page 2-88).

Refer to the procedure ”Installing the logreceiver tool” on page 6-93 in the “SDM system administration procedures” chapter of this document for detailed instructions on how to install the logreceiver tool on a workstation.

Log formatting

The Log Delivery application can format logs using Nortel standard (STD) or Switching Control Center 2 (SCC2). Logs in STD format specify the switch name, and if configured, the node (SDM) name. Logs in SCC2 format do not specify the switch or node name. Formatting can be set on a per-device basis.

Log buffering

In the event that any destination device is unable to receive logs for any reason, logs are buffered locally on the SDM until the device is ready to receive logs. The default buffer size is 150. The buffer size can be modified, using the Log Delivery commissioning tool. The buffer size must be at least 50 and cannot exceed 300.

Log delivery commissioning tool (logroute)

Log Delivery operating parameters are controlled by an online SDM commissioning tool, which is used to set up the parameter values, and can also be used to view or modify these values.

ATTENTION

You must busy and return the Log Delivery application to service to make new changes changes take affect. An interruption in log routing to all currently active devices will result. Any logs buffered for delivery to these devices will be lost during this operation.

ATTENTION

There is no locking mechanism on the logroute tool. Therefore, the logroute tool must only be run by one user at a time. Otherwise, changes made by one user may overwrite those of another user.

The Log Delivery commissioning tool allows customization of the following:

- global application parameters including buffer size, reconnect timeout value, lost logs threshold, ASCII line delimiter and log delimiter characters, and the number of days to keep log files
- the incoming log stream from the CM, to add or delete individual logs or log types
- output device list, including device type (UNIX file or TCP output), parameters specific to the device type, log output format (STD or SCC2) and the logs or log types to be sent to the device

The Log Delivery commissioning tool includes an online help facility that provides the valid ranges (and default values, where applicable) for each customizable parameter.

For additional information on configuring and troubleshooting the Log Delivery application, see page 2-82.

SDM maintenance overview

This chapter is an overview of the fault-tolerant SDM maintenance capabilities and methods.

”SDM monitoring and maintenance positions” on page 2-1 describes the user interfaces and output devices from which you can monitor and maintain the SDM. These include the CM MAP interface, the SDM remote maintenance interface (RMI), and the DMS log stream.

”SDM Log Delivery applications” on page 2-82 describes the SDM Log Delivery application and provides commissioning and troubleshooting guidelines.

”SDM troubleshooting strategy” on page 2-93 provides recommendations for isolating and clearing faults on the SDM fault-tolerant platform.

”Routine maintenance recommendations” on page 2-105 lists routine maintenance activities.

SDM monitoring and maintenance positions

Information about the state of the SDM is available from the following monitoring and maintenance positions:

- maintenance level of the MAP interface. See ”Maintaining the SDM using the MAP interface” on page 2-2.
- SDM remote maintenance interface. See ”Maintaining the SDM using the remote maintenance interface” on page 2-34.
- log streams. See ”SDM log reports” on page 2-78.
  - — from the SDM to an operations support system (OSS) or UNIX file using the SDM Log Delivery application. See page 1-27 for additional information.

Each of these maintenance access points is described in the following sections.

Maintaining the SDM using the MAP interface

The primary access point for maintaining the SDM is the application (APPL) subsystem of the MAP interface. The MAP command and display structure for the SDM is similar to that provided at other MAP levels. Commands at the SDM level allow you to do the following:

- monitor and alter the state of the SDM
- determine the state of the DS512 interface associated with the SDM
- query status information on the SDM system, application software, and hardware location
- provide access to the Platform sublevel to monitor and alter the state of the SDM devices

You can use the MAP interface to maintain the SDM. However, at least one of the communication links between the computing module (CM) and the SDM must be in service. If all of the links are out of service, the SDM is isolated and maintenance must be performed using the RMI, described on page 2-34.

Figure 2-1 shows an example of the SDM level of the MAP display. The display shows the SDM status, the number of links out of service, any current maintenance actions, and provides an SDM-specific command set. Fault conditions related to the SDM are reported in the alarm banner. In this example, the SDM is InSv. Using the command set provided, you can obtain additional details about the condition of the SDM to isolate and resolve faults.

Figure 2-1
SDM MAP level

Note: The above screen is an example of the SDM Map level for a North American product.

Determining the SDM node state at the MAP display

The following table lists and describes the SDM node states that are available on the MAP display at the SDM level. The MAP alarm banner indicator associated with each state is listed.

Table 2-1
SDM node state indicators at the SDM MAP level

SDM state at the MAP interface	Associated APPL banner alarm	Associated SDM banner alarm	Meaning of the state
InSv	APPL .	SDM .	No alarms are present. The SDM is in the in service (InSv) state. The SDM, its applications, and hardware devices are running normally without faults, and the CM and the SDM are communicating successfully.
OffL	APPL .	SDM .	No alarms are present. The SDM is in the off-line (OffL) state. In the OffL state, the CM and the SDM are not communicating, and no applications are running. The SDM is automatically designated as off-line when datafilled for the first time. It can also be set to the off-line state from the manual busy (ManB) state by the OffL command at the MAP interface.

—continued—

Table 2-1
SDM node state indicators at the SDM MAP level (continued)

SDM state at the MAP interface	Associated APPL banner alarm	Associated SDM banner alarm	Meaning of the state
ISTb	APPL SDM	SDM ISTb	An APPL SDM minor alarm is present. The CM is receiving in-service trouble (ISTb) status from the SDM. One or more of the following conditions may exist: • One or more SDM applications cannot run, but at least one application is running successfully. • The SDM cannot communicate with one or more of the operating company LAN nodes defined on the SDM. • A software resource threshold has been exceeded. • An automated incremental software backup has failed. • An SDM application has reported an ISTb condition. • A non-critical hardware fault is present. • At least one, but not all, DS512 links are out of service. • The SDM has been declared a minor babbler by the MS. The SDM is sending too much information before receiving acknowledgements. See page 2-12 for more information. • Disk mirroring is in progress or has failed. • There is an IP mismatch between the CM and the SDM. • A file system has exceeded its alarm threshold or any volume group is not InSv. • There is a fault with Distributed Computing Environment (DCE).

—continued—

Table 2-1
SDM node state indicators at the SDM MAP level (continued)

SDM state at the MAP interface	Associated APPL banner alarm	Associated SDM banner alarm	Meaning of the state
ManB	APPL SDM	SDM ManB	An APPL SDM minor alarm is present. The SDM has been manually busied (ManB) by command at the MAP interface.
ManB (NA)	APPL SDM	SDM ManB	An APPL SDM minor alarm is present. The SDM has been manually busied by command at the MAP interface. The CM cannot communicate with the SDM because the DS512 ports on the MS are unavailable. The operating condition and local state of the SDM are unknown to the CM. This is the case until at least one of the DS512 links is restored.
ManB/The SDM is not responding	APPL SDM	SDM ManB	An APPL SDM minor alarm is present. The SDM has been manually busied by command at the MAP interface. The CM is not receiving messages from the SDM. The operating condition and local state of the SDM are unknown to the CM until communications with the SDM are restored.
SysB	APPL SDM *C*	SDM SysB *C*	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system busy (SysB). One or more of the following conditions exist: • The CM is receiving system-busy status from the SDM. • The SDM is a major or critical babbler. The SDM is sending too much information before receiving acknowledgements. See page 2-12 for more information. • All software applications on the SDM have failed.

—continued—

Table 2-1
SDM node state indicators at the SDM MAP level (continued)

SDM state at the MAP interface	Associated APPL banner alarm	Associated SDM banner alarm	Meaning of the state
SysB (NA)	APPL SDM *C*	SDM SysB *C*	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system busy (SysB). The CM cannot communicate with the SDM because the DS512 ports on the MS are unavailable. The operating condition and local state of the SDM are unknown to the CM. This is the case until at least one of the DS512 links is restored.
SysB/The SDM is not responding	APPL SDM *C*	SDM SysB *C*	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system busy (SysB). The SDM node state can be SysB for the following reasons: • Communication links between the CM and the SDM are not operating. The operating condition and local state of the SDM are unknown to the CM until communications with the SDM are restored. • The SDM has been powered down or is rebooting after being powered down.
Note: The SysB state is reported as an APPL SDM critical alarm. ISTb and ManB states are reported as an APPL SDM minor alarm.			
—end—			

Note 1: The loss of a DS512 link will not change the SDM node state unless all the DS512 links are down.

Using SDM commands at the MAP display

The SDM MAP display is accessed at the SDM level of the MTC APPL level. The following commands are provided at the SDM MAP level:

- Quit is the standard SDM level menu command used to exit the current MAP level.
- Trnsl displays the link address information for the links between the MS and the SDM. See ”Using the Trnsl command” on page 2-8 for more information.
- Bsy sets the SDM to manual busy (ManB) state. See ”Using the Bsy command” on page 2-9 for more information.

- RTS returns the SDM to service from manual busy (ManB) state. See ”Using the RTS command” on page 2-10 for more information.
- OffL sets the SDM to offline (OffL) state from manual busy (ManB) state. Executing the OffL command disables communications between the CM and SDM.
- QuerySDM provides a variety of information about the status and configuration of the SDM. See ”Using the QuerySDM command” on page 2-11 for more information.
- Locate provides a list of hardware modules installed on the SDM and their physical location. See ”Using the Locate command” on page 2-12 for more information.
- Platform provides access to the SDM platform level for SDM device-level fault isolation and resolution functions. See ”Using the Platform command” on page 2-13 for more information.
- RebootSDM is a non-menu command that reboots the SDM. See ”Using the ReBootSDM command” on page 2-15 for more information.
- HaltSDM is a non-menu command that halts the SDM. See ”Using the HaltSDM command” on page 2-15 for more information.
- SDMRLogin is a non-menu command that allows you to log in to the SDM from the CM. See ”Using the SDMRLogin command” on page 2-16 for more information.

Using the Trnsl command

Trnsl displays the link address information for the DS512 links between the MS and the SDM. When Trnsl is executed, the following information is displayed:

- the SDM number, domain, and port
- the MS number, card, and port
- the link status and messaging condition
- whether C-side (MS) or P-side (SDM node control) actions are in progress

Using the Bsy command

Bsy sets the SDM to manual busy (ManB) state. The system response to the Bsy command depends on the status of the communication link between the CM and the SDM:

- If the CM and the SDM are communicating successfully, the CM sends the Bsy command to the SDM. If the SDM is in service, you receive a yes/no prompt. This indicates that executing the Bsy command causes a service interruption (all applications running on the SDM shut down). Executing the command changes the state of the SDM at the MAP display to ManB, changes the local state of the SDM (as it appears on the RMI) to ManB, and shuts down all SDM applications.
- If the CM and the SDM are not communicating, the CM cannot send the Bsy command to the SDM. The CM view of the SDM state (as it appears at the MAP display) changes to ManB (NA) or ManB/The SDM is not responding. This state depends on the reason for the communication problem. The local state of the SDM (as it appears at the RMI) and its operating condition are unaffected by the Bsy command. However, when CM-SDM communications are restored, the SDM aligns to the current CM view of its state.

  You can set the local state of the SDM to ManB when the CM and the SDM are not communicating. However, the Bsy command must be executed at the RMI, which shuts down any applications that are running.

- When the SDM is in OffL state, the CM sets the SDM state to ManB and enables CM-SDM communication. The CM then sends the Bsy command to the SDM.

The Bsy command has the options Force and Nowait. The Bsy command with the Force option overrides the following commands that are in progress:

- RTS
- RTS Force
- Bsy

The Nowait option is the standard DMS MTC command parameter used to return command entry capability immediately. That is, you can continue to enter other commands while the system is executing the Bsy command. Refer to logs output to determine the progress of the Nowait option.

Using the RTS command

RTS returns the SDM to service from manual busy state. The system response to this command depends on the status of the communication link between the CM and the SDM:

- If the CM and the SDM are communicating successfully, the CM sends the RTS command to the SDM. If the command executes successfully, the SDM is returned to service. If there are no faults on the SDM, the state of the SDM changes to InSv at the MAP interface, and at the RMI. If one or more applications on the SDM are not running, the SDM state is ISTb.
- If the CM and the SDM are not communicating, the CM cannot send the RTS command to the SDM. The CM view of the SDM state (as it appears at the MAP display) changes to SysB (NA) or SysB/The SDM is not responding. The state depends on the reason for the communication problem. The local state of the SDM (at the RMI) and its operating condition are unaffected by the RTS command. However, when CM-SDM communications are restored, the SDM aligns to the current CM view of its state.
- To perform a local return-to-service of the SDM when CM-SDM communications are down, the RTS command must be executed at the RMI.

The RTS command has the options Force and Nowait. The Force option invokes a forced return-to-service of SDM applications. Use the Force option with caution. It ensures the state change takes place, however, all errors (IP mismatch) are ignored and checks are bypassed. The Nowait option is the standard DMS MTC command parameter used to return command entry capability immediately. That is, you can continue to enter other commands while the system is executing the RTS command. Refer to logs output to determine the progress of the Nowait option.

ATTENTION

When the SDM or one of its applications or services is returned to service from a manual busy (ManB) state, the state of the SDM may move to in-service (InSV) briefly, then to in-service-trouble (ISTb) for a few minutes, and finally back to InSv.

The ISTb state is the result of the application not being fully capable of supplying service during initialization. For example, if the Operations Measurements application is not yet InSv, the Exception Reporting application will be ISTb.

Using the QuerySDM command

QuerySDM provides information about the SDM, as follows:

- QuerySDM with no additional parameters displays the status of the SDM as seen from the MAP display, its IP address on the CM side, and its physical location as defined in table SDMINV. The slot number is always blank. This information is displayed regardless of the state of the CM-SDM communication link.
- If there are no faults on the SDM, and the SDM is in service, QuerySDM displays the message ”No local SDM fault to report”.
- QuerySDM FLT displays any information on SDM software and device faults. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning. Stopped processes are not displayed when the node is in ManB state. The following information is included for device faults:
  - — the faulty component
  - — time stamp of the last SDM state change
  - — the faulty module, its product engineering code (PEC), and location
  - — other devices on the faulty module and their state
  - — reason text that describes the fault (if available)
- QuerySDM LOADS displays the version and status of software installed on the SDM. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning.
- QuerySDM STATUS displays local SDM alarms (LAN connectivity, CM connectivity, application software, and system software). QuerySDM STATUS also shows all devices on the SDM, and their states. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning.
- QuerySDM CONFIG displays configuration data (platform type, connectivity information, operating company LAN configurations, and system threshold values) related to the SDM. This information is obtained directly from the SDM and is only displayed if the CM-SDM communication link is functioning.

Error messages for QuerySDM with the FLT, LOADS, CONFIG, or STATUS options are generated for the following reasons:

- The request to the SDM cannot be sent because there are no available DS512 links.
- The CM timed out before the command complete message was received from the SDM.
- The SDM is not responding.

- The SDM is in the OffL or unequipped state.
- Messages could not be sent to the SDM for the following reasons:
  - — The node maintenance process could not obtain a CM-side message transport service (MTS) endpoint.
  - — The node maintenance process could not obtain an SDM-side MTS endpoint.
- The maximum number of simultaneous SDM commands has been exceeded. Try the command later.
- An unexpected software error was encountered.

In addition, error messages are generated for QuerySDM FLT for the following reasons:

- The MS has indicated that the SDM is a minor, major, or critical babbler. That is, the SDM node is sending too much information before receiving acknowledgements:
  - — When the MS indicates that the SDM is a minor babbler, the state of the SDM on the CM is set to ISTb. An APPL SDM minor alarm is generated. Refer to the procedure, "Clearing MAP alarms triggered by the SDM - APPL SDM minor" on page 4-3.
  - — When the MS indicates that the SDM is a major babbler, the state of the SDM on the CM is set to SysB. All links are maintenance open. Applications can no longer communicate between the SDM and the CM. An APPL SDM critical alarm is generated. Refer to the procedure, "Clearing MAP alarms triggered by the SDM - APPL critical" on page 4-29.
  - — When the MS indicates that the SDM is a critical babbler, the state of the SDM on the CM is set to SysB. All links are closed. Applications can no longer communicate between the SDM and the CM. An APPL SDM critical alarm is generated. Refer to the procedure, "Clearing MAP alarms triggered by the SDM - APPL SDM critical" on page 4-29.

Using the Locate command

Locate displays location information about the SDM hardware modules and the devices they support. The following information is displayed when this command is executed:

- the type of module, its location (including chassis and slot number), and PEC
- devices on the module

The SDM must be in ManB or higher (InSv, SysB or ISTb) state to execute this command successfully. The Locate command can only be used if the CM-SDM communication link is up. Error messages are displayed for the following reasons:

- There is no communication route to send the locate request to the SDM.
- The CM has timed out before receiving a command complete message from the SDM.
- The SDM is not responding.
- The SDM is in the OffL or unequipped state.
- Messages could not be sent to the SDM for the following reasons:
  - — The node maintenance process could not obtain a CM-side MTS endpoint.
  - — The node maintenance process could not obtain an SDM-side MTS endpoint.
- The maximum number of simultaneous SDM commands has been exceeded. Try the command later.
- An unexpected software error was encountered.

Using the Platform command

Platform displays state information on the SDM software components, hardware modules, and devices. The following information is displayed when this command is executed:

- SDM application and software state (APPL)
- SDM LAN connectivity state (LAN)
- SDM system software state (SYS)
- CM connectivity state (CON)
- hardware device states. A state is displayed for a hardware device on domain 0 (D0) and domain 1 (D1).

The Platform command can only be used if the CM-SDM communication link is up. Error messages are displayed if the CM-SDM communication link is down or the Platform MAP level could not be allocated.

The following commands are available from the Platform level:

- QUIT is the standard menu command used to exit the current MAP level.
- TRNSL displays information on the state of the CM to SDM connecting links. When Trnsl is executed, the following information is displayed:

— the SDM number, domain, and port

— the MS number, card, and port

— the link status and messaging condition

— whether C-side (MS) or P-side (SDM node control) actions are in progress

- BSY is a menu command that sets the requested SDM hardware device to a manual busy (ManB) state. The command has one optional parameter:

  — The FORCE option is the standard DMS MTC command parameter used to force the state change. Force works even if the change will cause a service outage. Use the Force option with caution. It ensures the state change takes place, however, all errors (IP mismatch) are ignored and checks are bypassed.

CAUTION
Possible service interruption
Using the FORCE option with the BSY command may cause a possible service interruption. BSY with the FORCE option overrides any commands in progress.

Error messages for BSY with the FORCE option are generated for the following reasons:

- The command could not be executed because of lack of SDM resources.
- The CM timed out before the command complete message was received from the SDM.
- Execution of the command was canceled because the user chose abort or a negative response to a confirmation prompt.
- The hardware device is already in a ManB state.
- The command could not be executed due to an abnormal condition or because communications with the SDM are down. The reason is described by one of the following error messages:

  — The SDM is Unequipped

  — The SDM is OFFL

  — No communication route to the SDM

  — No SDM C-side MTS address

  — No SDM P-side MTS address

  — Software error encountered

— The SDM is not responding

— Maximum number of SDM command users exceeded

- RTS is a menu command that returns the requested hardware device to service from a manual busy (ManB) state.
- The QuerySDM command provides a variety of information about the status and configuration of the SDM. See ”Using the QuerySDM command” on page 2-11 for more information.
- Locate provides a list of modules and devices installed on the SDM and their physical location. See ”Using the Locate command” on page 2-12 for more information.

Using the RebootSDM command

RebootSDM is a non-menu command that is used to reboot the SDM. It can only be executed if the node state is ManB and the links are available.

CAUTION

Reboot message

When a RebootSDM command is issued, the following message may appear on the SDM’s local console during the reboot:

```
Board Configuration Data Failure
```

Ignore this message. It is not service-affecting.

Using the HaltSDM command

HaltSDM is an unlisted menu command that halts the SDM. It can only be executed if the node state is ManB and the links are available.

CAUTION

Possible loss of service

If the RebootSDM or HaltSDM command is used on an SDM/FT system while there is a loss of power to the ICM on D0 of the main chassis (ICM 0), the system will not recover from the reboot. A loss of power can be caused by the removal of the power cable, turning off the circuit breaker in the MSP, or a faulty ICM 0. Restore power to ICM 0 and perform a reboot.

Using the SDMRLogin command

SDMRLogin is a non-menu command that allows root and maint (maintenance) users to log in to the SDM from any MAP level. Maintenance users are only allowed to perform surveillance and maintenance activities. They must not alter or create new files.

ATTENTION

Log in as the root user only when the procedure you are performing requires it. Otherwise, log in as a maint user. If you are logged in as the root user, use caution when copying, storing, or removing any files on the SDM.

Copying and storing files in a logical volume, or removing files from a logical volume, may cause the SDM to fail.

ATTENTION

Executing an SDMRLogin session from the CM to the SDM as the root user puts you in a restricted shell and does not allow root privileges. SDMRLogin is used to perform local maintenance activities. If you need to perform other operations that require root user privileges, log in to the SDM as the root user.

The SDM must be in InSv or ISTb state to execute the SDMRLogin command. When the SDMRLogin command is invoked, you are prompted for your userID, as follows:

```
SDM Remote Login command in progress.  Please wait...

telnet (sdm123)
AIX Version 4
(C) Coprights by IBM and by others 1982, 1994.
login:
```

You are prompted for your password. The screen then displays the number of unsuccessful login attempts since your last login, and your last unsuccessful login attempts.

```
Password:
************************************************************
**                                                        **
**               This is a private database.              **
**         All activity is subject to monitoring.         **
**     Any UNAUTHORIZED ACCESS OR USE IS PROHIBITED.      **
**                                                        **
************************************************************
Last unsuccessful login: Sat Apr 12 16:45:20 EDT 1997 on /dev/pts
/4 from 47.208.11.94
Last login: Mon Apr 14 11:46:41 EDT 1997 on /dev/pts/4 from cm

SDM>
```

Note 2: Although password beginning with a numeric character are valid on the SDM, they cannot currently be used following SDMRLogin.

Note 3: The UNIX shell prompt must not be modified during an SDM remote login session. If the prompt is modified, the remote login session will hang, and must be terminated using the BREAK<hx> command.

You are automatically placed in a restricted shell. Type “help” to display a command list. The commands available during an SDMRLogin session are as follows:

bsyapp followed by the application number, moves an application into the ManB state.

bsyhw followed by the domain number (0 or 1), and the device name, moves a hardware module to the ManB state. The bsyhw command can also be used with the FORCE option.

help displays help for commands for the SDMRLogin session. Type HELP for a list of all commands. Type HELP, followed by a command name, for help on a specific command.

rtshw followed by the domain number (0 or 1), and the device name, returns a hardware module to the InSv state.

rtsapp followed by the application number, returns an application to the InSv state.

offlapp followed by the application number, moves an application to the OffL state from the ManB state.

locate displays location information on SDM hardware modules, and the devices they support.

querySDM with no parameters, displays the status of the SDM, and the number of out-of-service links. QuerySDM FLT displays information on SDM software and device faults. QuerySDM LOADS displays software

versions installed on the SDM, and their current states. QuerySDM STATUS displays information on system software connectivity, including applications and devices, and their states. QuerySDM CONFIG displays configuration data related to the SDM.

logout logs you out of the SDM.

ls lists the commands available from the SDM Remote Login directory.

ping followed by the name or IP address of a network host confirms SDM LAN connectivity to the network host. For example, ping cm confirms connectivity to the CM.

ps reports UNIX process status.

who displays users logged on to the SDM.

who_is_on indicates the number of users logged in to the SDM, the number of users logged on the maintenance menu system, and the state of the SDM.

Enter the Logout command to end the remote login session. Entering the logout command returns you to the same MAP level from which you entered the SDMRLogin command. If you enter the Ctrl-b<hx> command, you return to the command interpreter (CI) level.

Error messages are displayed for the following reasons:

- The SDM is not in the InSv or ISTb state. Put the SDM in the InSv state and reenter the SDMRLogin command.
- There are eight other SRL sessions active. The maximum number of SDMRLOGIN sessions allowed from the CM to the SDM is eight.
- The SDM has been taken out of the InSv or ISTb state during an active SDMRLogin session.
- A telnet session could not be established between the CM and the SDM.
- The terminal that you are using for the remote login does not suppress the echoing of password entries. You may continue or exit the remote login session.
- The terminal that you are using for the remote login is being used to output DMS logs. You may continue or exit the remote login session.

Monitoring SDM-related alarms at the MAP display

The MAP displays SDM alarms under the APPL header of the maintenance level alarm banner and the SDM header of the APPL level alarm banner. Figure 2-2 shows an example of an SDM alarm under the APPL header of the maintenance level alarm banner.

Note: Power-related faults on the SDM also trigger a frame supervisory panel (FSP) alarm under the external (Ext) header. The modular supervisory panel (MSP) also provides an audible alarm, and visual indications on the cabinet and at the end of the aisle.

Figure 2-2
SDM alarms on the Maintenance banner

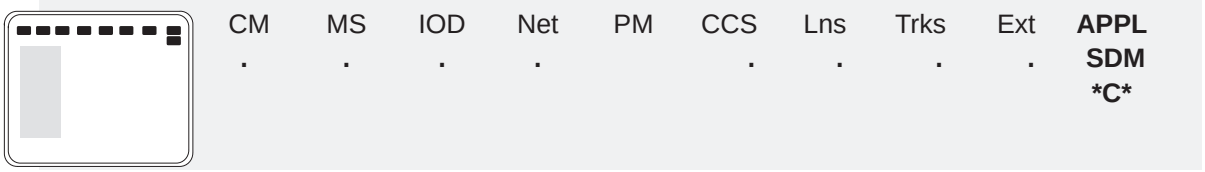


Table 2-2 lists the following various maintenance level alarm values

- alarms associated with the SDM
- SDM node states that trigger the alarms
- meaning of each combination of alarm and node state

The SDM node states appearing at the MAP display, represent the CM view of the state of the SDM. The SDM state at the MAP display is the true state of the SDM whenever the communication link between the SDM and the CM is functioning.

If the communication link between the SDM and the CM is not functioning, the operating condition and local state of the SDM are unknown to the CM. In this case, the CM designates the SDM as SysB, with a communication fault, as described in table 2-2. Under these conditions, the SDM state displayed at the MAP interface and the local node state of the SDM (as it appears on the RMI) may be mismatched.

Table 2-2
SDM alarms at the MAP alarm banners

Alarms on Maintenance banner	Associated SDM alarm in APPL banner	SDM state at the MAP interface	Meaning
APPL SDM	SDM ISTb	ISTb	An APPL SDM minor alarm is present. The CM is receiving in-service trouble (ISTb) status from the SDM. One or more of the following conditions may exist: • One or more SDM applications cannot run, but at least one application is running successfully. • The SDM cannot communicate with one or more of the operating company LAN nodes defined on the SDM. • A system software resource threshold has been exceeded. • An automated incremental software backup has failed. • An SDM application has reported an ISTb condition. • A non-critical hardware fault is present. • At least one, but not all, DS512 links are out of service. • The SDM has been declared a minor babbler by the MS. The SDM is sending too much information before receiving acknowledgements. See page 2-12 for more information. • Disk mirroring is in progress or has failed. • There is an IP mismatch between the CM and the SDM. • A file system has exceeded its alarm threshold or any volume group is not InSv. • There is a fault with Distributed Computing Environment (DCE).

—continued—

Table 2-2
SDM alarms at the MAP alarm banners (continued)

Alarms on Maintenance banner	Associated SDM alarm in APPL banner	SDM state at the MAP interface	Meaning
APPL SDM	SDM ManB	ManB	An APPL SDM minor alarm is present. The SDM has been manually busied by command at the MAP interface.
		ManB (NA)	An APPL SDM minor alarm is present. The SDM has been manually busied by command at the MAP interface. The CM cannot communicate with the SDM because the DS512 links cannot transmit or receive messages. The operating condition and local state of the SDM are unknown to the CM until at least one DS512 link is restored.
		ManB/The SDM is not responding	An APPL SDM minor alarm is present. The SDM has been manually busied by command at the MAP interface. The CM is not receiving messages from the SDM. The operating condition and local state of the SDM are unknown to the CM until communications with the SDM are restored.
APPL SDM *C*	SDM SysB *C*	SysB	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system busy. One or more of the following conditions exist: • The CM is receiving system-busy status from the SDM. • The SDM is a major or critical babbler. • All software applications on the SDM have failed.
		SysB (NA)	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system busy. The CM cannot communicate with the SDM because the DS512 interface is unavailable to transmit or receive messages. The operating condition and local state of the SDM are unknown to the CM until communications are restored.

—continued—

Table 2-2
SDM alarms at the MAP alarm banners (continued)

Alarms on Maintenance banner	Associated SDM alarm in APPL banner	SDM state at the MAP interface	Meaning
		SysB/The SDM is not responding	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system busy. The SDM node state can be SysB for the following reasons: • Communication links between the CM and the SDM are not operating. The operating condition or local state of the SDM are unknown to the CM until communications with the SDM are restored. • The SDM has been powered down or is rebooting after being powered down.
Note: The SysB state is reported as an APPL SDM critical alarm. ISTb and ManB states are reported as an APPL SDM minor alarm.			
—end—			

Logging in to the SDM

SDM maintenance and administration procedures included in this document require logging in to the SDM as either the root user or the maintenance (maint) user. Maintenance users are only allowed to perform surveillance and maintenance activities, and change their own passwords.

CAUTION
SDM failure
Log in as the root user only when the procedure you are performing requires it. Otherwise, log in as a maint user. If you are logged in as the root user, use caution when copying, storing, or removing any files on the SDM.

Copying and storing files in a logical volume, or removing files from a logical volume, may cause the SDM to fail.

This section describes how to log in to the SDM as the root user or the maint user, and shows the screens that are displayed.

At the prompt, log in to the SDM by typing

login: *user*

and pressing the Enter key.

where

user is either “root” for root user, “maint” for maintenance user

Enter the required password at the prompt by typing

User’s* Password: *password

and pressing the Enter key.

where

User is the userID (root, maint) of the user entered at login

password is the userID password

Root user login

When the root user user logs in, the system displays the following information:

- the last unsuccessful login
- the last login
- the number of local users who logged in locally
- the number of users who logged in to the SDM using ETA
- the number of users who logged in to the CM using ETA
- an alarm banner that displays the status of the SDM and its major components

```
Last unsuccessful login:  Tue Feb 3 10:43:21 EST on /dev/pts/14 from
47.208.10.44
Last login:  Tue Feb 3 15:58:42 EST 1998 on /dev/pts/21 from cm

There are 22 local logins.
There are 2 ETA logins to the SDM.
There are 3 ETA logins to the CM.

Current SDM status:
SDM     CON     LAN     APPL     SYS     HW
 .       .       .        .       .       .
```

Maint user login

When the maint user user logs in, the system displays the number of unsuccessful login attempts since the last login, the last unsuccessful login, the last login, and an alarm banner that displays the status of the SDM and its major components. (See page 2-43 for more information on the alarm

banner,) The system also indicates whether there are other users logged on to the SDM or the CM by way of the ETA. Figure 2-3 shows the screen that is displayed when a maint user logs in to the SDM.

Note: All users, except the root user, see the screen shown in figure 2-3.

Figure 2-3
Maint user login

```
Last login: Fri Nov 21 10:08:12 EDT 1997 on /dev/pts/4 from 47.208.0.93

There are 8 local logins.
There are no ETA logins to the SDM.
There are no ETA logins to the CM.

Current SDM status:
SDM     CON     LAN     APPL     SYS     HW
 .       .       .       .        .       .
```

Return key and Enter key

The carriage return key is identified in different ways (such as Enter, Return or Carriage Return) on various types of terminals. It is always used to enter commands and parameters into the system.

The procedures contained in this book and in other NTPs instruct you to press the Enter key after each step. If your terminal has a Return key, press the Return key instead. Do not press the Enter key located beside the numeric key pad.

Restricted shell

Figure 2-4 shows the list of restricted shell commands available to maint users. This screen is displayed when maint users type HELP at the UNIX prompt. To use the restricted shell after you have accessed the HELP, use the Quit command.

At the UNIX prompt, enter the desired command. Type HELP to redisplay the command list shown in figure 2-4. If you wish to access RMI from the restricted shell, type “sdmmtc”.

Figure 2-4
SDM restricted shell screen

```
The following commands are available:
 sdmmtc        - start the SDM Maintenance Interface
 billmtc       – start the SDM Billing Maintenance Interface
 who_is_on     – displays the users logged in to the SDM as well as
                 users logged into the Maintenance Menu System
 who           – displays users logged on to the SDM in long format
 ping <host>   – send ICMP ECHO_REQUEST packets to network hosts
 logroute      – invoke the Log Delivery commissioning tool
 listlogfile   – list all log files
 copylogfile   – copy one log file to another
 dellogfile    – remove log files
 viewlogfile   – view log file
 ftplogfile    – start ftp session to transfer log files
 help          – displays this help information
 exit          – logout of the SDM
maint:
```

Restricted shell commands

The commands available in the restricted shell are as follows:

sdmmtc accesses the RMI.

who_is_on indicates the number of users logged in to the SDM, and the number of users using the RMI. It is useful to determine the number of users on the system before performing service-affecting procedures.

who displays the names of the users logged on to the SDM, and the time at which they logged on.

ping confirms SDM LAN connectivity to a network host.

logroute accesses the Log Delivery commissioning tool.

listlogfile lists all log files stored in the /data/logs directory.

copylogfile copies one log file to another.

dellogfile removes log files stored in the /data/logs directory.

viewlogfile allows you to view a log file stored in the /data/logs directory.

ftplogfile allows you to begin an FTP session to transfer log files. (For more information, see page 2-26.)

help displays help information for the restricted shell.

exit logs you out of the SDM.

FTPLOGFILE command

The FTPLOGFILE command changes the current directory to /data/logs and invokes an FTP client to transfer the log files. Invoking the FTPLOGFILE command also invokes restricted file transfer protocol (RFTP). RFTP functions as an FTP client, but some functions are removed to prevent maint users from saving log files on the SDM.

The following list describes the FTP client commands that are available in RFTP:

! escapes to the restricted shell.

$ executes a macro.

account sends an account command to a remote server.

append appends to a file.

ascii sets the transfer type to ASCII.

bell sounds a beep when the command is complete.

binary sets the transfer mode to binary.

bye terminates and exits the FTP session.

case toggles mget with uppercase and lowercase ID mapping.

cd changes the remote working directory.

cdup changes a remote working directory to its parent directory.

chmod changes the file permissions of a remote file.

close terminates an FTP session.

cr toggles carriage return stripping when getting an ASCII file.

delete deletes a remote file.

debug toggles the debugging mode. Additional messages are displayed for a better understanding of what the client is doing.

dir lists the contents of a remote directory.

disconnect terminates an FTP session.

form sets the file transfer format.

glob toggles metacharacter expansion (* and ?) of local file names.

hash toggles whether you wish to display the number of byte blocks transferred.

help obtains information on any command.

idle sets the idle timer on the remote side.

image sets the transfer mode to binary.

lcd changes the local working directory.

ls lists the contents of a remote directory. This command is enabled, but, you cannot save the listing in a local file.

macdef defines a macro.

mdelete deletes multiple files.

mkdir makes a directory on the remote machine.

mode sets the transfer mode.

modtime determines the last time a file was modified.

mput sends multiple files from the SDM to the remote machine.

nmap sets templates for default file name mapping.

nlist lists the contents of a remote directory. NLIST is the same as the LS command, except the contents are not sorted.

ntrans sets the translation table for default file name mapping.

open opens a connection to a remote file system.

prompt forces prompting on multiple commands.

proxy issues a command on an alternate connection.

sendport toggles the PORT command for each data connection.

put sends one file from the SDM to the remote location.

pwd obtains the working directory on a remote machine.

quit terminates and exits an FTP session.

quote sends an arbitrary FTP command. Quote is enabled, however, if the RETR command is invoked, the command is not allowed.

rstatus shows the status of a remote machine.

rhelp gets help from a remote server.

rename renames a file on the remote machine.

reset clears queued command replies.

restart restarts a file transfer at bytecount, a parameter given to restart the transfer at a certain point.

rmdir removes a directory on a remote machine.

runique toggles the storing of unique copies of local files. If the file already exists, a ".1" is appended to the file name.

send sends one file from the SDM to the remote location.

site sends a site-specific command to a remote server.

size determines the size of a remote file.

status shows the current status of any of the toggle commands, including the type of transfer mode.

struct sets a file transfer structure.

system determines the remote system type.

sunique toggles the storing of unique copies of remote files. If the file already exists, a ".1" is appended to the file name.

tenex sets the transfer mode to tenex.

trace toggles packet tracing.

type sets the file transfer type.

user sends new user information.

umask sets default permission settings on the remote side.

verbose toggles whether you wish to display more messages on the screen.

? obtains local help information.

The following list describes the FTP client commands that are disabled when RFTP is invoked:

get transfers a file from the remote location to the SDM.

mdir lists the contents of multiple remote directories.

mget transfers multiple files from the remote machine to the SDM.

mls lists the contents of multiple remote directories.

newer gets a file if the remote file is newer than the local file.

recv receives files.

reget gets a file restarting at the end of a local file.

When a disabled command is invoked, an error message is displayed. The local change directory (LCD) command is enabled to allow the maint user to change from the /data/logs directory to another directory, if required.

Node and application control commands

Node control commands change the state of the SDM. Application control commands change the states of the application and service packages. The SDM node and package states are influenced by each other. When the SDM is in ManB state, all applications are in ManB state, unless they are in OffL state. (Applications in OffL state would remain in OffL state.)

Note: SDM application states depend on the SDM node state. An application in the ManB state when the SDM is returned to service will be brought into service. This includes any applications that were manually busied prior to when the SDM was busied. If you wish to keep an application out of service, regardless of SDM node state changes, busy the application and take it off-line.

Similarly, when some applications are ManB, ISTb, or failed state, the SDM state becomes ISTb. If all applications are in ManB or failed state, the SDM state becomes SysB. An application in OffL state does not affect the SDM node state. An application can be returned to service if the SDM state is InSv, ISTb, or SysB.

Node control commands can only be used locally (from the SDM RMI) if there is no connectivity between the SDM and the CM. Application control commands can be used regardless of connectivity between the SDM and the CM. Node and application commands can be entered at the input command line by root or maint users during an SDMRLogin session.

Note 1: The root user can use the command line interface at any time to execute any of the node and application control commands.

Note 2: Node and application commands are not available when maint users telnet to the SDM. Restricted shell commands are available. When a maint user establishes an SDMRLogin session, restricted shell commands are available. However, the user does not have access to the RMI.

Messages are displayed when these restricted shell commands are executed successfully and when they fail. Commands time out if they cannot communicate with the node control process. If a command fails, try the command again. If it continues to fail, contact your next level of support.

Note 3: The node control commands BSYSDM, RTSSDM, OFFLSDM, REBOOTSDM, and HALTSDM cannot be used during an SDMRLogin session.

Table 2-3 lists node control commands and their meanings. Application control commands are listed in table 2-4.

Table 2-3
Node control commands

Command	Meaning
BSYSDM [FORCE]	This command puts the SDM into the ManB state. This command can also be used with the FORCE option. **(Use the FORCE option with caution. It ensures that the state change takes place. However, all errors [IP mismatch] are ignored and checks are bypassed.)** No notification is sent to inform you when the command is complete. Use QuerySDM to determine when the command has completed. This command fails if one of the following conditions exists: • The SDM is already in the ManB state. • A command is in progress. (**BSYSDM with the FORCE option overrides any commands in progress.**) • The SDM is connected to the CM. Execute the command from MAPCI. • Invalid syntax has been entered. • There is no response from internal software.
RTSSDM [FORCE]	This command puts the SDM into the InSv state. This command can also be used with the FORCE option. **(Use the FORCE option with caution. It ensures that the state change takes place. However, all errors [IP mismatch] are ignored and checks are bypassed.)** **Note:** When the SDM or one of its applications or services is returned to service from a manual busy (ManB) state, the state of the SDM may move to in-service (InSV) briefly, then to in-service-trouble (ISTb) for a few minutes, and finally back to InSv. The ISTb state is the result of the application not being fully capable of supplying service during initialization. For example, if the Operations Measurements application is not yet InSv, the Exception Reporting application will be ISTb. This command fails if one of the following conditions exists: • The SDM is not in the ManB state. • A command is in progress. (RTSSDM with the FORCE option only overrides checks and errors, such as an IP address. A command in progress causes the RTSSDM FORCE command to fail.) • The SDM is connected to the CM. Execute the command from MAPCI. • There is an IP address mismatch. (RTSSDM with the FORCE option overrides IP address checks and errors.)

—continued—

Table 2-3
Node control commands (continued)

Command	Meaning
OFFLSDM	This command puts the SDM in the OffL state from the ManB state. This command fails if one of the following conditions exists: • The SDM is not in the ManB state. • A command is in progress. • The SDM is connected to the CM. Execute the command from MAPCI.
REBOOTSDM	This command reboots the SDM. The SDM must be in the OffL or ManB state. A broadcast message is transmitted to all terminals connected to the SDM. This command fails if one of the following conditions exists: • The SDM is not in the OffL or ManB state. • A command is in progress. • The SDM is connected to the CM. Execute the command from the MAPCI.
HALTSDM	This command shuts down the SDM. The SDM must be in the OffL or ManB state. The SDM must be physically power cycled when this command is finished. A broadcast message is transmitted to all terminals connected to the SDM. This command fails if one of the following conditions exists: • The SDM is not in the OffL or ManB state. • A command is in progress. • The SDM is connected to the CM. Execute the command from MAPCI.
—end—	

Table 2-4 lists application control commands and their meanings.

Table 2-4
Application control commands

Command	Meaning
INITPROC	This command tells the SDM that changes have been made to the application configuration file. This command is only used during installation of applications. It is not normally issued by users.
BSYAPP <package number>	This command, followed by the package number (shown when QuerySDM LOADS is executed), moves an application into the ManB state. This command fails if one of the following conditions exists: • The package (a group of software installed on the SDM) is already in the ManB state. • The package name is unknown. • A command is in progress.
RTSAPP <package number>	This command, followed by the package number (shown when QuerySDM LOADS is executed), moves an application into the InSv state from the ManB or SysB states. **Note:** When the SDM or one of its applications or services is returned to service from a manual busy (ManB) state, the state of the SDM may move to in-service (InSV) briefly, then to in-service-trouble (ISTb) for a few minutes, and finally back to InSv. The ISTb state is the result of the application not being fully capable of supplying service during initialization. For example, if the Operations Measurements application is not yet InSv, the Exception Reporting application will be ISTb. This command fails if one of the following conditions exists: • The package is already in the InSv state. • The package is in the OffL state. • The package name is unknown. • A command is in progress.
OFFLAPP <package number>	This command, followed by the package number (shown when QuerySDM LOADS is executed), moves an application into OffL state from ManB state. This command fails if one of the following conditions exists: • The package is not in the ManB state. • The package name is unknown. • A command is in progress.

—continued—

Table 2-4
Application control commands (continued)

Command	Meaning
QUERYSDM [FLT|LOADS STATUS|CONFIG]	This command displays the following information: • QuerySDM with no options displays the state of the node (default), and the number of links out of service. • QuerySDM FLT displays all faults on the system. • QuerySDM LOADS displays the installed and registered application packages, their version numbers, and their current states and numeric identifiers. • QuerySDM STATUS displays the status of system components. • QuerySDM CONFIG displays the contents of the SDM configuration file, which lists all commissioned and configurable values.
LOCATE	This command displays location information for hardware modules.
	—end—

Maintaining the SDM using the remote maintenance interface

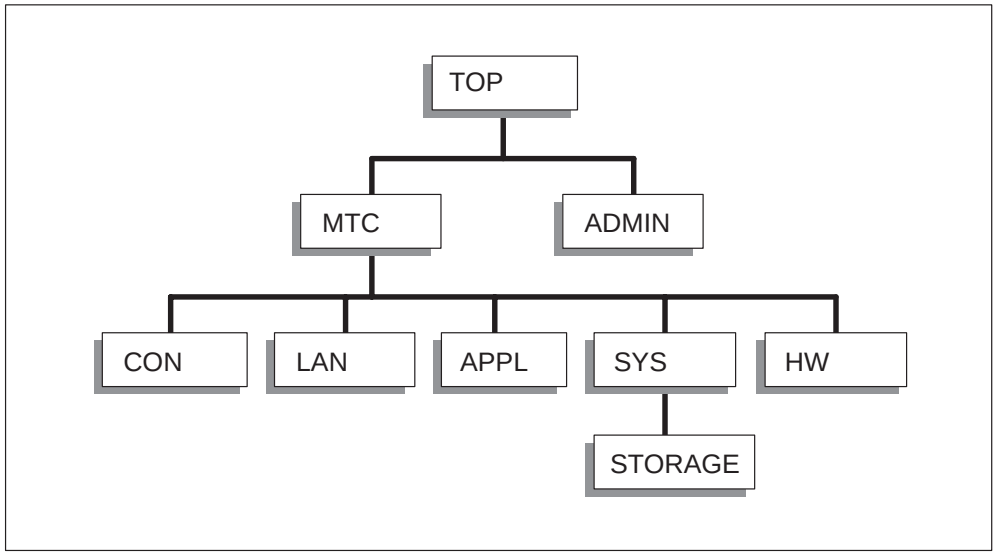
The RMI is the secondary maintenance, administrative, and diagnostic tool for the SDM. This ASCII-based display provides maintenance information about the overall state of the SDM, alarms, SDM and CM connectivity, application software, operating system resources, and hardware.

System administration functions include administering user accounts, software updates, and backup and restore. A restricted shell provides maintenance users with additional diagnostic tools that are useful for monitoring and maintaining the system. Context-sensitive help is provided for all menu screens.

The RMI can be used to alter the state of the SDM if communications between the SDM and the CM are not functioning. Otherwise, state changes must be performed at the MTC APPL level of the MAP interface, as described on page 2-2.

Figure 2-5 shows the top and maintenance menu levels of the RMI. The top menu level is the starting point for RMI maintenance and administrative functions. RMI maintenance screens are similar to MAP display screens. Each RMI maintenance screen contains an alarm banner, command list, input and output areas, and a clock. The maintenance level functionality is described in this section. Administrative functions are described in the "SDM system administrative overview" chapter on page 3-4.

Figure 2-5
RMI maintenance levels



Accessing the remote maintenance interface

There are several methods to access the RMI:

- dialing into the console port (SP0) on the SDM from a VT100-compatible terminal using a modem connection
- connecting a VT100-compatible terminal directly to SP0 on the CPU controller module, using a null modem cable
- using a telnet connection from a workstation on the operating company LAN if telnet is enabled on the SDM. If telnet is not enabled, use the ETA application (optional).
- using Enhanced Terminal Access (ETA) from a remote workstation to log in to the SDM in a secure environment. ETA is an optional SDM application.
- using a VT100-compatible terminal connected to a terminal server on the operating company LAN, if telnet is enabled on the SDM. If telnet is not enabled, use the optional ETA application.

Note: SDMRLogin cannot be used to access the RMI.

Using telnet

Before you try to telnet, set your terminal to emulate a VT100 or an 80-character × 24-line xterm window.

Establish a telnet connection from a UNIX prompt by typing

>telnet *sdm_ip_address*

and pressing the Enter key.

where

sdm_ip_address is the IP address or the hostname of the SDM

For example, if the IP address of the SDM is 131.129.128.169, type

>telnet 131.129.128.169

When the connection is established, you can log in to the SDM using a valid user name and password.

Note: Telnet must be enabled to use this method. The default state is enabled. Nortel recommends that you use ETA to access the SDM remotely because it authenticates all users in a secure environment. UserIDs and passwords are passed across the network in an insecure environment when you telnet to the SDM. ETA is an optional SDM application.

Using Enhanced Terminal Access

ETA is an optional SDM application that provides secure remote access to the SDM across the operating company's TCP/IP wide area network (WAN). ETA is not part of the base platform. If your system includes ETA, telnet must be disabled to use ETA.

Establish an ETA connection from a UNIX prompt by typing "eta", and pressing the Enter key. Figure 2-6 shows the Distributed Computing Environment (DCE) login screen that is displayed after you establish an ETA connection. Enter your DCE userID in the principal name field. Use the tab key to move to the password field. Enter your DCE password, and press the Enter key or select "OK".

Note: For more information on the ETA application, refer to the NTP, *SuperNode Data Manager Enhanced Terminal Access User Guide*.

Figure 2-6
DCE login window

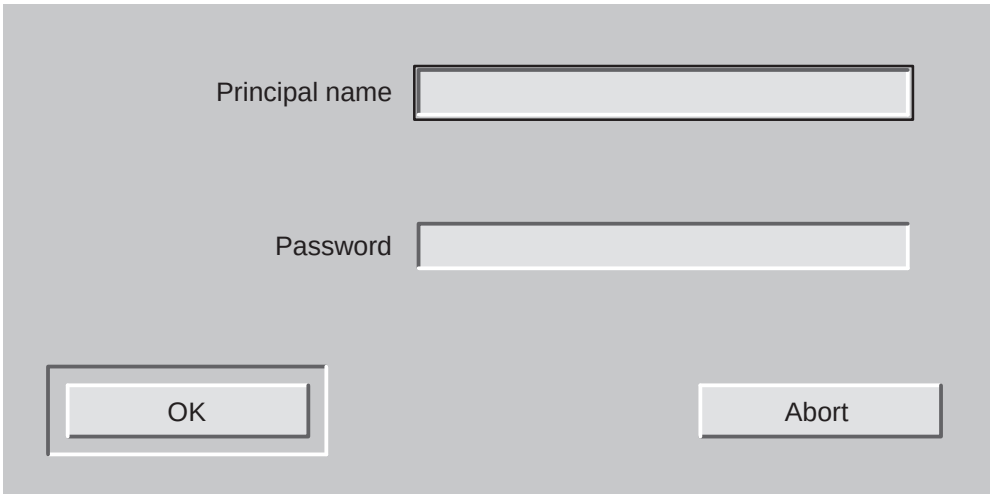
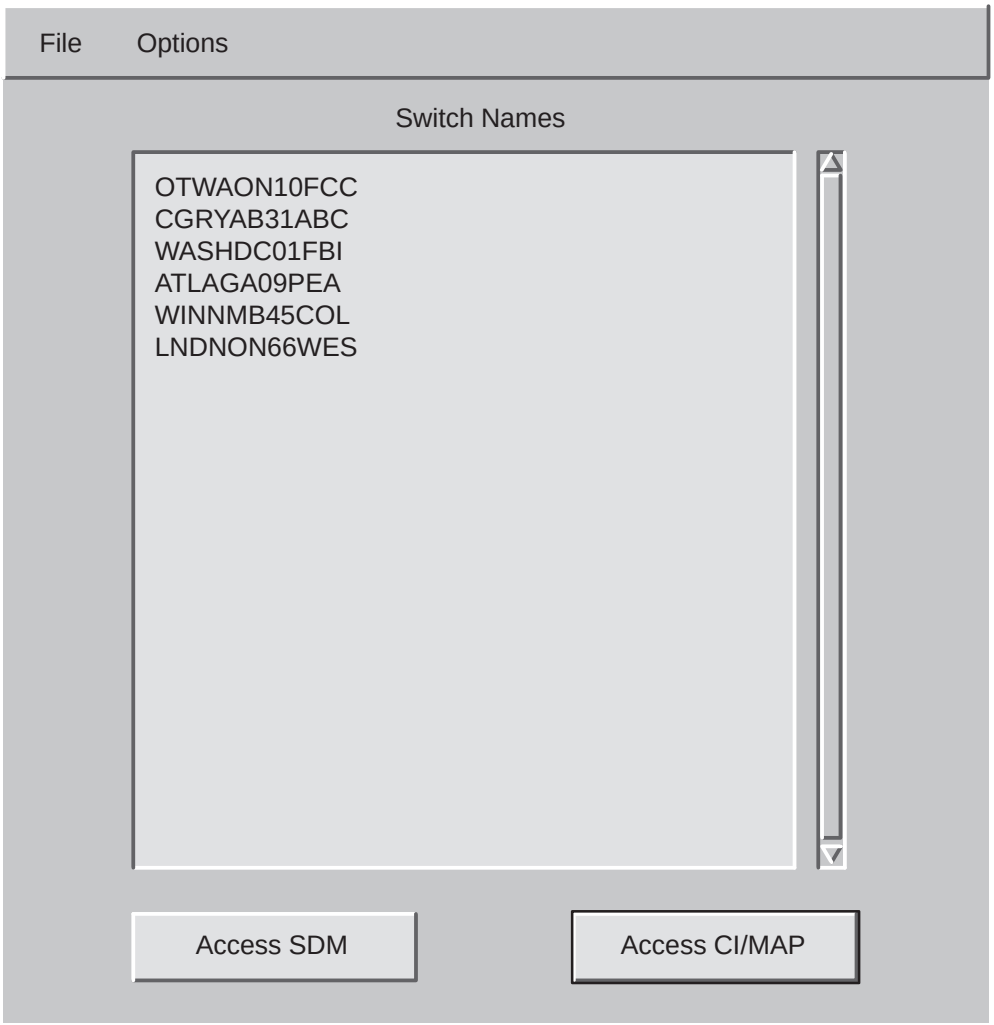


Figure 2-7 shows the Enhanced Terminal Access menu that is displayed following successful DCE login. This menu displays a list of the switches which have SDMs in the DCE cell. Highlight a switch name and select "Access SDM".

Figure 2-7
Enhanced Terminal Access window



At the UNIX prompt, access the RMI by typing “sdmmtc”, and pressing the Enter key.

Using a dial-up connection

Nortel recommends that you use the General DataComm (GDC) maintenance modem provided with the SDM equipment whenever a console dial-up modem connection to the SDM from a remote location is required.

For more information on using a dial-up connection to the SDM, refer to the procedure ”Establishing a modem connection” on page 4-84 in the “SDM maintenance procedures” chapter of this document.

Static and dynamic information

The RMI displays two types of information – static and dynamic. Static information is displayed once each time you request it. Static information is displayed when the QuerySDM, Logs, Tst and Locate commands are invoked. The information displayed from these commands does not change until the command is executed a second time. Dynamic information is displayed at the maintenance menu levels, and at the RMI alarm banner. The information displayed does not depend on your input. It is updated whenever there is a change. For example, the alarm banner displays major components on the SDM and their states. If an application goes to ISTb state, the APPL component under the alarm banner automatically changes to ISTb.

Static information is displayed below dynamic information when there is enough room to include both dynamic and static information. If there is not enough room, the dynamic information disappears. If MORE is shown at the command input line, there are additional screens of static information. Press the Enter key to display additional screens. When the last screen of static information is displayed, pressing the Enter key clears the output window and re-displays any dynamic information.

Note: The current state of all hardware modules can be seen dynamically at the hardware (HW) menu level of the RMI, or the platform MAP level under the SDM MAP level. The current state of the hardware modules can be viewed statically with the "MAPCI>QUERYSDM STATUS" command or the "SDM>QUERYSDM STATUS" command.

Using the RMI menu system

Navigation through the maintenance menu system is linear, meaning that each menu has only one path leading to it. From any menu, you can do the following:

- return to the top level of the RMI by typing TOP
- return to the previous menu (except from the top level) by entering the menu name or using the quit command
- go to a level of the RMI by entering one of the menu names that appear in the alarm banner, with the exception of SDM
- type the corresponding menu level number or the menu name to access a menu. For example, to go to the maintenance menu level of the RMI, select option 2 from the top menu level of the RMI. Alternatively, you can type MTC at any menu level of the RMI.
- type QUIT ALL to exit the RMI

- type d <# lines> to scroll down when the dynamic output extends beyond the current screen. Typing “d” without specifying the number of lines scrolls down to either the end of the display or the end of the current page. Typing “d” with the specified number of lines scrolls down to either the specified number of lines or to the end of the display.
- type u <# lines> to scroll up when the dynamic output extends beyond the current screen. Typing “u” without specifying the number of lines scrolls up to either the start of the display or the start of the current page. Typing “u” with the specified number of lines scrolls up to either the specified number of lines or the start of the display.

Note: You must press the Enter key after typing each of the RMI commands described above.

The following set of navigation and interface commands is available at any maintenance menu level of the RMI:

- The Quit command is always displayed with the other RMI commands that are available at the current maintenance menu level. Quit is used to go back to the previous menu. Use this command by typing QUIT or 0 (menu option for Quit). The Quit All command allows you to exit the RMI from any maintenance menu level, and from the administration and access menu levels. Use this command by typing QUIT ALL or 0 ALL, and pressing the Enter key.
- The QuerySDM command can be invoked at any maintenance level menu of the RMI except the Storage sub-level. QuerySDM has a number of options that provide different types of information about the SDM. Use the QuerySDM command by typing QUERYSDM or 14 (menu option for QuerySDM) followed optionally by one of the QuerySDM parameter values (FLT, STATUS, CONFIG, or LOADS). See page
- The Locate command can be invoked at any maintenance menu level of the RMI with the exception of the storage sub-level. Locate provides a list of modules installed on the SDM and their locations. Use the Locate command by typing LOCATE or 15 (menu option for Locate). See page 2-77 for more information on the Locate command.
- The Help command is always displayed with the other RMI commands that are available at the current menu level. The Help command gives information on a menu or on a command, and how to use it. Help messages are also displayed when incorrect information is entered. Use this command by typing the following:
  - — HELP or 17 (menu option for Help) to get information on the current screen, and on commands available at that level
  - — HELP and a command name or by typing 17 and a command name to get information on that command

- The Refresh command is always displayed with the other RMI commands that are available at the current menu level. Use this command to refresh the screen after using a command that displays static information, such as Locate or QuerySDM. Use this command by typing REFRESH or 18 (menu option for Refresh).

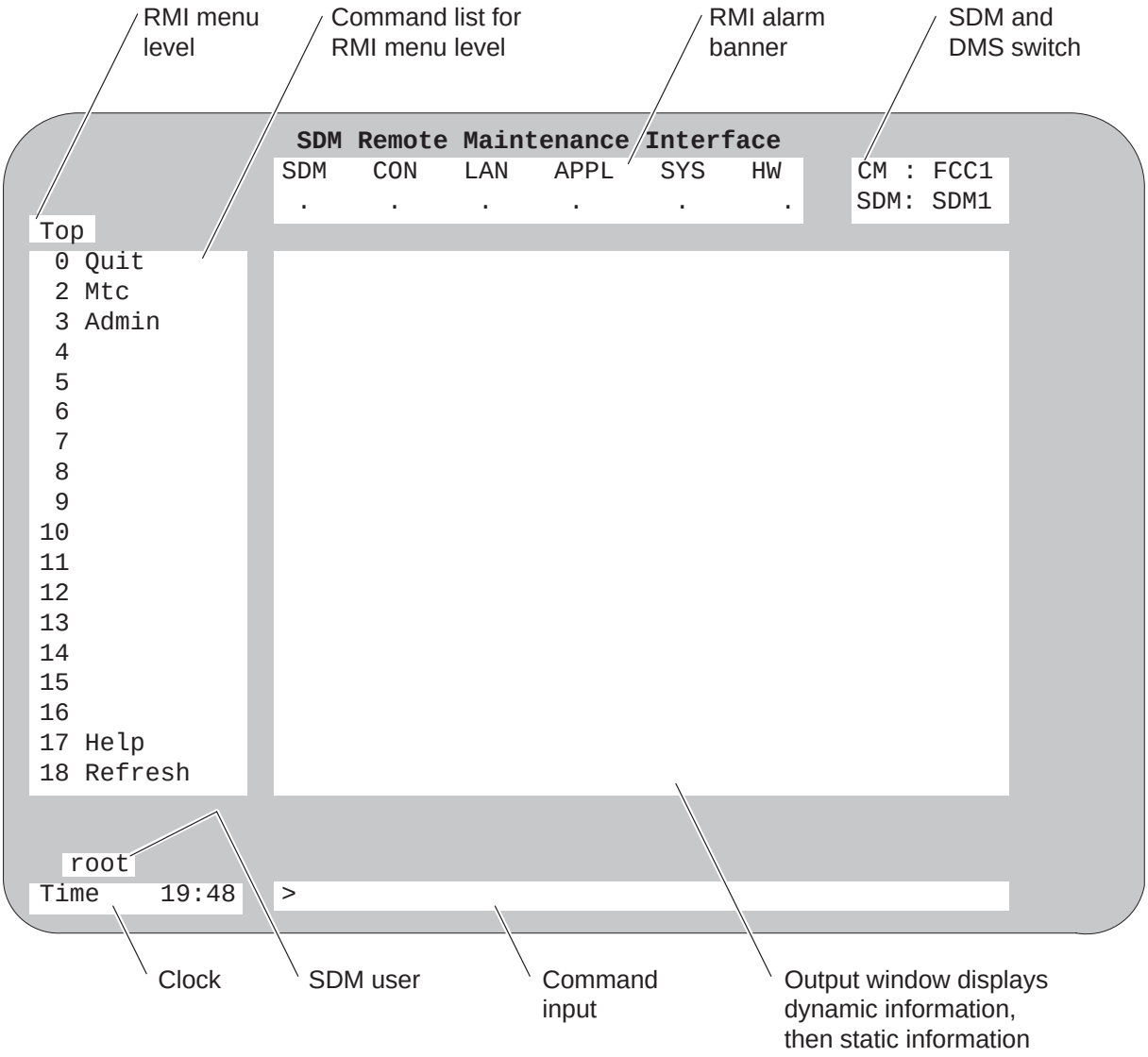
The following sections describe each of the menus and displays in the RMI, and the functionalities they provide.

Top menu level of the RMI

Figure 2-8 shows the top menu level of the RMI, and highlights the major components found on RMI menu levels.

Note: Users must type “sdmmtc” at the UNIX after logging in.

Figure 2-8
Top menu level of the RMI



This screen is the entry point into the RMI menu system, which is split into maintenance (Mtc) and administrative (Admin) functions. Figure 2-8 also shows the common information found on RMI menu screens.

Note: Administrative functions of the RMI are described in the "SDM system administrative overview" chapter on page 3-4. To re–access the Top menu level of the RMI, type TDP from any RMI menu level.

Monitoring SDM status and alarms at the RMI

Each maintenance menu level displays an alarm banner. The information in the alarm banner is dynamically updated to show the overall state of the SDM, and the states of its major components. The alarm banner is identical at all menu levels.

The alarm banner is also displayed at the administration menu level of the RMI (the starting point for RMI administrative functions). The alarm banner is also displayed at the access menu level. The alarm banner is not displayed when the following options are selected from the administration menu level of the RMI:

- time
- user
- backup
- install

When all SDM components are functioning normally, the alarm banner shows all components in-service. When SDM faults are detected, the affected component under the alarm banner dynamically changes from in-service state to the appropriate fault state. A symbol below each major component in the alarm banner indicates that component's state.

The following six components are displayed in the alarm banner:

- SDM displays the overall status of the SDM.
- CON displays the status of the SDM connections to the CM, and the state of DS512 links. See page 2-50 for more information about this menu level.
- LAN displays the status of the connectivity to the operating company LAN. See page 2-54 for more information about this menu level.
- APPL displays the status of the software applications running on the SDM. See page 2-57 for more information about this menu level.
- SYS displays the status of AIX operating system resources and logical volumes. See page 2-61 for more information about this menu level.
- HW displays the status of all hardware devices connected to the SDM. See page 2-69 for more information about this menu level.

All components, except SDM, have their own menu levels that display further information to assist you in determining why the alarm has occurred. These menus can be accessed at any level of the RMI by typing the component name. For example, access the connectivity (Con) menu level of the RMI by typing CON. SDM node states are described in table 2-6. Additional information on a particular component can be obtained by using the QuerySDM command.

SDM major component states are described in table 2-5. States are displayed symbolically under each component in the alarm banner. These states can also be displayed on the CM through the QuerySDM status command, however, additional details at the connectivity, LAN and system (Sys) menu levels of the RMI are not displayed. (See table 2-6 for the meaning of the symbols that are displayed on the RMI.)

Table 2-5
SDM components at the RMI

SDM component at RMI	Alarm banner symbol	Explanation and action
SDM		Refer to table 2-6 for information on the SDM state.
CON	.	The SDM is receiving heartbeats from the CM, and there is no IP mismatch between the SDM and the CM. All DS512 links are InSv.
	I	There is an IP mismatch or some of the DS512 links are down.
	S	The SDM is not receiving heartbeats from the CM. Check for alarms under the APPL header of the alarm banner at the MTC level of the MAP display. If the SDM is not communicating with the CM, an SDM critical alarm is displayed at the MAP interface. Use the procedure ”Clearing MAP alarms triggered by the SDM - APPL SysB critical” in this document to isolate and clear the fault.

—continued—

Table 2-5
SDM components at the RMI (continued)

SDM component at RMI	Alarm banner symbol	Explanation and action
LAN	.	Connectivity between the SDM and the operating company LAN node(s) is InSv. DCE is functioning normally.
	S	There is no connectivity between the SDM and the operating company LAN nodes, and DCE is in SysB state. When DCE is in SysB state, the SDM applications that use DCE automatically go in ISTb state, and can no longer operate.
	I	Connectivity between the SDM and one or more of the operating company LAN nodes is failing, or an abnormal condition has been observed with DCE. To isolate and clear the fault, use the procedure ”Clearing MAP alarms triggered by the SDM - APPL SysB minor” on page 4-3 in this document. If the problem is with DCE, refer to the troubleshooting information in the “SDM system administration overview” chapter of this document. ***Note:*** If DCE has not been configured using the SDM commissioning tool, or DCE has not been configured correctly, the DCE state is unequipped (uneq). If DCE is unequipped, it is not included in the calculation of the overall LAN or SDM state.

—continued—

Table 2-5
SDM components at the RMI (continued)

SDM component at RMI	Alarm banner symbol	Explanation and action
APPL	.	All applications on the SDM are functioning normally.
	I	One or more applications has reported an ISTb or failed condition. If there is a mix of different states for the applications, the overall state for APPL is ISTb.
	M	All applications have been manually stopped.
	S	All applications have failed.
	O	All applications have been put in OffL state. The OffL state does not generate a alarm. Use the procedure ”Clearing MAP alarms triggered by the SDM - APPL SysB minor” on page 4-3 in this document. ***Note:*** The APPL state indicates the state of all applications that are not in the OffL state.
SYS	.	There is no operating system software alarm.
	I	There is one or more operating system software alarms. Use the procedure ”Clearing MAP alarms triggered by the SDM - APPL SysB minor” on page 4-3 in this document.
HW	.	All hardware devices are in service.
	I	One or more hardware devices are not in service. Use the QuerySDM and Trnsl commands to isolate the hardware fault. If required, follow the appropriate hardware replacement procedure in this document. ***Note:*** The Trnsl command can only be used at the MAP display.
		—end—

Commands at the top menu level

The following commands are available at the top menu level of the RMI:

- Mtc is the entry point into the maintenance portion of the RMI. This is the starting point for all maintenance activities.

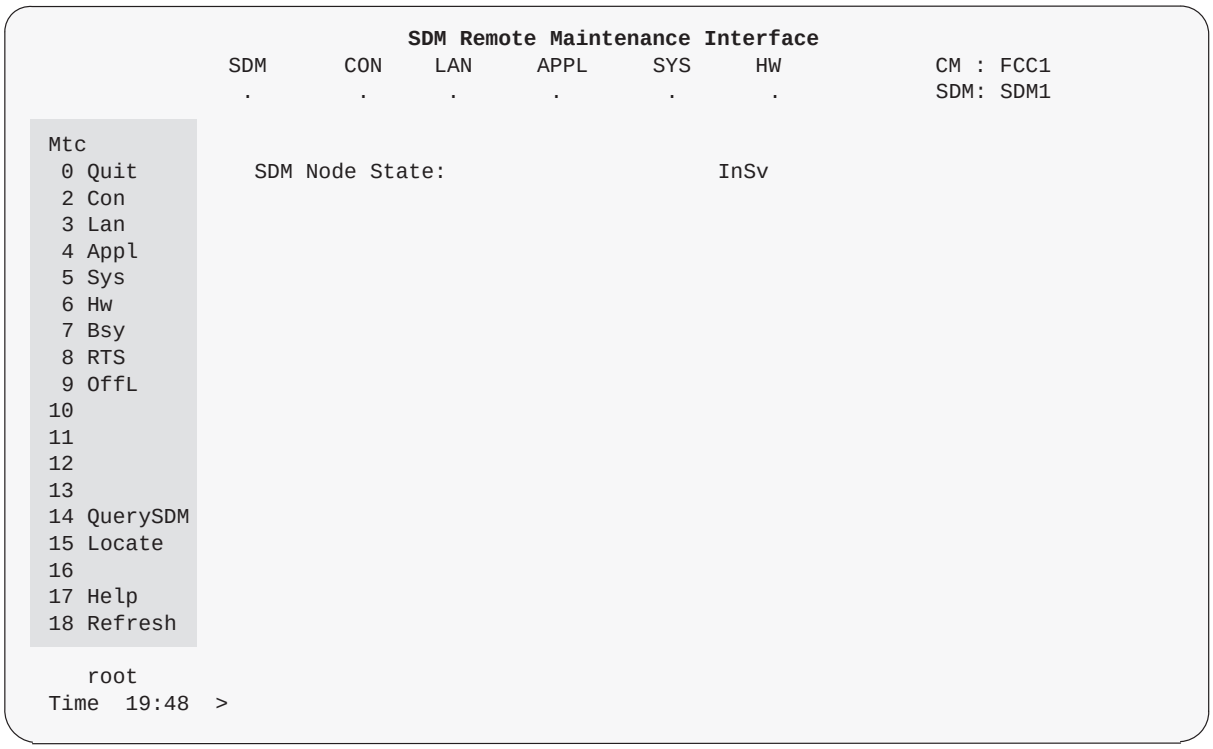
- Admin is the entry point into the administrative portion of the RMI. This is the starting point for all administration activities. (Administrative functions of the RMI are described in the “SDM system administrative overview” chapter on page 3-4.)

Maintenance menu level of the RMI

Figure 2-9 shows the maintenance menu level of the RMI. This menu provides the entry point for all maintenance functions on the RMI. In the example shown, the SDM node state and all components are InSv or functioning normally.

Select option 2 from the top menu level of the RMI to access the maintenance level. You can also access the maintenance menu level by typing MTC from any level of the RMI.

Figure 2-9
Maintenance menu level



Monitoring the SDM node state at the RMI

The `SDM Node State:` line appears at most maintenance menu levels of the RMI. It is dynamically updated, and indicates the overall state of the SDM. The node state of the SDM is also dynamically updated on the alarm banner that appears on all maintenance menu levels, and the administration menu level of the RMI. SDM node states are described in table 2-6.

Table 2-6
SDM state indicators at the RMI

SDM node state at RMI	Alarm banner symbol	Meaning	Explanation
InSv	.	in service	There are no hardware or software faults on the SDM. All applications, processes, hardware devices, and CM and operating company LAN connections are operational.
ISTb	I	in service trouble	The SDM node state is ISTb if one or more of the following faults have been reported on the SDM: • A hardware component is not InSv. • An operating system software alarm is present. • Some application software package are not InSv except OffL software packages. • Communication between the CM and the SDM has failed. • The operating company LAN connectivity has failed. • A file system has exceeded its alarm threshold or any volume group is not InSv.
SysB	S	system busy	The SDM node state at the RMI shows SysB only if all software applications on the SDM have failed.
ManB	M	manual busy	The SDM has either received a ManB command from the CM, or has been manually busied at the RMI while communications to the CM are down. All application and service software processes have stopped.
OffL	O	offline	The SDM is offline, and is not communicating with the CM. The SDM has received the OffL command from the CM, or it has been set to the OffL state locally at the RMI while isolated from the CM.

The SDM node state at the RMI is normally the same as the CM view of its state at the MAP display. If the CM and the SDM are unable to communicate, either because of a fault in the communications link, or because the SDM is out of service, the node states at the RMI and the MAP interface may be mismatched. However, when CM-SDM communications are restored, the SDM node state at the RMI aligns to the current CM view.

Commands at the maintenance menu level

The following commands are available at the maintenance menu level of the RMI:

- CON displays the status of SDM connections to the CM. See page 2-50 for more information about this menu level.
- LAN displays the status of the connectivity to the operating company LAN, and the state of DCE. See page 2-54 for more information about this menu level.
- APPL displays the status of the software applications running on the SDM. See page 2-57 for more information about this menu level.
- Sys displays the status of the AIX operating system resources and logical volumes. See page 2-61 for more information about this menu level.
- HW displays the status of all hardware devices connected to the SDM. See page 2-69 for more information about this menu level.
- BSY sets the SDM to the manual busy (ManB) state. Select option 7 or type BSY to invoke this command.
- RTS returns the SDM to service from the ManB state. Select option 8 or type RTS to invoke this command. The RTS command can also be used with the FORCE option.
- OFFL is used to set the SDM to the offline state from the ManB state. Communications between the CM and the SDM are disabled when this command is executed. Select option 9 or type OFFL to invoke this command.
- QuerySDM provides information about the status and configuration of the SDM. The information displayed is always static. (Use the Refresh command to delete the information displayed by this command.) QuerySDM, without any parameters, displays information specific to the current screen. QuerySDM can also be used with the FLT, LOADS, STATUS and CONFIG options as follows:
  - — QuerySDM FLT displays all faults present on the SDM. For more information on this command, see page 2-73.
  - — QuerySDM LOADS displays all software loaded on the SDM. For more information on this command, see page 2-74. (At the application level of the RMI, QuerySDM, without any parameters, displays the same information. See page 2-59.)
  - — QuerySDM STATUS displays the status of all hardware devices on the SDM. For more information on this command, see page 2-72. (At the hardware level of the RMI, QuerySDM, without any parameters, displays the same information. See page 2-70.)

— QuerySDM CONFIG displays all locally-commissioned datafill on the SDM. For more information on this command, see page 2-76. (At the system level of the RMI, QuerySDM, without any parameters, displays the same information. See page 2-67.)

- REBOOTSDM is a hidden command that is used to reboot the SDM. It is only available to root users and only at the maintenance menu level of the RMI. The SDM must be in the OffL or ManB state to execute this command.

CAUTION
Reboot message
When a RebootSDM command is issued, the following message may appear on the SDM's local console during the reboot:
`Board Configuration Data Failure`
Ignore this message. It is not service-affecting.

- HALTSDM is a hidden command that is used to halt the SDM. It shuts down the operating system on the SDM. A power recycle is required to return the SDM to service. The SDM must be in the OffL or ManB state to execute this command.

Connectivity menu level of the RMI

Figure 2-10 shows the connectivity (Con) menu level of the RMI. This menu displays the status of the connections from the SDM to the CM. The heartbeat and the IP address synchronization state of the SDM-CM-LAN are displayed, as well as the states of DS512 connections. These state indicators are updated dynamically. In the example shown, the SDM node state and connectivity to the CM are ISTb. Two of the four DS512 links are closed.

Note 1: The Con menu level of the RMI can take up to 12 minutes to report that all DS512 links have been closed. This will only occur if all the DS512 links are disconnected from the CM to the SDM. The SDM will report a CM connectivity alarm due to lost heartbeats within 1 min. The CM will report this problem immediately. Monitor the DS512 link status at the MS MAP level.

Note 2: If all links are down for no obvious reason, and the CM, the MS cards, and the DS512 controller module are in service, the DS512 personality module may be faulty. Replace the DS512 personality module. If this does not correct the problem, contact Nortel for assistance.

Note 3: If a single DS512 link remains out of service for more than two minutes, there may be a link failure. Busy the link manually using the BSY command from the MS level of the MAP. Then attempt to return it to service using the RTS command. If the RTS command fails, contact your next level of support.

Select option 2 from the maintenance menu level of the RMI to access the connectivity level. You can also access this menu by typing CON from any menu level of the RMI.

Figure 2-10
Connectivity menu level

```
                          SDM Remote Maintenance Interface
                 SDM      CON    LAN     APPL     SYS     HW          CM : FCC1
                  I        I      .       .        .       .          SDM: SDM1
Con
 0 Quit          SDM Node State:                      IsTb
 2               CM Connectivity State:               IsTb
 3
 4 Logs          Heartbeat status:                    InSv
 5               IP address synchronization:          InSv
 6 Tst
 7               DS512 Link States:
 8                 I/O domain 0, port 0:            Open
 9                 I/O domain 0, port 1:            Closed
10                 I/O domain 1, port 0:            Open
11                 I/O domain 1, port 1:            Closed
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh

  root
Time  19:48  >
```

Logs at the connectivity menu level

Figure 2-11 shows static information that is displayed when the logs option is used. The logs option displays the current logs associated with SDM to CM connectivity. These logs describe the event, and the date and time it occurred. They are generated when connectivity from the SDM to the CM is lost or restored. The most recent log is displayed when a connectivity problem occurs or when it is corrected. The order of the logs is predefined by base software. Refer to table 2-7 on page 2-79 for more information about SDM logs and the required actions.

To display the logs, select option 4 or type LOGS at the connectivity menu level of the RMI. The dynamic information shown in figure 2-10 is replaced

by the static log information. Press the Enter key to scroll down the screen. When the last screen of log information is shown, press the Enter key to redisplay the information that was previously displayed.

Figure 2-11
Logs at the connectivity menu level

```
                          SDM Remote Maintenance Interface
                SDM      CON    LAN     APPL     SYS     HW           CM : FCC1
                 I        I      .       .        .       .           SDM: SDM1
Con             Log information retrieved on Thu Oct 9 08:54:36 1997:
 0 Quit
 2              SDM600 Connection has been established
 3                Type: CM
 4 Logs           CM Link Up: heartbeat received by the CM
 5                Tue Oct 7 08:43:51 1997
 6 Tst
 7              SDM600 DS512 link up
 8                Module Location: Shf:SDMM, Slot:1, Port:0
 9                Link open
10                Tue Oct 7 08:08:11 1997
11
12              SDM300 DS512 link down
13                Module Location: Shf:SDMM, Slot 12, Port:1
14 QuerySDM       Link closed
15 Locate         Tue Oct 7 08:32:41 1997
16
17 Help         SDM600 DS512 link up
18 Refresh        Module Location: Shft:SDMM, Slot 1, Port:0

  root
Time  19:48   MORE...
```

QuerySDM at the connectivity menu level

Figure 2-12 shows the static information displayed when the QuerySDM command with no options is used at the connectivity menu level of the RMI. QuerySDM displays the CM and SDM IP addresses, and the CM/SDM netmask below the information displayed at the connectivity menu level.

To use this command, select option 14 or type QUERYSDM. For more information on using this command with its parameters, FLT, LOADS, STATUS, and CONFIG, see page 2-72.

Figure 2-12
QuerySDM at the connectivity menu level

```
                          SDM Remote Maintenance Interface
                  SDM      CON    LAN     APPL     SYS     HW          CM : FCC1
                   I        I      .       .        .       .          SDM: SDM1
Con
 0 Quit           SDM Node State:                      IsTb
 2                CM Connectivity State:               IsTb
 3
 4 Logs           Heartbeat status:                    InSv
 5                IP address synchronization:          InSv
 6 Tst
 7                DS512 Link States:
 8                  I/O domain 0, port 0:             Open
 9                  I/O domain 0, port 1:             Closed
10                  I/O domain 1, port 0:             Open
11                  I/O domain 1, port 1:             Closed
12
13                  CM IP address:                   47.105.155.1
14 QuerySDM         SDM IP address:                  47.105.155.5
15 Locate           SDM-CM netmask:                  255.255.255.248
16
17 Help
18 Refresh

  root
Time  19:48  >
```

Other commands at the connectivity menu level

The Tst command is used to test the connectivity of the DS512 links to the CM. The links you wish to test must be closed from the CM before you can test their connectivity. The Tst command displays static information. To test a specific link, use the options, DOMAIN and PORT. If the domain and port numbers are not specified, all links are tested.

Determine the number for DOMAIN as follows:

- Use 0 for DOMAIN if the DS512 controller module is in slot 1 of the main chassis.
- Use 1 for DOMAIN if the DS512 controller module is in slot 12 of the main chassis

Use 0 for PORT if you are testing port 0, and 1 for PORT if you are testing port 1.

For example, typing TST 0 1 to tests the link of the DS512 controller module in domain 0, and port 1 on the DS512 personality module.

Change is a hidden command for root users only. This command allows you to change an IP address. Type CHANGE. The system prompts you for

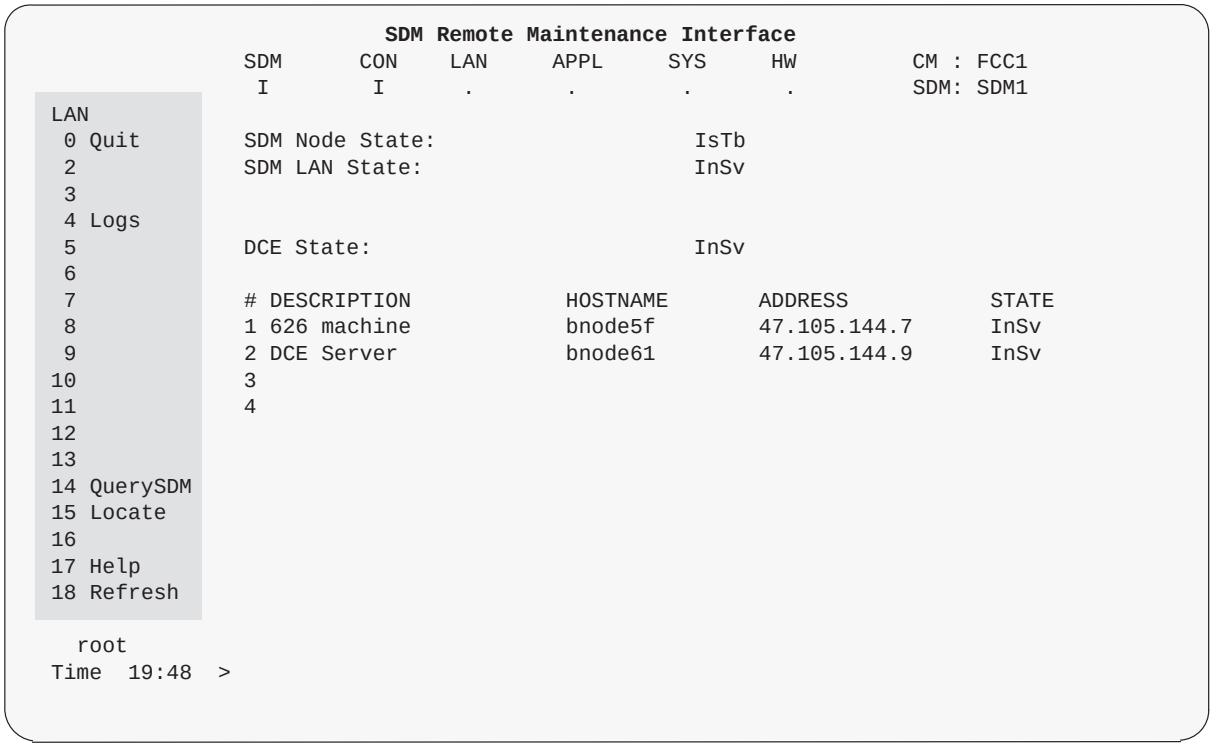
confirmation. You are prompted for the CM IP address, the SDM IP address, and the CM-SDM LAN netmask. You may change any, all, or none of these values. You are prompted to confirm the resulting values before the change is made.

LAN menu level of the RMI

Figure 2-13 shows the LAN menu level of the RMI. This menu dynamically updates the status of the connectivity from the SDM to up to four operating company LAN nodes. The SDM node state, the overall state of the operating company LAN, and the state of DCE, and the status of the DCE server are also displayed. In the example shown, the SDM node is ISTb, and the LAN and DCE states are InSv.

Select option 3 from the maintenance menu level of the RMI to access the LAN menu level. You can also access this menu by typing LAN from any menu level of the RMI.

Figure 2-13
LAN menu level of the RMI

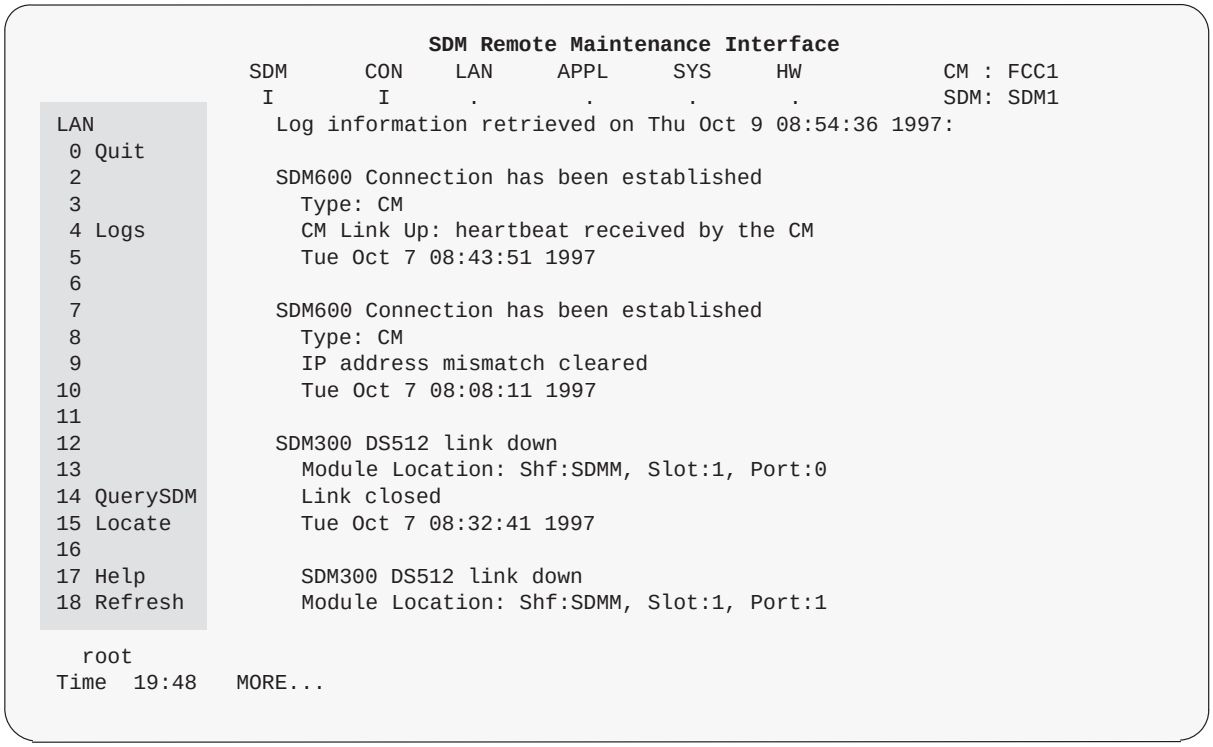


Logs at the LAN menu level

Figure 2-14 shows the static information that is displayed when the logs option is used. The logs option displays the current logs associated with LAN connectivity. These logs describe the event, and the date and time it occurred. The most recent log is displayed when connectivity from the SDM to the operating company LAN is lost or not established. The order of the logs is predefined by base software. Refer to table 2-7 on page 2-79 for more information about SDM logs and the required actions.

To display the logs, select option 4 or type LOGS at the LAN menu level of the RMI. The dynamic information shown in figure 2-13 disappears to make from for the static log information. Press the Enter key to scroll down the screen. When the last screen of log information is shown, press the Enter key to re-display the information that was previously displayed.

Figure 2-14
Logs at the LAN menu level



QuerySDM at the LAN menu level

Figure 2-15 shows the static information that is displayed when the QuerySDM command with no parameters is used at the LAN menu level of the RMI. QuerySDM displays the SDM hostname, the SDM-to-operating company LAN IP address, netmask, and gateway status below the information displayed at the LAN menu level.

To use this command, select option 14 or type QUERYSDM. For more information on using this command with its parameters FLT, LOADS, STATUS, and CONFIG, see page 2-72.

Figure 2-15
QuerySDM at the LAN menu level

```
                        SDM Remote Maintenance Interface
                  SDM      CON    LAN     APPL     SYS     HW         CM : FCC1
                   I        S      .       .        .       .         SDM: SDM1
LAN
 0 Quit           SDM Node State:                    IsTb
 2                SDM LAN State:                     InSv
 3
 4 Logs
 5                DCE State:                         InSv
 6
 7                # DESCRIPTION             HOSTNAME       ADDRESS           STATE
 8                1 626 machine             bnode5f        47.105.144.7      InSv
 9                2 DCE Server              bnode61        47.105.144.9      InSv
10                3
11                4
12
13
14 QuerySDM       SDM hostname:         SDM
15 Locate         SDM LAN IP address:    47.105.144.29
16                SDM LAN netmask:      255.255.240.0
17 Help           SDM LAN gateway:      Uncommissioned
18 Refresh

  root
Time  19:48  >
```

Other commands at the LAN menu level

LAN nodes defined at the RMI are used for monitoring connectivity to hosts on the operating company LAN. When a LAN node is defined at the RMI, the SDM periodically checks its connectivity status and raises an alarm if connectivity fails.

- Add is a hidden command, for root users only, that adds a LAN node entry into the first available position. You are prompted to enter the description, hostname, and IP address of the operating company node. You will then be prompted to confirm, reject, or edit the values for the first node.

- Del is a hidden command, for root users only, that removes a specified operating company LAN node entry. Delete a specific operating company LAN node entry by typing DEL, followed by the node number (1 to 4). The screen then displays the hostname, description, and IP address of the operating company LAN node that you are deleting. You are also prompted to confirm whether you wish to proceed with deleting the operating company LAN node.

Change is a hidden command for root users only that changes LAN parameter values. The parameters are LAN and the node number (1 to 4). Use the Change command as follows:

- Type CHANGE LAN to change the operating company LAN parameter values. The SDM hostname, and the operating company LAN's IP address, netmask and gateway are each displayed separately on the screen. Press Enter after each one until you see all values displayed on the screen. You will then be prompted to confirm, reject or edit the values. Choose the appropriate response, and complete the desired action.
- Type CHANGE, followed by the node number (1 to 4) to change a specific operating company LAN node number. The description of the specified operating company node, the hostname for the specified operating company node, and the IP address for the specified operating company node are each displayed separately on the screen. Press Enter after each one until you see all values displayed on the screen. You will then be prompted to confirm, reject or edit the values. Choose the appropriate response, and complete the desired action.

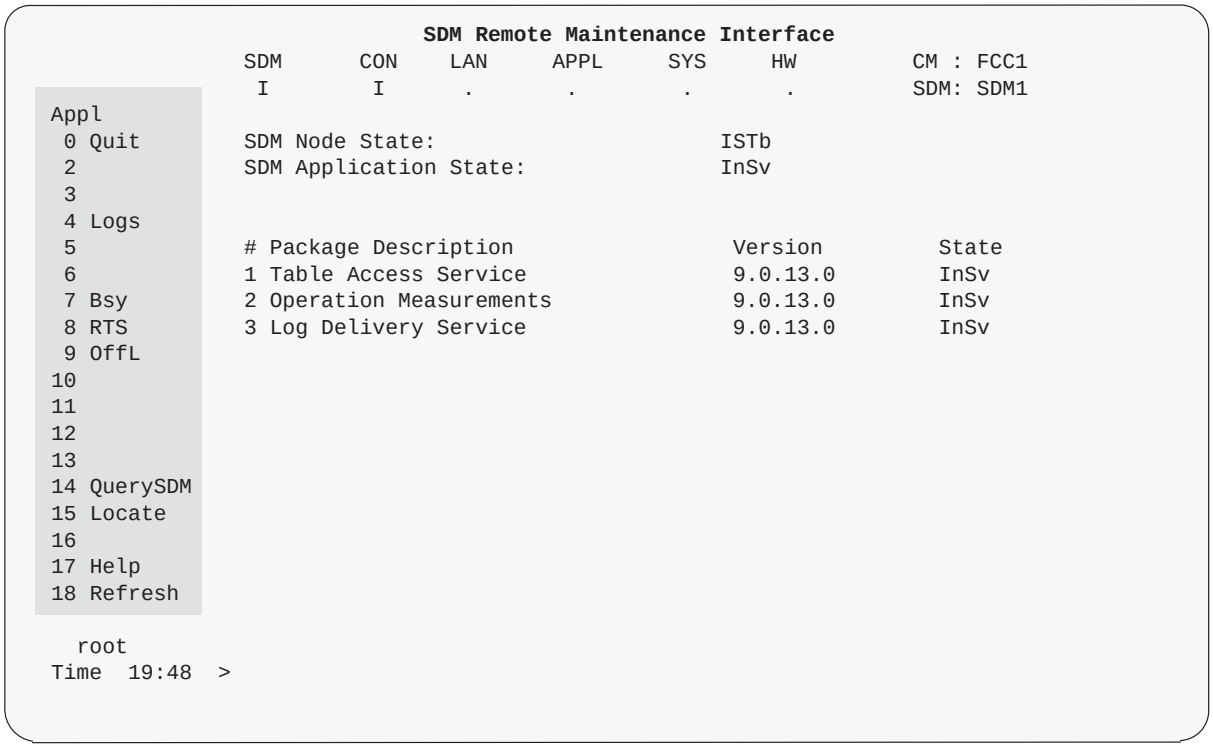
Note: For information on commissioning SDM-LAN connectivity, refer to the procedure "Commissioning SDM-LAN connectivity" on page 4-89 in the "SDM maintenance procedures" chapter of this document.

Application menu level of the RMI

Figure 2-16 shows the application menu level of the RMI. This menu displays the status of all application and service packages on the SDM. A package is all the SDM software related to a particular application or service. The application menu level includes the package number, followed by the package name, the version, and the current state of the package. In the example shown, the SDM node state is ISTb and the SDM application state is InSv. There are three packages installed on the SDM.

Select option 4 from the maintenance menu level of the RMI to access the application level. You can also access this menu by typing APPL from any menu level of the RMI.

Figure 2-16
Application menu level



Logs at the application menu level

Figure 2-17 shows the static information that is displayed when the logs option is used. The logs option displays the current logs associated with SDM software packages. Each log describe the event, and the date and time it occurred. The most recent log is displayed when a software application is not running normally. The order of the logs is predefined by base software. Refer to table 2-7 on page 2-79 for more information about SDM logs and the required actions.

To display the logs, select option 4 or type LOGS at the application menu level of the RMI. The dynamic information shown in figure 2-16 disappears to make room for the static log information. Press the Enter key to scroll down the screen. When the last screen of log information is shown, press the Enter key to re-display the information that was previously displayed.

Figure 2-17
Logs at the application menu level

```
                              SDM Remote Maintenance Interface
                  SDM      CON    LAN     APPL     SYS     HW         CM : FCC1
                   I        I      .       .        .       .         SDM: SDM1
Appl              Log information retrieved on Thu Oct 9 09:45:53 1997:
 0 Quit
 2                SDM603
 3                Package: pk1
 4 Logs             Process: pk1proc1
 5                  State: restarted
 6                  Tue Oct 7 00:00:51 1997
 7 Bsy
 8 RTS            SDM0603
 9 OffL           Package: SDM_BASE.logs
10                  Process: start_sdmlaq
11                  State: started
12                  Tue Oct 7 14:39:06 1997
13
14 QuerySDM       SDM0603
15 Locate         Package: SDM_BASE.logs
16                  Process: start_RTOsf
17 Help             State: started
18 Refresh          Tue Oct 7 14:39:07 1997

  root
Time  19:48   MORE...
```

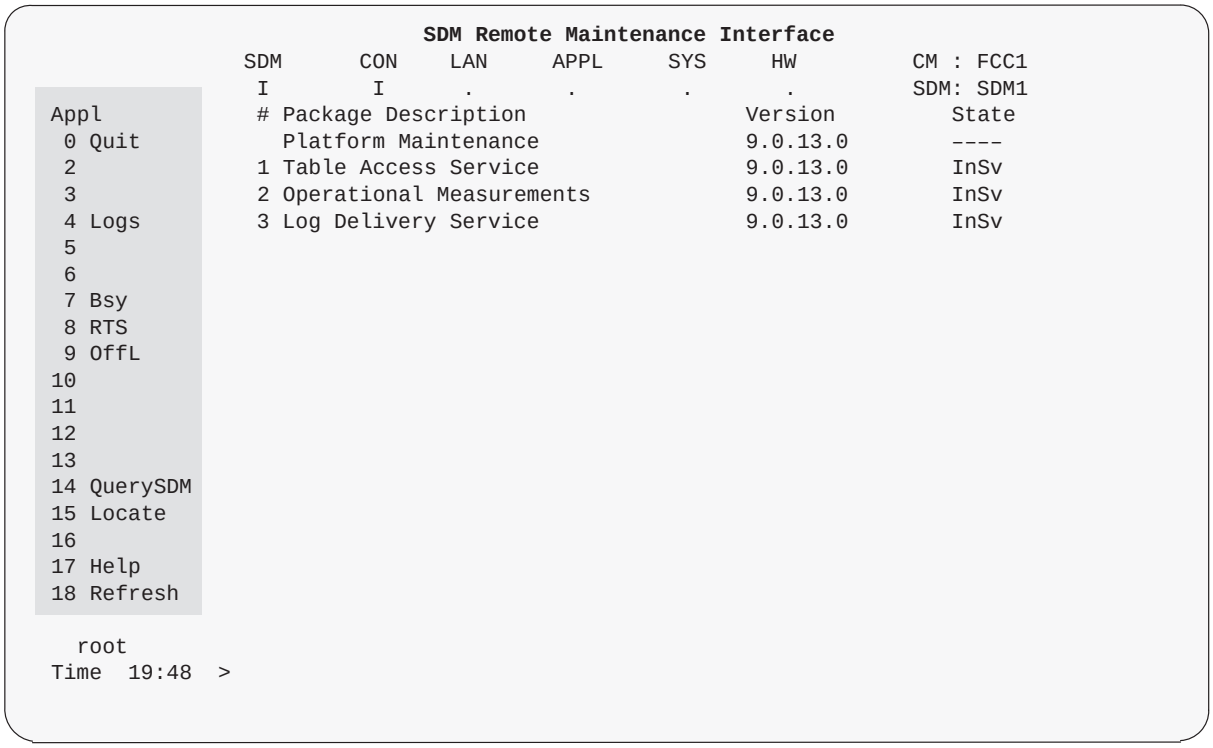
QuerySDM at the application menu level

Figure 2-18 shows the static information that is displayed when the QuerySDM command, with no parameters, is used at the application menu level of the RMI. QuerySDM displays the status of software packages on the SDM.

To use this command, select option 14 or type QUERYSDM. For more information on using this command with its parameters, FLT, LOADS, STATUS, and CONFIG, see page 2-72.

Note: QuerySDM at the application menu level of the RMI displays the same information as QuerySDM LOADS at any RMI maintenance menu level, and QuerySDM LOADS at the SDM MAP display level. See page 2-74 for more information on QuerySDM LOADS at the RMI, and page 2-11 for more information on QuerySDM LOADS at the SDM MAP display level.

Figure 2-18
QuerySDM at the application menu level



Other commands at the application menu level

The following commands are also available at this level:

- Bsy issues a busy command to a package. When a package is busied, the execution of all software associated with that package is stopped. To use this command, select option 7 or type BSY following the package ID number.
- RTS issues a return-to-service command to a package. When a package is returned to service, the execution of all software associated with that application is restarted.
- The information derived from the RTS command is displayed beneath the information currently displayed at the application level. Use the Refresh command to redisplay the information that was previously displayed.
- The FORCE option may be used with RTS to override the execution of other commands. To use RTS with the FORCE option, type 8 FORCE or type RTS FORCE, followed by the package ID number.

ATTENTION

When the SDM or one of its applications or services is returned to service from a manual busy (ManB) state, the state of the SDM may move to in-service (InSV) briefly, then to in-service-trouble (ISTb) for a few minutes, and finally back to InSv.

The ISTb state is the result of the application not being fully capable of supplying service during initialization. For example, if the Operations Measurements application is not yet InSv, the Exception Reporting application will be ISTb.

- OffL issues an offline command to the package. The package must be in ManB state before the offline command is invoked. An offline package does not generate an alarm condition. The parameter for this command is the package ID number.
- The information derived from the OffL command is displayed beneath the dynamic information. To use this command, select option 9 or type OFFL, followed by the package ID number.

System menu level of the RMI

Figure 2-19 shows the system menu level of the RMI. This menu provides information about the operating system, including current CPU usage, swap space, process space, and the automated incremental backup status. Resources that have exceeded their thresholds are marked by an asterisk (*), and trigger an ISTb alarm.

In the example shown, the SDM node state is ISTb. The SDM storage state is InSv. The automated incremental backup is completed.

The automated incremental backup status can be disabled, enabled, completed, or failed. Disabled indicates that the automated backup is not enabled. Enabled indicates that the automated backup has been enabled, but not executed yet. Completed indicates that the last automated incremental backup has been successfully completed. Failed indicates that the last automated incremental backup has failed.

Select option 5 from the maintenance menu level of the RMI to access the system menu level. You can also access this menu by typing SYS from any RMI menu level.

Figure 2-19
System menu level

```
                    SDM Remote Maintenance Interface
               SDM      CON     LAN      APPL      SYS      HW          CM : FCC1
                I         S       .        .         I        .          SDM: SDM1

Sys
 0 Quit        SDM Node State:                    ISTb
 2             SDM System State:                  ISTb
 3             SDM Storage State:                 InSv
 4 Logs        Automated Incremental Backup:      Completed on 10/09/97
 5 Storage
 6             #  Description                                      Current / Threshold
 7             1  CPU (run queue entries)                             0/ 250
 8             2  Number of Processes:                              50/  3 *
 9             3  Number of Zombies:                                 0/ 70
10             4  Swap Space (% full):                              23/  2 *
11             5  Number of Swap Queue Entries:                      6/ 80
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh

  root
Time  19:48  >
```

Logs at the system menu level

Figure 2-20 shows the static information that is displayed when the logs option is used. The logs option displays the current logs associated with system resources. Each log describes the event, and the date and time it occurred. The most recent log is displayed when system software resources exceed or return below their alarm thresholds. The order of the logs is predefined by base software. Refer to table 2-7 on page 2-79 for more information about SDM logs and the required actions.

To display the logs, select option 4 or type LOGS at the system menu level of the RMI. The dynamic information shown in figure 2-19 disappears to make room for the static log information. Press the Enter key to scroll down the screen. When the last screen of log information is shown, press the Enter key to redisplay the information that was previously displayed.

Note: When an alarm condition exists, the value displayed on the main system level menu is the current value for the resource, whereas the value in the log is the value that caused the threshold to be exceeded.

Figure 2-20
Logs at the system menu level

```
                          SDM Remote Maintenance Interface
                SDM      CON    LAN     APPL     SYS     HW            CM : FCC1
                 I        I      -       I        I       .            SDM: SDM1
Sys             Log information retrieved on Thu Nov 13 09:45:53 1997:
 0 Quit
 2              SDM302 Resource threshold exceeded
 3                Type: CPU
 4 Logs           Value: 6 run queue entries
 5                Threshold: 5 entries
 6                Tue Nov 3 14:39:02 1997
 7
 8              SDM602 Resource is within set limit
 9                Type: Number of swap queue entries
10                Tue Nov 3 14:52:02 1997
11
12              SDM302 Resource threshold exceeded
13                Type: Number of zombie processes
14 QuerySDM       Value: 4 zombies
15 Locate         Threshold: 3 zombies
16                Tue Nov 3 10:13:02 1997
17 Help
18 Refresh      SDM308 Automated incremental back up failed

  root
Time  19:48   MORE...
```

Storage at the system menu level

Figure 2-21 shows the static information that is displayed when the storage option is used at storage menu level of the RMI. The storage menu level displays the SDM node, system, storage, and disk mirroring states. It also displays the volume groups on the system, and their threshold values. The system shown in figure 2-21 consists of the root volume group (rootvg) and the data volume group (datavg).

Root users may add disks to the storage system, or change existing logical volumes. Both root and maint users can display the current list of logical volumes, including the available free disk space. To view the current list of

logical volumes, select option 5 at the system menu level of the RMI, or type STORAGE at any RMI menu level.

CAUTION

Logical volume names

Logical volume names can be created using an unlimited number of characters. However, a logical volume (LV) name longer than 21 characters will appear truncated on the storage menu level of the RMI because the storage menu only displays 21 characters. When performing an LV command, use the correct logical volume name otherwise the command will fail.

The maximum number of logical volumes on a system that can be monitored through the RMI is 16. In the example shown, seven logical volumes exist. Rootvg is created automatically by the system at installation time. It contains a base set of logical volumes that are required to start the system, including paging space, journal log, boot data and dump storage.

Datavg requires the installation of the NTRX50GP or NTRX50FU I/O controller module. When the I/O controller module is installed, datavg must be created. The method by which this is done depends on whether the system is a new system requiring datavg or an existing system that is migrating to a rootvg/datavg system. For more information, refer to the procedures, ”Creating a file system in the data volume group” on page 4-151 and ”Migration from a rootvg system to a rootvg/datavg system” on page 4-144 in the “SDM maintenance procedures” chapter in this document.

If there are additional disks on the system, the datavg volume group is expanded with the new disks or, datavg is created using the new disks. All SDM applications should write their data to datavg.

Figure 2-21
Storage menu level

```
                        SDM Remote Maintenance Interface
                SDM      CON    LAN     APPL     SYS     HW          CM : FCC1
                 I        S      .       .        I       .          SDM: SDM1
Storage
 0 Quit         SDM Node State:                    ISTb
 2              SDM System State:                  ISTb
 3              SDM Storage State:                 InSv
 4
 5              Disk mirroring (rootvg):                              Mirrored
 6                Volume              Size(MB)                 (% full/ threshold)
 7              1 /                     24                          22/ 80
 8              2 /usr                  204                         81/ 90
 9              3 /var                  40                          16/ 80
10              4 /tmp                  24                          10/ 90
11              5 /home                 304                         32/ 70
12              6 /sdm                  304                         67/ 97
13              (unallocated)           2852
14
15              Disk mirroring (datavg):                              Mirrored
16                Volume              Size(MB)                 (% full/ threshold)
17 Help         7 /sba                  512                         4/ 80
18 Refresh      (unallocated)           7568

  root                            ...Down...
Time  19:48  >
```

ATTENTION

Nortel recommends that logical volume management operations are performed from the local console. Nortel also recommends that logical volume management operations are not performed at the same time by more than one user with root privileges.

Commands at the storage menu level

Add is a hidden command used by root users to add new disks or a logical volume to the storage system. The parameter to add one or more disks to the system is DSK. Add a new disk by typing ADD DSK.

ATTENTION

A logical volume on the SDM must never reach 100% disk full. The system enters into abnormal conditions when a logical volume reaches 100% disk full.

If the specified logical volume exceeds its alarm threshold, contact your system administrator. The system administrator must assess the current condition of the logical volume and take appropriate action immediately. If required, contact Nortel for assistance.

To add a logical volume, use the following parameters:

- LV indicates a volume.
- VOLUME specifies the name of the volume group that you are creating. All volume groups are appended to the directory "/data". Do not precede the name by "/".
- SIZE specifies the size of the new logical volume (in Megabytes). Sizes are rounded up to the next multiple of 4 Mbytes.

For example, typing ADD LV SBA 100 adds a 100-Mbyte file system called SBA (SuperNode Billing Application).

Change is a hidden command used to expand an existing logical volume, or to change the alarm threshold for a logical volume. The parameters to expand an existing logical volume are as follows:

- LV indicates a volume
- VOLUME specifies the name of the volume from the storage menu level of the RMI. The name must be preceded by "/".
- SIZE specifies the expanded size of the logical volume (in Mbytes). Sizes increased are rounded up to the next multiple of 4Mbytes.

For example, typing CHANGE LV SBA 120 expands the current logical volume SBA by 120 Mbytes.

The parameters to change the alarm threshold for a logical volume are as follows:

- ENTRYNUMBER specifies the item number to change. (The entry number is shown to the left of the logical volume range in the storage menu level of the RMI.)
- NEWTHRESHOLDVALUE specifies the new desired value.

For example, typing CHANGE 2 80 changes the threshold of the /usr (item 2) volume group shown in figure 2-21 to 80 percent full.

QuerySDM at the system menu level

Figure 2-22 shows the static information that is displayed when the QuerySDM command with no parameters is used at the system level of the RMI. QuerySDM displays information on SDM configuration, including CM connectivity. It also displays the performance log SDM620 pre-defined time interval (TI).

To use this command, select option 14 or type QUERYSDM. For more information on using this command with its parameters, FLT, LOADS, STATUS, and CONFIG, see page 2-72.

The QUERYSDM command can also be used at the system menu level with an additional parameter, TI. QuerySDM TI displays time interval information about the performance log SDM620. This log reports current SDM system performance data, such as CPU usage, number of processes, swap space occupancy, and logical volume capacities. The pre-defined time interval is the time in minutes between the generation of two successive SDM620 logs.

To change the time interval, use the hidden command, CHANGE at the system menu level. For more information on the Change command, see ”Other commands at the system menu level” on page 2-68.

Note: QuerySDM at the system menu level of the RMI displays the same information as QuerySDM CONFIG at any RMI maintenance menu level, and QuerySDM CONFIG at the SDM MAP display level. See page 2-76 for more information on QuerySDM CONFIG at the RMI. See page 2-11 for more information on QuerySDM CONFIG at the SDM MAP display level.

Figure 2-22
QuerySDM at the system menu level

```
                          SDM Remote Maintenance Interface
               SDM      CON    LAN     APPL     SYS     HW          CM : FCC1
                I        S      .       .        .       .          SDM: SDM1
Sys            SDM Configuration
 0 Quit
 2             General
 3             ------------------------------------------------------------
 4 Logs        Platform:                          FT
 5             Console Login Greeting:            SDM Console
 6             Paging Space:                      256
 7
 8             CM Connectivity
 9             ------------------------------------------------------------
10             Connectivity type:                  DS512
11             CM IP address:                      47.105.155.1
12             EIU IP address (CM side):           Uncommissioned
13             EIU IP address (SDM side):          Uncommissioned
14 QuerySDM    SDM IP address:                     47.105.155.5
15 Locate      SDM-CM netmask:                     255.255.255.248
16             CM CLLI:                            FCC1
17 Help
18 Refresh     LAN Connectivity

  root
Time  19:48  MORE...
```

Other commands at the system menu level

Change is a hidden command for root users only. The CHANGE command modifies current system threshold values or modifies the time interval value that controls how often the performance log SDM620 is generated.

The parameters for changing system thresholds are ENTRYNUMBER (the number shown under # header of the item whose value you wish to change) and NEWTHRESHOLDVALUE (the new desired value). For example, CHANGE 7 95.

For example, type CHANGE LV SBA 120 to expand the current logical volume SBA by 120 Mbytes.

To change the performance log interval, type CHANGE TI and press the Enter key. Then type the new value and press the Enter key again. You are prompted to confirm the new value. The time interval must be entered in minutes. The valid range for this value is 5 to 20 160 minutes, (2 weeks). See ”Changing system thresholds” on page 4-188 for more information on how to change the performance log SDM620 time interval.

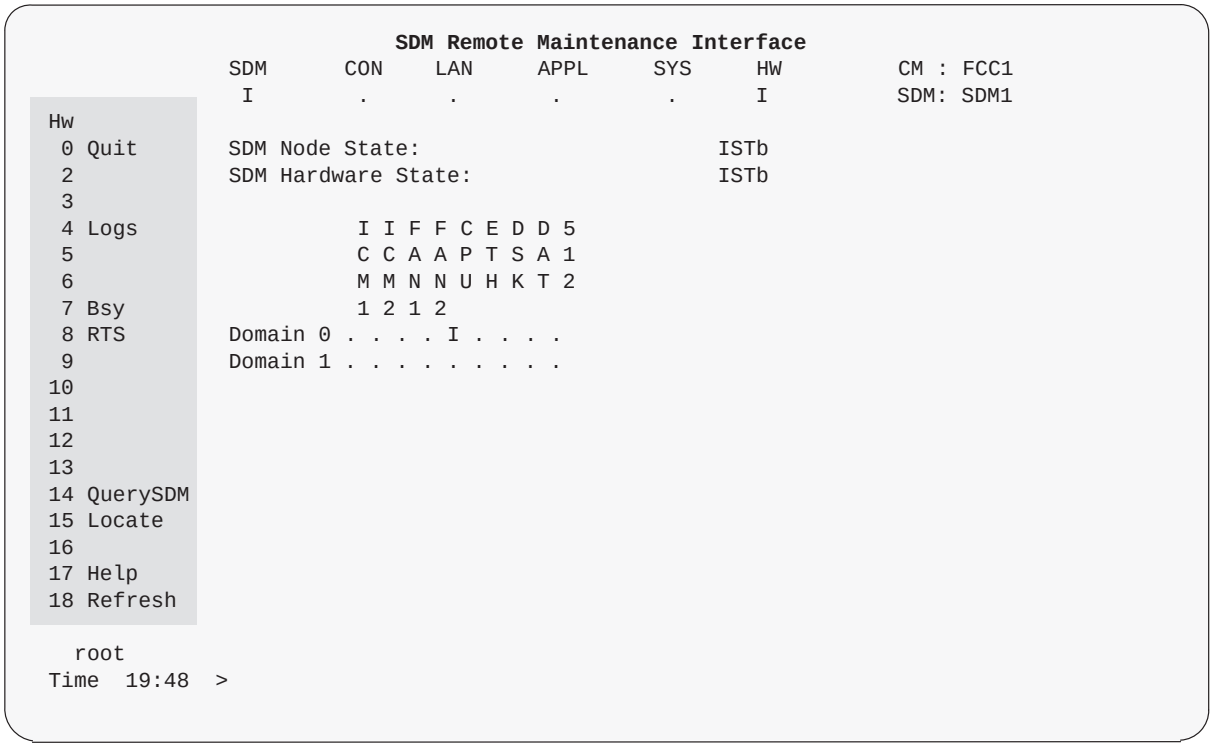
The default value for the time interval is 5 min. If a user enters a value of less than 5 minutes, a warning message appears on the RMI system menu and the system uses the default value of 5 min. The maximum value for the time interval is 20 160 minutes or 14 days.

Hardware menu level of the RMI

Figure 2-23 shows the hardware menu level of the RMI. This menu displays the status of hardware components on the SDM by deviceID in each domain. In the example shown, the hardware component is ISTb because the CPU controller module is ISTb. The overall SDM node state is also ISTb.

Select option 6 from the maintenance menu level of the RMI to access the hardware menu level. You can also access this menu by typing HW from any maintenance menu level of the RMI.

Figure 2-23
Hardware menu level



Logs at the hardware menu level

Figure 2-24 shows the static information that is displayed when the logs option is used. The logs option displays the current logs associated with the hardware devices. These logs describe the event, and the date and time it occurred. The most recent log is displayed when the SDM detects that a hardware device has been returned to the InSv state, or when a hardware

device is manually taken out of service. The order of the logs is predefined by base software. The log displays the suspected module, its location and PEC. It also indicates whether the module needs replacing, and displays other devices on the module and their state. Refer to table 2-7 on page 2-79 for more information about SDM logs and the required actions.

To display the logs, select option 4 or type LOGS at the system menu level of the RMI. The dynamic information shown in figure 2-23 disappears to make room for the static log information. Press the Enter key to scroll down the screen. When the last screen of log information is shown, press the Enter key to re-display the information that was previously displayed.

Figure 2-24
Logs at the hardware menu level

```
                        SDM Remote Maintenance Interface
                SDM      CON    LAN     APPL     SYS     HW         CM : FCC1
                 I        S      -        .        .       I         SDM: SDM1
Hw              Log information retrieved on Thu Oct 9 10:19:20 1997:
 0 Quit
 2              SDM0609 Hardware device detected 512(1)
 3                Tue Oct 7 14:20:47 1997
 4 Logs
 5              SDM309 Hardware device fault
 6                Device: CPU(1)
 7 Bsy            Device state: Fail
 8 RTS            Suspected module: CPUset (PEC:NTRX50FK)
 9                Location: Shelf:SDMM, Slot:10, Front
10                Other devices on module: none
11                Fault category: Fault on module
12                Reason: Voting delay loser (presumed BAD)
13                Tue Oct 7 06:57:21 1997
14 QuerySDM
15 Locate       SDM309 Hardware device out of service
16                Device: 512(o)
17 Help           Device state: Fail
18 Refresh        Suspected module: DS512 controller (PEC:NTRX50GA)

  root
Time  19:48     MORE...
```

QuerySDM at the hardware menu level

Figure 2-25 shows the static information that is displayed when the QuerySDM command with no parameters is used at the hardware menu level of the RMI. QuerySDM displays information on SDM configuration, including CM connectivity.

To use this command, select option 14 or type QUERYSDM. For more information on using this command with the parameters, FLT, LOADS, STATUS, and CONFIG, see page 2-72.

Note: QuerySDM at the hardware menu level of the RMI displays the same information as QuerySDM STATUS at any RMI maintenance menu level, and QuerySDM STATUS at the SDM MAP display level. See page 2-72 for more information on QuerySDM STATUS at the RMI, and page 2-11 for more information on QuerySDM STATUS at the SDM MAP display level.

Figure 2-25
QuerySDM at the hardware menu level

```
                        SDM Remote Maintenance Interface
                SDM      CON    LAN     APPL     SYS     HW         CM : FCC1
                 I        S      .       .        .       I         SDM: SDM1
Hw
 0 Quit         SDM Node State:                        ISTb
 2              SDM Hardware State:                    ISTb
 3
 4 Logs                    I F C E D D 5
 5                         C A P T S A 1
 6                         M N U H K T 2
 7 Bsy
 8 RTS           Domain 0 . . . . . . I
 9               Domain 1 . . F . . . I
10
11               A L S C     I F C E D D 5
12               P A Y O     C A P T S A 1
13               P N S N     M N U H K T 2
14 QuerySDM
15 Locate        . . . S  D0 . . . . . . I
16                        D1 . . F . . . I
17 Help
18 Refresh

  root
Time  19:48  >
```

Other commands at the hardware menu level

The following commands are also available at this level:

- Bsy busies a hardware device or module. Busying a specific device busies all devices on the same module. For example, if you busy the Ethernet LAN controller device on the I/O controller module, all subtending devices (disk and tape drive) are automatically busied. The parameters for the Bsy command are DOMAIN and DEVICENAME. DOMAIN is 0 if the module is in slots 1 to 8, or 1 if the module is in slots 9 to 16. DEVICENAME is the name of the device you wish to busy, as shown at the hardware menu level. The information derived from this command is displayed under the dynamic information. For example, BSY 0 ETH or 7 0 ETH. The FORCE option may be used with BSY to bypass error checks.

- Add and Del (delete) are hidden commands for root users only. These commands add and delete specified modules from the SDM. For more information on how to add or delete modules, see the procedures "Adding I/O controller modules" on page 4-64 and "Removing I/O controller modules" on page 4-72 in the "SDM maintenance procedures" chapter in this document.

  Note: For this product release, the I/O controller module (NTRX50FU) is the only module that can be added to the system. This module will not be functional until the next product release.

- RTS returns a device or module to service. The parameters for the RTS command are DOMAIN (0 if the module is located in slots 1 to 8, or 1 if the module is located in slots 9 to 16) and DEVICENAME (as displayed on the hardware menu level). The information generated by this command is displayed beneath the dynamic information.

Note: Hardware modules must be returned to service at low traffic periods. Returning them to service at high traffic periods can cause problems.

QuerySDM STATUS command

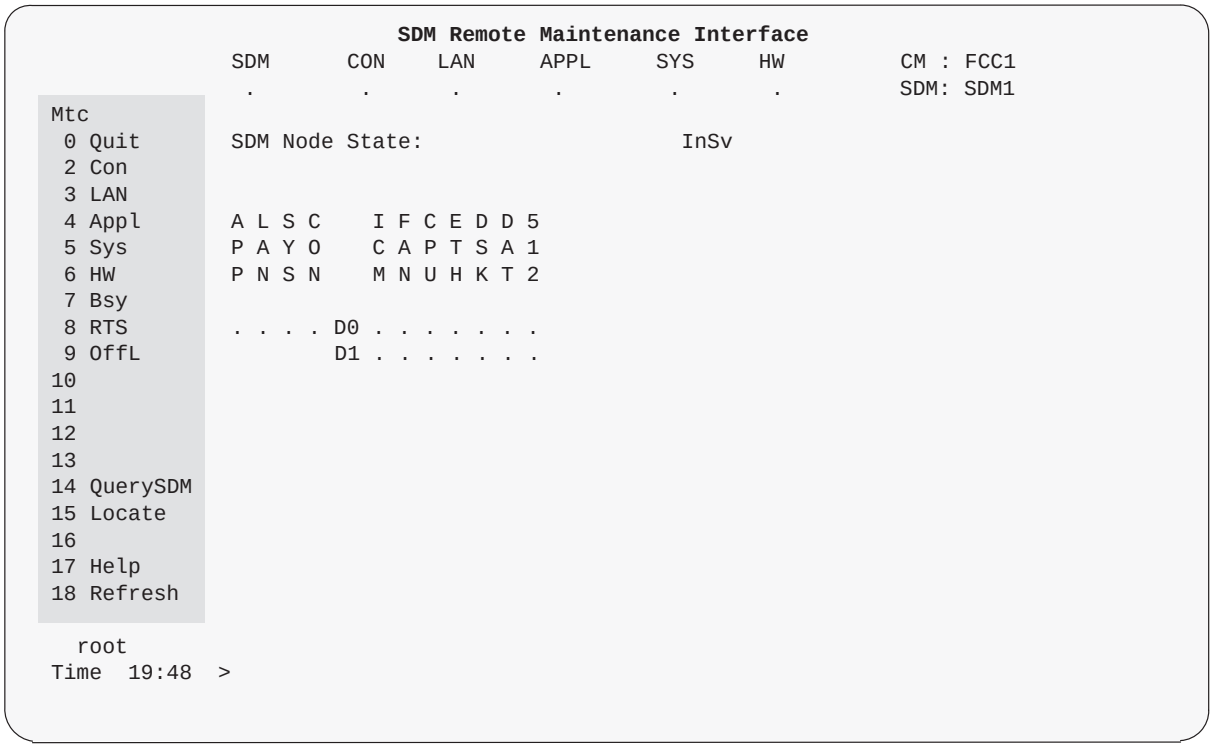
Figure 2-26 shows the static information that is displayed when the the QuerySDM STATUS command is invoked. QuerySDM STATUS can be invoked at any maintenance menu level of the RMI. QuerySDM STATUS displays the status of SDM applications, SDM to operating company LAN connectivity, system resources, and SDM-to-CM connectivity. Hardware status in each domain is also shown. See page 2-48 for information on SDM state indicators.

In the example shown, all components are InSv and all applications are running. Connections to the operating company LAN and the DCE server, as well as system resources are functioning normally. There are no hardware faults.

Select option 14 with the STATUS option from any maintenance menu level of the RMI to invoke this command. You can also access this menu by typing QUERYSDM STATUS. The information is displayed below any existing dynamic information that was displayed before the command was invoked. Use the Refresh command to delete the static information.

Note: QuerySDM STATUS displays the same information as QuerySDM at the hardware menu level of the RMI, and QuerySDM STATUS at the SDM MAP display level. See page 2-70 for more information on QuerySDM at the hardware menu level, and page 2-11 for more information on QuerySDM STATUS at the SDM MAP display level.

Figure 2-26
QuerySDM STATUS command



QuerySDM FLT command

Figure 2-27 shows the static information that is displayed when the QuerySDM command with the FLT option is invoked. QuerySDM FLT can be invoked at any maintenance menu level of the RMI. This command displays information that helps to isolate hardware, software and connectivity faults on the SDM. QuerySDM FLT displays the following information:

- the device or software package name where the fault resides
- the state of the device or software package
- the suspected module that contains the fault, and its location and PEC
- a process identification for the software fault
- other devices on the module, and their states
- a text reason detailing the fault (if available)
- a time stamp indicating the last state change

QuerySDM FLT displays the message “No local SDM fault to report” if there are no hardware, software, or connectivity faults on the SDM. If there

is only one type of fault on the SDM (for example, software) only the software faults appear on the display.

In the example shown, a cable fault exists on the LAN personality module. The state of the device, its location, and possible reason for the fault are given.

Select option 14 with the FLT option from any maintenance level of the RMI to invoke this command. You can also access this menu by typing QUERYSDM FLT. Some dynamic information may disappear when this command is invoked. Use the Refresh command to delete the static information displayed by this command.

Figure 2-27
QuerySDM FLT command

```
                        SDM Remote Maintenance Interface
                SDM      CON    LAN     APPL     SYS     HW         CM : FCC1
                 M         .      .       M        .       I         SDM: SDM1
Mtc
 0 Quit         SDM Node State:                     ManB
 2 Con
 3 LAN
 4 Appl         Hardware device out of service
 5 Sys            Device: ETH(1)
 6 HW             Device state: Fail
 7 Bsy            Suspected module: LAN personality module (PEC:NTRX50FS)
 8 RTS            Location: Shelf:SDMM, Slot:13, Back
 9 OffL           Other devices on module: none
10                Fault category: Fault on personality module
11                Reason: FTent: Personality Module Offline (cable fault occurred)
12                Wed Apr 30 17:42:22 1997
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh

  root
Time  19:48   >
```

QuerySDM LOADS command

Figure 2-28 shows the information that is displayed when QuerySDM with the LOADS option is invoked. QuerySDM LOADS can be invoked at any maintenance level of the RMI. This command lists all software loaded on the SDM, and helps to isolate application faults. In the example shown, all applications are running.

Select option 14 with the LOADS option from any maintenance menu of the RMI to invoke this command. You can also access this menu by typing QUERYSDM LOADS. Some dynamic information may disappear when this command is invoked. Use the Refresh command to delete the static information displayed by this command.

Note: QuerySDM LOADS displays the same information as QuerySDM at the application menu level of the RMI, and QuerySDM LOADS at the SDM MAP display level. See page 2-59 for more information on QuerySDM at the application level, and page 2-11 for more information on QuerySDM LOADS at the SDM MAP display level.

Figure 2-28
QuerySDM LOADS command

```
                          SDM Remote Maintenance Interface
               SDM      CON    LAN     APPL     SYS     HW          CM : FCC1
                .        .      .       .        .       .          SDM: SDM1
Mtc
 0 Quit        SDM Node State:                   InSv
 2 Con
 3 Lan
 4 Appl        # Package Description                    Version     State
 5 Sys           Platform Maintenance                   9.0.13.0    ----
 6 Hw          1 Table Access Service                   9.0.13.0    InSv
 7 Bsy         2 Operation Measurements                 9.0.13.0    InSv
 8 RTS         3 Log Delivery Service                   9.0.13.0    InSv
 9 OffL
10
11
12
13
14 QuerySDM
15 Locate
16
17 Help
18 Refresh

  root
Time  19:48  >
```

The following package state indicators are shown:

- "InSv" indicates that all package software is functioning, and no trouble conditions are reported.
- "IsTb" indicates that one or more software processes in the package have reported a trouble condition, or that one or more has failed.
- "ManB" indicates a package has been stopped manually.
- "OffL" indicates a package has been put in the offline state.

- "Fail" indicates all UNIX processes associated with a package have exceeded their daily threshold, and are no longer running.

QuerySDM CONFIG command

Figure 2-29 shows the information that is displayed when QuerySDM with the CONFIG option is invoked. QuerySDM CONFIG can be invoked at any maintenance menu level of the RMI. Use this command to determine configuration settings that were set during commissioning of the SDM. This command displays information on the following:

- the type of platform, the console login greeting, and paging space
- CM connectivity information, including CM and IP addresses, SDM-CM netmask, and CM CLLI
- operating company LAN configurations, including IP addresses, netmask, hostnames, LAN type, and whether FTP and telnet is enabled or disabled
- system threshold values

Select option 14 with the CONFIG option from any maintenance menu of the RMI to invoke this command. You can also access this menu by typing QUERYSDM CONFIG.

Figure 2-29
QuerySDM CONFIG command

```
                        SDM Remote Maintenance Interface
               SDM      CON    LAN     APPL     SYS     HW         CM : FCC1
                .        .      .       .        .       .         SDM: SDM1
Mtc            SDM Configuration
 0 Quit
 2 Con         General
 3 Lan         ------------------------------------------------------
 4 Appl        Platform:                          FT
 5 Sys         Console Login Greeting:            SDM Console
 6 Hw          Paging Space:                      256
 7 Bsy
 8 RTS         CM Connectivity
 9 OffL        ------------------------------------------------------
10             Connectivity type:                 DS512
11             CM IP address:                     47.104.123.1
12             EIU IP address (CM side):          Uncommissioned
13             EIU IP address (SDM side):         Uncommissioned
14 QuerySDM    SDM IP address:                    47.105.145.5
15 Locate      CM-SMD netmask:                    255.255.255.248
16             CM CLLI:                           FCC1
17 Help
18 Refresh     LAN Connectivity

  root
Time  19:48    MORE...
```

Locate command

Figure 2-30 shows the static information that is displayed when the locate command is invoked. Locate displays information on all modules in the SDM, and their locations. The dynamic information displayed on a menu before the Locate command was invoked may disappear to make room for the information generated by the Locate command. Press the Enter key to scroll down the screen. When the last screen of information is shown, press the Enter key to re-display the information that was previously displayed. Locate displays the following information:

- a description of the hardware device
- the module's location and slot number (if applicable)
- the module's PEC
- devices on the module

Select option 15 from any maintenance menu or type LOCATE to use this command.

Figure 2-30
Locate command

```
                              SDM Remote Maintenance Interface

                  SDM:      CON:     LAN:     APPL:    SYS:     HW      CM : FCC1
                   .         .        .        .        .        .      SDM: SDM1
 Mtc              Site Flr RPos Bay_id Shf  Description            Slot  EqPEC
  0 Quit          HOST 01  A02  CSDM   SDMM 512(0)                  01  NTRX50GA FRNT
  2 Con           HOST 01  A02  CSDM   SDMM                        01  NTRX50GH BACK
  3 Lan           HOST 01  A02  CSDM   SDMM ETH(0),DSK(0),DAT(0)   02  NTRX50FQ FRNT
  4 Appl          HOST 01  A02  CSDM   SDMM                        02  NTRX50FS BACK
  5 Sys           HOST 01  A02  CSDM   SDMM CPU(0)                 06  NTRX50FK FRNT
  6 Hw            HOST 01  A02  CSDM   SDMM                        06  NTRX50FD BACK
  7 Bsy           HOST 01  A02  CSDM   SDMM CPU(1)                 10  NTRX50FK FRNT
  8 RTS           HOST 01  A02  CSDM   SDMM 512(1)                 12  NTRX50GA FRNT
  9 OffL          HOST 01  A02  CSDM   SDMM                        12  NTRX50GH BACK
 10               HOST 01  A02  CSDM   SDMM ETH(1),DSK(1),DAT(1)   13  NTRX50FQ FRNT
 11               HOST 01  A02  CSDM   SDMM                        13  NTRX50FS BACK
 12               HOST 01  A02  CSDM   SDMM FAN1(0)                --  NTRX50FE FRNT
 13               HOST 01  A02  CSDM   SDMM FAN1(1)                --  NTRX50FF FRNT
 14 QuerySDM      HOST 01  A02  CSDM   SDMM ICM1(0)                --  NTRX50FG BACK
 15 Locate        HOST 00  A02  CSDM   SDMM ICM1(0)                --  NTRX50FH BACK
 16               HOST 01  A02  CSDM   SDME DSK2(0),DSK3(0)        02  NTRX50FU BACK
 17 Help          HOST 01  A02  CSDM   SDME                        02  NTRX50FS BACK
 18 Refresh       HOST 01  A02  CSDM   SDME DSK2(1),DSK3(1)        10  NTRX50FU FRNT

   root
 Time  19:48   MORE...
```

The list is sorted by shelf and slot numbers. The "SDMM" shelf value indicates that the module is located in the main chassis. The "SDME" shelf

value indicates that the module is located in the I/O expansion chassis. The description field contains the devices on the module and domain numbers.

SDM log reports

One type of log report provides information related to the SDM:

- SDM events are recorded internally to the SDM in a series of UNIX log reports (SDM logs). These log reports are local to the SDM, and do not appear in the generic DMS log utility stream. SDM logs are described in table 2-7 on page 2-79.

SDM logs

The SDM generates detailed customer logs that are available on the SDM RMI maintenance menu level and from the output of the SDM Log Delivery application. From the RMI maintenance menu level, logs are available from the CON/LAN/APPL/SYS and HW levels. SDM logs fall into three categories: trouble (TBL) logs, state change logs, and information (INFO) logs.

Trouble logs

TBL logs (SDM3xx) provide an indication of some type of fault for which corrective action can be taken. These logs are generated for connectivity failures, system resource problems, and application software and hardware failures. Each of these trouble conditions corresponds to an alarm on the SDM RMI alarm banner. When a TBL log is generated by the SDM, the alarm is displayed under the appropriate component on the RMI alarm banner to reflect the fault condition.

State change logs

State change logs (SDM5xx) provide information about SDM state changes to InSv, ManB, ISTb, and SysB. While state changes from InSv to ISTb or SysB require corrective action, the logs indicating these changes do not provide detailed information about the reason for the state change. Specific information is contained in the TBL logs.

When the SDM or the SDM Log Delivery is returned to service from a ManB state, some logs may be delivered with the CM_CLLI in the Office ID field of the log header, instead of the datafilled LOG_OFFICE_ID. This occurs only for logs generated by SDM applications, and only occurs until at least one log has been delivered that originated from a CM-based application. The discrepancy corrects itself as soon as the first CM log is received on the SDM.

Info logs

INFO logs (SDM6xx) provide information about events that do not normally require corrective action. These logs are generated for system restarts, non service affecting state changes, and for events that clear TBL logs.

Table 2-7 lists the SDM logs generated by the SDM, describes the triggers for each log, and provides a summary of the actions to take.

Table 2-7
SDM logs generated by the SDM

Log	Trigger	Action
SDM300	The connection from the SDM to the CM or the operating company LAN server(s) is down.	See Fault diagnosis with SDM-CM communication out of service on page 2-94. Contact your SDM system administrator or Nortel for assistance.
SDM301	The maintenance system detects that a logical volume is not mirrored.	Check hardware faults, as mirroring may be lost due to a hard disk failure on the SDM. If a disk has just been replaced and brought back in-service, the system may take more than 15 minutes to restore mirroring.
SDM302	The SDM has detected that a system software resource has exceeded its threshold.	Use the procedure for clearing an APPL SDM minor alarm on page 4-3 in the "SDM maintenance procedures" chapter of this document to isolate and clear the problem.
SDM303	An SDM application or software has failed more than three times in a day, or has declared itself to be in trouble.	Users with root permissions can examine the log files in /usr/adm to determine the cause of the process failure. If required, contact your SDM system administrator or Nortel for assistance.
SDM304	The SDM Log Delivery application cannot deliver logs to the specified UNIX file.	Use the Log Delivery online commissioning tool (logroute) to verify the existence and validity of the device name. See page 2-82 for more information on the logroute tool or the procedure "Log Delivery Device commissioning" on page 4-101. If required, contact your SDM system administrator or Nortel for assistance.

—continued—

Table 2-7
SDM logs generated by the SDM (continued)

Log	Trigger	Action
SDM306	SDM Table Access software has detected that the CM software load is incompatible with the SDM software load.	Upgrade the CM software to a version that is compatible with the SDM software. ***Note:*** SDM software should never be at a lower release level than CM software.
SDM308	Automated incremental backup (I-tape) or manual system image backup (S-tape) has failed.	Check to ensure that the backup tape is inserted. If the problem cannot be isolated, perform the incremental backup manually. See the procedure ”Creating SDM backup tapes - Manual incremental backup” on page 6-39 in this document. If required, contact your SDM system administrator or Nortel for assistance.
SDM309	A hardware device is faulty or has been manually taken out of service.	Use the QuerySDM commands from the MAP display. Refer to the appropriate procedure in the “SDM hardware replacement procedures” of this document. For all other faults, check the cabling to the module. If you cannot determine the reason for the fault, contact your next level of support.
SDM315	SDM Table Access application has detected corruption in the Data Dictionary on the CM.	Contact your next level of support.
SDM317	A Distributed Computing Environment (DCE) problem is detected.	Contact your next level of support to determine the cause of the failure.
SDM500	Indicates the initial startup of the SDM. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM501	Indicates an SDM state change to in service (InSv). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None

—continued—

Table 2-7
SDM logs generated by the SDM (continued)

Log	Trigger	Action
SDM502	Indicates an SDM state change to manual busy (ManB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM503	Indicates an SDM state change to system busy (SysB). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure ”Clearing MAP alarms triggered by the SDM - APPL SDM critical” on page 4-29 in this document.
SDM504	Indicates an SDM state change to in-service trouble (ISTb). This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	Refer to the procedure ”Clearing MAP alarms triggered by the SDM - APPL SDM minor” on page 4-3 in this document.
SDM505	Indicates an SDM state change to offline (OffL) state. This log is included in the SDM Log Delivery log stream, but does not appear on the RMI.	None
SDM550	Indicates an SDM node status change. One or more of the following can cause the status change: • SDM node state • hardware device • software component • application	Refer to the following procedures in this document, depending on the alarm code displayed: • ”Clearing MAP alarms triggered by the SDM - APPL SDM critical” on page 4-29 when a critical alarm is generated. • ”Clearing MAP alarms triggered by the SDM - APPL SDM minor” on page 4-3 when a minor alarm is generated.
SDM600	The connection from the SDM to the CM or the operating company LAN server(s) has been re-established. This log is generated only after a connectivity failure has been corrected, and not at system startup.	None
SDM601	The maintenance system detects that mirroring has been re-established after a logical volume mirroring failure.	None

—continued—

Table 2-7
SDM logs generated by the SDM (continued)

Log	Trigger	Action
SDM602	A system software resource has returned below its alarm threshold (see also SDM 302 log).	None
SDM603	A fault on an application process has cleared (see also SDM 303 log).	None
SDM604	The SDM Log Delivery application generates this log when the CM does not have enough CPU time to format logs, and discards the logs.	No immediate action is required. However, if large numbers of logs are lost, contact Nortel for assistance.
SDM608	An automated incremental software backup (I-tape) or system image backup (S-tape) has completed.	None
SDM609	A hardware device has been returned to the in-service state.	None
SDM616	A log delivery connection attempt was rejected.	None
SDM617	A Distributed Computing Environment (DCE) problem is cleared.	None
SDM620	Reports SDM system performance data such as CPU usage, number of processes, swap space occupancy, and logical volume capacities.	None
SDM650	SDM link maintenance requests the logging of a failed link maintenance action. An example of a link maintenance action is the system testing of a link.	None

—end—

SDM Log Delivery application

The SDM Log Delivery application provides access through the SDM to the generic DMS log stream, and local SDM logs. The log stream is available from the SDM in several ways:

- The log stream can be directed to up to ten operations support systems (OSS) through TCP/IP.
- The log stream can be directed to up to ten UNIX files on the SDM.

A maximum of ten devices (UNIX files and TCP/IP links) can be commissioned.

Logreceiver tool

The logreceiver tool is a client application, included with the Log Delivery application, that runs on a remote workstation and receives logs sent to the workstation from an SDM by the operating company LAN. The logreceiver tool can either store these logs in a file or display them on the screen. To run logreceiver in this release, the workstation must be an HP 700/800 workstation running HP-UX 9.05 or later, or a Sun SPARC workstation running Solaris version 2.4 or later.

To route logs from an SDM to a workstation, the SDM must be configured to send logs to a TCP device, whose IP address is the IP address of the workstation, using the logroute commissioning tool. A port number must be included when this TCP device is configured. (For more information, see ”Commissioning TCP-client devices for Log Delivery” on page 2-88).

The logreceiver tool must also be installed on the workstation before logs can be routed from an SDM to that workstation. Refer to the procedure ”Installing the logreceiver tool” on page 6-93 in the “SDM system administration procedures” chapter of this document, for detailed instructions on how to install the logreceiver tool on a workstation.

Once the logreceiver tool has been installed on the workstation and the SDM has been configured to send logs to a TCP device, the logreceiver tool must be started on the workstation. The following options are available for running logreceiver:

- display logs directly on the workstation screen as they are generated
- store logs in a file for viewing when convenient by
  - — displaying the file using UNIX commands

With each of these options, a command must be issued at the workstation to start the logreceiver tool’s execution. In all cases, the command must include a port number. The port number must be the same as the port number used in configuring the TCP device on the SDM. The port number must not be in use for any other purpose on the workstation, otherwise the following error message appears, `Failed to listen for connection request on port xxx, exiting` will result. You will then have to change the port number used in configuring the TCP device on the SDM.

To check the port numbers in use, type

>more /etc/services

and press the Enter key. You will see the list of port numbers in use on the display. To scroll through the display, press the Enter key again.

To display logs directly on the workstation screen as they are generated, type

>logreceiver *port*

and press the Enter key.

where

port is the port number used when configuring the TCP device on the SDM

A message `Accepted connection request from host xxx` is displayed just before the first log received is written to the screen.

ATTENTION

The valid port range for a TCP device is 5001–32767.

To store logs in a file, type

>logreceiver *port* -f *filename*

and press the Enter key.

where

port is the port number used when configuring the TCP device on the SDM

filename is the name of the file

Note 1: If the file does not yet exist, it will be created automatically. The logs from the SDM will be stored in this file. If the file already exists, the logs from the SDM will be appended to it provided its UNIX access permissions allow writing to it. In either case, a messsage `Accepted connection request from host xxx` will be displayed on the screen just before the first log received is written to the file.

Note 2: If the file already exists, but its permissions do not allow writing to it, an error message `Failed to open file filename` is displayed on the screen.

Note 3: The file continues to fill up until either the logreceiver execution is terminated, or all free storage in the file system is exhausted. In the latter case, the logreceiver execution is terminated automatically, and you must remove the file or free up some storage.

In all these cases, type “control -c” and press the Enter key to terminate execution of the logreceiver tool.

Logreceiver cannot execute simultaneously from two different UNIX windows on a workstation using the same port number. Logreceiver can execute simultaneously from two or more different UNIX windows on the same workstation, provided a different port number is used in each execution. The executions may involve either the same or different SDMs. The workstation determines the SDM solely from the port number. If two or more SDMs are configured to send logs to the same workstation using the same port number, the workstation will connect to the SDM whose configuration was activated first. Do not configure two SDMs to the same workstation using the same port number.

Log Delivery commissioning

Log Delivery operating parameters are controlled by an online SDM commissioning tool, which is used to set up the application, and can also be used to view or modify the parameters. To access the logroute tool, log in to the RMI as maint, and enter the command “logroute”.

For more information on configuring the Log Delivery service, refer to the procedures ”Log Delivery device commissioning” on page 4-101, ”Log Delivery global parameters commissioning” on page 4-124, or ”Log Delivery CM configuration file commissioning” on page 4-134 in the SDM Maintenance procedures chapter of this book.

The Log Delivery logroute tool allows customization of the following:

- global application parameters including buffer size, reconnect timeout value, lost logs threshold (number of lost logs before a system log is generated), ASCII line delimiter and log delimiter characters, and the number of days to keep log files
- the incoming log stream from the CM, to add or delete individual logs
- client device parameters, including device type (UNIX file or TCP output), parameters specific to the device type, log output format (standard [STD] or switching control center 2 [SCC2]), and the log set to be sent to the device

The Log Delivery logroute tool includes an on-line help facility that provides the valid ranges (and default values, where applicable) for each customizable parameter. The commissioning tool is subdivided into three functional areas:

- Device List (menu option 1)
- Global Parameters (menu option 2)
- CM Configuration File (menu option 3)

Note: When any commissioning changes are saved, the Log Delivery application must be busied and returned to service for the new settings to take effect. The Log Delivery application is unavailable for a brief period while this takes place.

Figure 2-31 shows the top-level Log Commissioning menu that is displayed when you access the Log Delivery commissioning tool.

Figure 2-31
Log Delivery commissioning tool

```
                          Logroute Main Menu


                      1 – Device List
                      2 – Global Parameters
                      3 – CM Configuration File









c:change menu, q:quit, h:help, s:save changes

      Warning:   You must save, then BSY and RTS the Log Delivery
      ========   application for any changes to take effect.

Enter command ==>
```

Log Delivery device commissioning list

The Device List menu specifies the output devices for Log Delivery, and the device-specific operating characteristics for each defined device. When you access this menu, the Log Delivery output devices currently defined are displayed. At initial commissioning time, no output devices are defined, and all required output devices must be specified. This menu can also be used to add or delete devices, or to select already-defined devices to change their specifications. For more information on Log Delivery device commissioning, refer to the procedure ”Log Delivery device commissioning” on page 4-101.

Up to 10 output devices (UNIX files and TCP/IP links) in total can be commissioned. This total of 10 can be made up of any combination of UNIX files and TCP/IP links.

Figure 2-32 shows an example of the topmost Device List menu. In this example, one output device (a TCP/IP) has already been commissioned.

Figure 2-32
Log Delivery device list commissioning menu

```
                              Device List

Devices:                                                    Type:
1 –  HOST:  47.208.7.54                PORT : 5001          TCP









c:change device, a:add device, d:delete device, q:quit, h:help, m:main

Enter command ==>
```

The Device List menu provides access to the following device-specific sub-menus:

- TCP Device defines TCP/IP output links to OSSs. For each TCP/IP link, the IP address of the OSS host machine, the port number to be used on that machine, and the log format must all be defined.
- File defines SDM-resident UNIX output files. The filename and log format must be defined for each UNIX file.

At this menu, you can select a device that has already been defined to view or modify its current parameters, delete a device that is currently defined, or add a new device. If you choose to add a new device, you are prompted to enter the device type (TCP or file).

When you select a device that is already defined, or after you specify the type of device to add, a sub-menu is then displayed that is specific to the device type. These sub-menus are described in the following subsections:

- ”Commissioning TCP client devices for Log Delivery” on page 2-88
- ”Commissioning file client devices for Log Delivery” on page 2-89

Commissioning TCP client devices for Log Delivery

Figure 2-33 shows an example of the TCP Device menu, with one device already defined. All logs are being routed to this device.

Figure 2-33
Log Delivery commissioning – TCP Device menu example

```
                              TCP Device


Device Parameters   1 – HOST IP    : 47.208.7.54
                    2 – PORT       : 5001
                    3 – FORMAT     : STD

Log Routing         ADDREP ALL









c:change parameter, a:add log routing, d:delete log routing
f:forward, b:back, q:quit, h:help, p:previous menu, m:main menu

Enter command ==>
```

By default, each device receives no logs at initial commissioning; that is, all logs are suppressed. To route logs to a device, use the “add log routing” command. Two different types of log routing entries can be added:

- addrep, which puts additional logs into the incoming log stream for the device
- delrep, which suppresses logs from the incoming log stream

The incoming log stream is the cumulative result of all existing log routing entries for the device, applied in sequence. Addrep and delrep can be followed either by ALL, which adds or removes the entire log stream, or by a specific log or log type.

Commissioning file client devices for Log Delivery

Figure 2-34 shows an example of the File device menu, with one device already defined. No logs are being routed to this device.

Figure 2-34
Log Delivery commissioning – File device menu example

```
                              File


Device Parameters   1 – FILENAME   : /data/logs/File1
                    2 – FORMAT     : STD

Log Routing









c:change parameter, a:add log routing, d:delete log routing
f:forward, b:back, q:quit, h:help, p:previous menu, m:main menu

Enter command ==>
```

By default, each device receives no logs at initial commissioning; that is, all logs are suppressed. To route logs to a device, use the "add log routing" command. Two different types of log routing entries can be added:

- addrep, which puts additional logs into the incoming log stream for the device
- delrep, which suppresses logs from the incoming log stream

The incoming log stream is the cumulative result of all existing log routing entries for the device, applied in sequence. Addrep and delrep can be followed either by ALL, which adds or removes the entire log stream, or by a specific log or log type.

To remove log routing entries, use the delete log routing command.

Log delivery file storage

A Log Delivery stream routed to a UNIX file device on the SDM is stored in the directory /data/logs. When you define the filename using the commissioning tool, the filename automatically begins with /data/logs. When defining the filename, you can either append a file name to /data/logs

or append a subdirectory name, followed by a filename if you are the root user (subdirectory must already exist). For example, to store the logs in a file named File1 with no additional directory structure, append File1. If you wish to store the file in a subdirectory called CMlogs, for example, append CMlogs/File1.

Log Delivery UNIX files are automatically closed (and a new file started) at noon and midnight each day. The closed files are appended with a suffix; either <date>.am or <date>.pm, depending on when the file was closed. (<date> is the calendar date the file was closed).

The closed files remain stored until manually removed, or until they are automatically removed when they reach their expiry date. The default expiry date is five days after file closure. This value can be globally changed by accessing the Global Parameters menu of the Log Delivery commissioning tool, and modifying the parameter “Number of days to keep log files”.

Log Delivery global commissioning parameters

The Global Parameters menu allows you to configure operating characteristics that apply to the Log Delivery application as a whole. These parameters apply to all Log Delivery output devices and are independent of device-specific parameters. Figure 2-35 shows the default values for Global Parameters commissioning menu. For more information on configuring the Log Delivery global parameters refer to the procedure ”Log Delivery global parameters commissioning” on page 4-124.

The global parameters are set to default values at initial installation and should not require modification in most cases. The ranges are as follows:

- buffer size (number of logs): 50 to 300
- reconnect timeout value (secs): 1 to 3600
- lost logs threshold: 1 to 300
- number of days to keep log files: 1 to 45

The following global parameters are represented by ASCII character codes:

- incoming end of line character
- outgoing end of line characters
- start of log characters
- end of logs characters

These parameters can be modified according to your requirements. The default values of 10 and 13 shown in figure 2-35 represent line feed (go to the next line) and carriage return.

Figure 2-35
Log Delivery global parameters commissioning menu

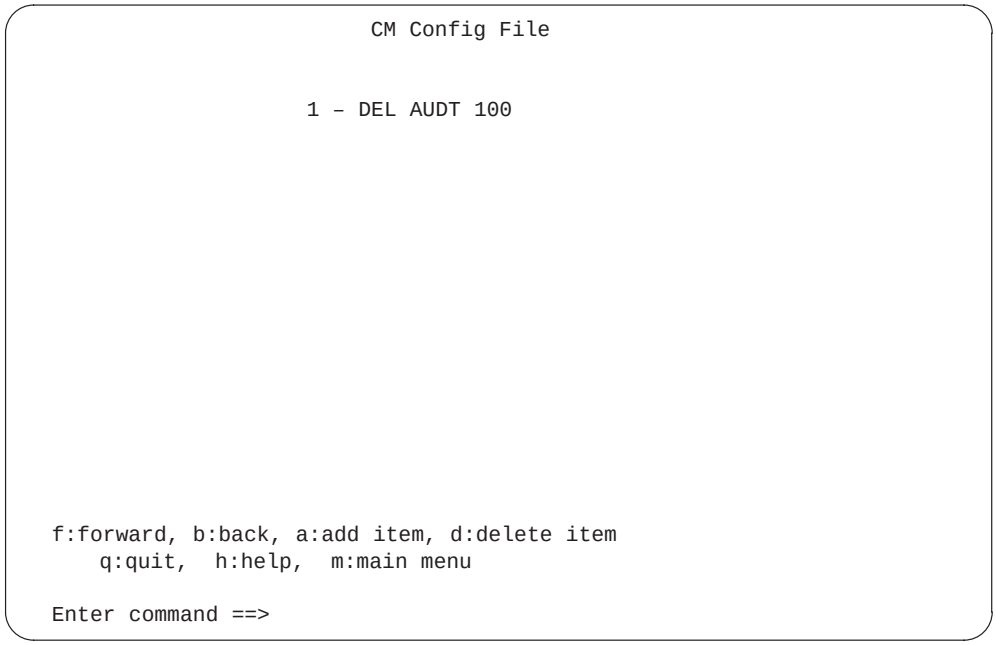
```
                        Global Parameters



      1 – Buffer size (number of logs)    :   150
      2 – Reconnect timeout value (secs)  :   15
      3 – Lost logs threshold (NT only) :     100
      4 – Incoming end of line character  :   10
      5 – Outgoing end of line characters :   10 13
      6 – Start of log characters         :   10 13
      7 – End of logs characters          :   10 13
      8 – Number of days to keep log files:   5









   c:change item,  q:quit,  h:help,  m:main

   Enter command ==>
```

Log Delivery CM configuration file commissioning parameters

The CM configuration file menu is used to add or delete log reports from the incoming log stream from the computing module (CM) to the Log Delivery application. At initial commissioning, all logs in the CM log stream are included by default, and this parameter does not require manual definition unless you wish to modify the incoming global log stream. For more information on configuring the Log Delivery CM configuration file commissioning parameters, see the procedure ”Log Delivery CM configuration file commissioning” on page 4-134.

Figure 2-36 shows an example of the CM configuration file commissioning menu. In this example, one log report (AUDT 100) has been deleted from the incoming CM log stream.

Figure 2-36
Log Delivery CM configuration file commissioning example



Troubleshooting Log Delivery problems

This section describes fault conditions affecting Log Delivery operation and how to isolate and clear them.

Lost logs

Lost logs can be detected by examining the sequence numbers of the logs at a client output device and determining if they are sequential. If they are not sequential, logs are likely being lost. To clear the problem, access the Log Delivery commissioning tool, select the Global Parameters menu, and increase the buffer size.

No logs being received at a Log Delivery client

If no logs are being received at a Log Delivery client, check the following Log Delivery commissioning parameters:

- At the Device Parameters menu of the Log Delivery commissioning tool, verify that the client is defined, and that the log stream for the client is defined.

Logs not formatted properly

If the log reports at a Log Delivery client device are not formatted correctly, access the Log Delivery commissioning tool and check the following:

- At the Device Parameters menu, verify that the correct log format has been commissioned for the device (STD or SCC2).

- At the Global Parameters menu, check that the parameters for start and end of line, and start and end of log, are set correctly.

SDM troubleshooting strategy

ATTENTION

The information contained in this section is an overview only. Use the detailed procedures provided in this document to isolate and clear any SDM faults.

This section summarizes troubleshooting information for the SDM fault-tolerant platform in the following subsections:

- ”Fault reporting” on page 2-93 describes the ways in which SDM faults may be visible.
- ”Fault diagnosis with SDM-CM communications in service” on page 2-94 describes the ways in which SDM faults may be visible when SDM-CM communications is in service, and provides a brief overview on diagnosing such faults.
- ”Fault diagnosis with SDM-CM communications out of service” on page 2-94 describes the ways in which SDM faults may be visible when SDM-CM communications is out of service, and provides a brief overview on diagnosing such faults.
- ”Fault diagnosis with the SDM out of service” on page 2-94 describes the ways in which SDM faults may be visible when the SDM is out of service. It also provides pointers to procedures and information in this document to isolate and clear such faults.
- ”Hardware LED status indicators” on page 2-95 describes the meaning of the LED status indicators on the SDM fault-tolerant hardware.
- ”State mismatches between the CM and the SDM” on page 2-102 describes the conditions under which an SDM state mismatch can occur, how a mismatch condition is handled, and a comparison of meanings of SDM node states at the MAP interface and the RMI.

Fault reporting

All SDM faults are visible at the MAPCI SDM display. All service-related faults are reported under the APPL alarm banner. SDM faults are also visible at the RMI, and by status LED indicators provided on the SDM hardware. Power-related and thermal-related SDM problems are also reported by the EXT alarm, and by the office alarm system.

The RMI is accessible from a local or remote VT100 console, or from the operating company LAN through telnet (telnet access must be enabled).

Fault diagnosis with SDM-CM communications in service

The following indicators are displayed when faults occur, and communications from the SDM to the CM are in service:

- APPL SDM minor alarm at the MAP display
- SDM In Service LED is on; component Out of Service LED is on if hardware has failed
- SDM state is ISTb at the RMI

If the SDM and the CM are able to communicate successfully by at least one of the four DS512 links from the SDM to the MS, all SDM fault conditions can be isolated from the MAP display by accessing the SDM at the MTC;APPL;SDM level, and issuing the QuerySDM FLT command.

If required, the MAP-based SDM remote login functionality can be used to perform any required state changes of individual hardware elements before and after physical replacement. Hardware state changes can also be made at the RMI. Either of these two interfaces can also be used to stop and restart SDM applications, if required.

Fault diagnosis with SDM-CM communications out of service

The following indicators are displayed when faults occur, and communications from the SDM to the CM are out of service:

- APPL SDM critical alarm at the MAP display
- SDM state at the MAP display indicates “Links OOS: 4”, combined with the qualifier “The SDM is not responding” or “NA”
- SDM System in Service LED is on

If the SDM is in service, but is unable to communicate with the MS, the communications problem must first be examined using the MTC;MS level of the MAP display. If required, further diagnosis of the communications problem can be performed using the RMI, and by physical inspection of the link hardware.

Note: Because there are four DS512 links available, with fault-tolerant hardware on the MS and SDM sides of the links, this scenario is highly unlikely.

Fault diagnosis with the SDM out of service

The following indicators are displayed when faults occur with the SDM out of service:

- APPL SDM critical alarm at the MAP display
- SDM state at the MAP display indicates “The SDM is not responding”

- SDM System In Service LED is off
- EXT alarm at the MAP display if the fault is power-related or due to a thermal shutdown

If the SDM is out of service, the problem can be isolated using a local or remote console, and by examining the status LED indicators provided on the SDM hardware.

The following information will assist you in diagnosing faults when the SDM is out of service:

1 If a APPL SDM critical alarm at the MAP display is present, refer to the appropriate alarm clearing procedure on page 4-29 in the “SDM maintenance procedures” chapter of this document to isolate and clear the alarm.

2 If the SDM state at the MAP display indicates “The SDM is not responding”, refer to the following:

— QuerySDM command reference information on pages 2-11 and 2-49

— SDMRLogin overview section on page 2-16

— the RMI overview on page 2-34

3 If the SDM System In Service LED is off, refer to the following:

— the procedure ”Clearing MAP alarms triggered by the SDM - APPL SDM critical” on page 4-29 in the “SDM maintenance procedures” chapter of this document

— the generic MS alarm clearing procedures provided with your DMS switching system

— the connectivity (Con) menu level of the RMI

4 If an EXT alarm is present at the MAP display due to a power-related fault or a thermal shutdown, refer to the following:

— the procedure ”Clearing MAP alarms triggered by the SDM - APPL SDM critical” on page 4-29 in the “SDM maintenance procedures” chapter of this document

— the procedure ”Clearing MAP alarms triggered by the SDM - Ext FSP major” on page 4-49 in the “SDM maintenance procedures” chapter of this document

— hardware LED information on page 2-95

Hardware LED status indicators

The SDM fault-tolerant platform is equipped with a number of LEDs, which provide information on the status of SDM hardware resources. These

include LEDs visible on both the front and rear of the main and I/O expansion chassis.

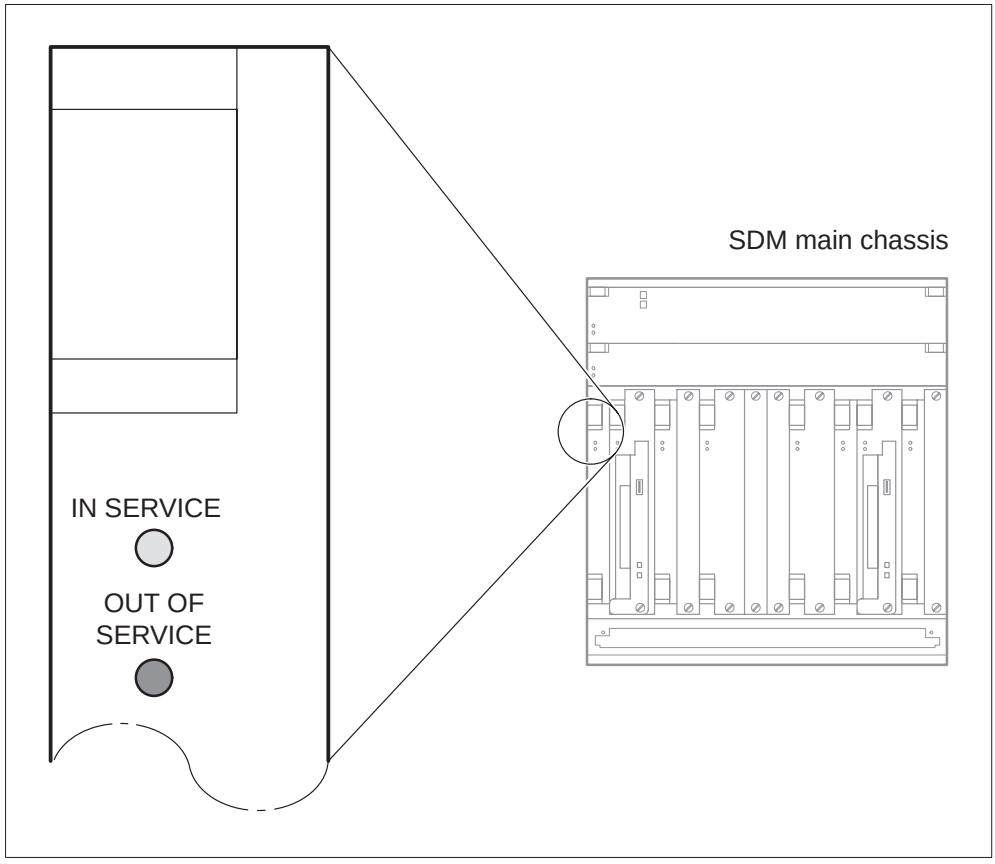
Controller module LEDs

The In Service (green) LED and the Out of Service (red) LED on a controller module can be on, off or flashing. The controller modules at the front of both the main chassis and the I/O expansion chassis, contain these LEDs. The fan tray units in each chassis also contain these LEDs.

Note: The I/O controller module (NTRX50FQ) also contains LEDs on its tape drive. Refer to the procedure ”Cleaning the SDM-DAT drive” on page 4-55 for further information on the meaning of these LEDs.

Figure 2-37 shows the two LEDs that are visible on each controller module.

Figure 2-37
Status LEDs visible on controller modules



Interconnect module LEDs

The In Service (green) LED and the Out of Service (red) LED on an interconnect module (ICM) can be on or off. The ICMs located at the back of both the main and the I/O expansion chassis contain these LEDs.

Figure 2-38 shows the two LEDs that are visible on each interconnect module.

Figure 2-38
Status LEDs visible on interconnect modules

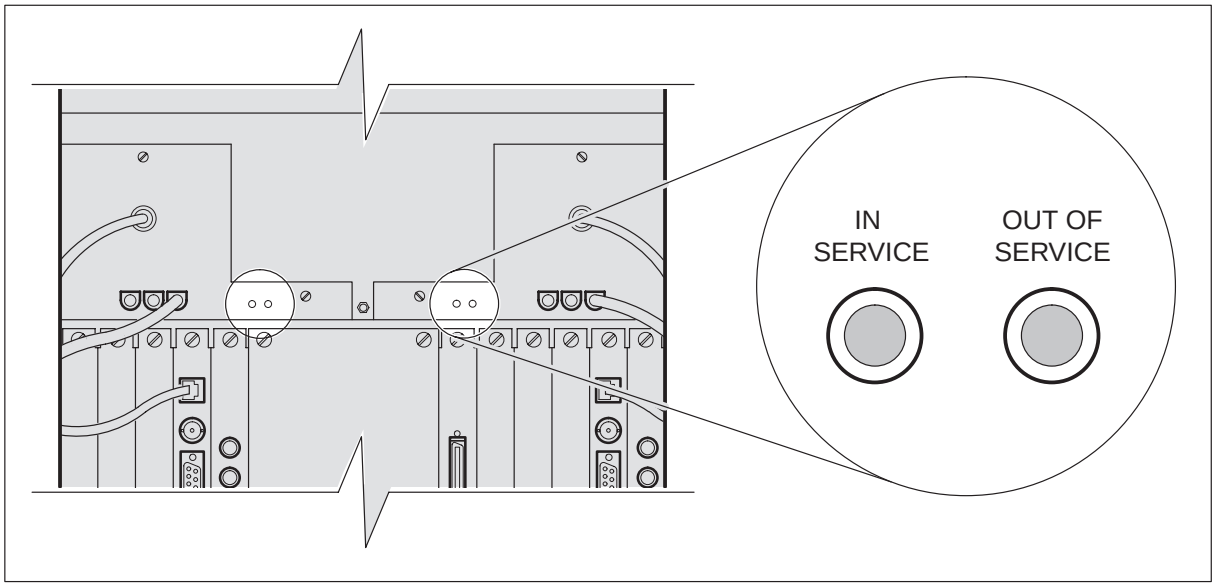


Table 2-8 shows the various combinations of controller module and ICM LEDs, and their meanings.

Table 2-8
SDM controller module and ICM LEDs

In Service (green) LED	Out of Service (red) LED	Meaning
on	off	The module is providing service to the system, and functioning normally.
off	off	The module is in an undefined state for one of the following reasons: • The module has passed its power-on selftest and is awaiting a command. • The module has been deleted from the system, but it is still on the shelf.
on	on	The power-on selftest diagnostic is running on the module, or the module has failed its power-on selftest.
off	on	The module is not providing service to the system for one of the following reasons: • A fault that was detected by the module has been acknowledged. • The module has been taken offline by a command. ***Note:*** Immediately after a fault occurs it is unacknowledged. Within several seconds, the SDM becomes aware of the fault. When this occurs, the fault is acknowledged.
flashing	off	The module is being reintegrated into the system.
off	flashing	The module is not providing service to the system. A fault that was detected by the module has not been acknowledged.

—end—

System LEDs

The System In Service (green) LED and the Component Out of Service (red) LED can be either on, off or flashing. Only the fan tray in the main chassis contains system LEDs. Figure 2-39 shows the LEDs that are visible on the fan tray units located in the front of the main chassis.

Figure 2-39
Fan tray LEDs

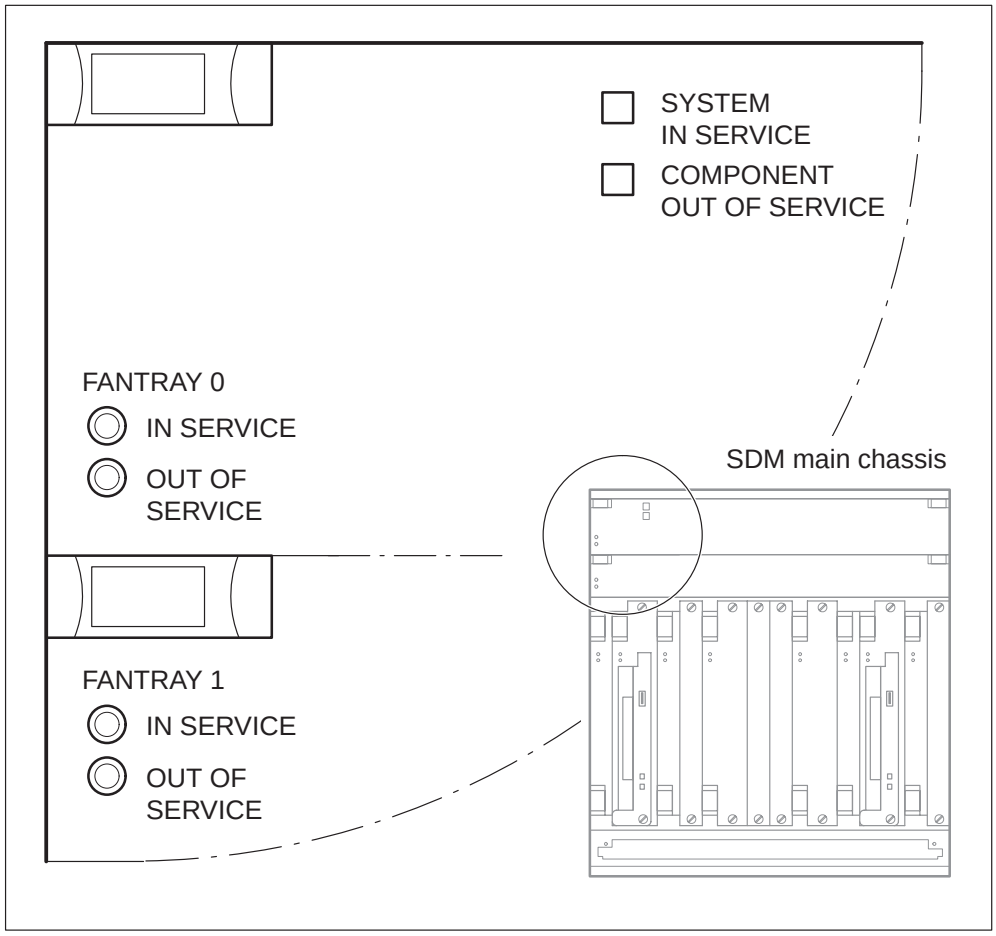


Table 2-9 describe the various states of the System In Service and the Component Out of Service LEDs, and their meanings.

Table 2-9
SDM system LEDs

System In Service (green) LED	Component Out of Service (red) LED	Meaning
on	off	The system is running, indicating the following: • There are no software or hardware modules that are out of service due to unacknowledged or acknowledged faults or offline commands. • No software or hardware modules are being reintegrated into the system. ***Note:*** Immediately after a fault occurs it is unacknowledged. Within several seconds, the SDM becomes aware of the fault. When this occurs, the fault is acknowledged.
off	off	The system is not providing service because it has just been powered on, or has encountered a fatal fault.
off	on	The system is not providing service because it is trying to boot the system software.
off	flashing	The system is not providing service because a failure has occurred while booting system software.
on	on	The system is running, however, at least one software or hardware module is out of service due to an acknowledged fault or an offline command. This state also indicates the following: • No software or hardware modules are out of service because of unacknowledged faults. • No software or hardware modules are being reintegrated into the system. ***Note:*** Immediately after a fault occurs it is unacknowledged. Within several seconds, the SDM becomes aware of the fault. When this occurs, the fault is acknowledged.

—continued—

Table 2-9
SDM system LEDs (continued)

System In Service (green) LED	Component Out of Service (red) LED	Meaning
on	flashing	The system is running. No software or hardware modules are being reintegrated into the system. This state also indicates the following: • At least one software or hardware module is out of service because of unacknowledged faults. • Some software and/or hardware modules may be out of service due to acknowledged faults or offline commands.
flashing	off	The system is running, however, at least one CPU controller module or I/O controller module is being reintegrated into the system. This state also indicates that no software or hardware modules are out of service due to unacknowledged or acknowledged faults, or offline commands.
flashing	on	The system is running. There are no software or hardware modules that are out of service due to unacknowledged faults. This state indicates the following problems have occurred: • Some software and/or hardware module is out of service because of acknowledged faults or offline commands. • At least one software or hardware module is being reintegrated into the system.
flashing	flashing	The system is running, however, the following problems have occurred: • At least one software or hardware module is out of service because of unacknowledged faults. • At least one software or hardware modules are being reintegrated into the system. • Some software and/or hardware module may be out of service due to acknowledged faults or offline commands.

—end—

State mismatches between the CM and the SDM

Under normal operating conditions, the SDM node states at the MAP display and the RMI are identical. However, if the link between the CM and the SDM is down, either due to a fault in the link, or because the SDM itself is not in service, the SDM node state at the MAP display and the RMI may become mismatched. When CM-SDM communications are restored, the SDM node state aligns to the CM view of its state. Manual state changes to the SDM must be performed at the MAP interface, unless the CM-SDM link is down, in which case state changes must be performed at the RMI.

Table 2-10 shows a comparison of the CM view and RMI view of the SDM node states. At the MAP display, the SDM node state can be determined by accessing the MTC APPL SDM level. At the RMI, the SDM node state is visible at the RMI.

Table 2-10
SDM maintenance states – MAP interface vs RMI

SDM node states	Meaning at the MAP interface	Meaning at the RMI
InSv	No alarms are present. The CM is receiving in-service (InSv) status from the SDM.	Messages between the SDM and the CM are being successfully sent and received. All SDM applications and hardware devices are in service with no faults.
ISTb	An APPL SDM minor alarm is present. The CM is receiving in-service trouble (ISTb) status from the SDM.	The SDM node state is ISTb if one or more of the following conditions is present on the SDM: • A hardware component is not InSv. • An operating system software alarm is present. • An application software package is not InSv. • Communication between the CM and the SDM has failed. • Connectivity to a LAN node has failed. • A file system has exceeded its alarm threshold or any volume group is not InSv.

—continued—

Table 2-10
SDM maintenance states – MAP interface vs RMI (continued)

SDM node states	Meaning at the MAP interface	Meaning at the RMI
ManB	An APPL SDM minor alarm is present. The SDM has been manually busied by command from the MAP interface. Messages are successfully being exchanged between the CM and the SDM.	The SDM has either received a ManB command from the CM, or has been manually busied at the RMI while communications to the CM are down. All application and service software processes are stopped.
ManB (NA)	An APPL SDM minor alarm is present. The SDM has been manually busied by command from the MAP interface. The CM cannot communicate with the SDM because the DS512 ports on the MS are unavailable. The actual operating condition and local state of the SDM are unknown to the CM until at least one of the DS512 links is restored.	not applicable
ManB/The SDM is not responding	An APPL SDM minor alarm is present. The SDM has been manually busied by command from the MAP interface. The CM is not receiving messages from the SDM. The actual operating condition and local state of the SDM are unknown to the CM until communications are restored.	not applicable
SysB	An APPL SDM critical alarm is present. The CM is receiving system busy (SysB) status from the SDM, indicating that no applications are running.	The SDM node state at the RMI shows SysB only if all software applications on the SDM have failed.

—continued—

Table 2-10
SDM maintenance states – MAP interface vs RMI (continued)

SDM node states	Meaning at the MAP interface	Meaning at the RMI
SysB (NA)	An APPL SDM critical alarm is present. The CM has designated the SDM node state as system-busy. The CM cannot communicate with the SDM because the DS512 ports on the MS are unavailable. The actual operating condition and local state of the SDM are unknown to the CM until at least one of the DS512 links is restored.	not applicable
SysB/The SDM is not responding	An APPL SDM critical alarm is present. The CM is not receiving messages from the SDM and has designated its state as system-busy. The actual operating condition and local state of the SDM are unknown to the CM until communications are restored. The SDM has been powered down or is rebooting. All software applications on the SDM have failed.	not applicable
OffL	The SDM has been set to offline (OffL) state by command at the MAP interface, or the initial datafill for the SDM has just been completed. Communications to the SDM are disabled.	The SDM is offline, and is not communicating with the CM. The SDM has received the OffL command from the CM, or it has been set to OffL state locally at the RMI while isolated from the CM.
—end—		

Routine maintenance recommendations

Nortel recommends that you perform the following activities as part of the SDM routine maintenance strategy. Some tasks can be performed by maintenance users, while others require root user permissions for accessing the SDM.

Maintenance user tasks

The following activities require maintenance user permissions:

- Check dial-up access to SP0 on the CPU personality module by periodically dialing into the SDM from a remote VT100 terminal and logging in to the RMI. This ensures that the RMI is readily available for maintenance purposes.
- If your system is configured with a local VT100 terminal, connected directly to SP0 by a null modem, log in to the RMI periodically to ensure it is readily available for maintenance activities.
- Clean the SDM tape drive after the first 4 hours of tape movement of a new cartridge, and then after each 25 hours of use, using the appropriate cleaning tape (Hewlett-Packard part number 92283K or equivalent). For more information, see the procedure ”Cleaning the SDM DAT drive” on page 4-55 in the “SDM maintenance procedures” chapter of this document.

Root user tasks

The following activities require root user permissions:

- Backup the SDM software and data as required. Refer to the “SDM system administration overview” chapter on page 3-1 of this document for more information.
- Monitor log files in the /var/adm directory for system or security abnormalities.

SDM system administration overview

ATTENTION

The information in this chapter is intended for SDM system administrators who have root user privileges for accessing the SDM. Nortel recommends that SDM system administrators have specialized AIX training before performing system administration procedures.

ATTENTION

Network File system (NFS) is not supported and should not be used on the SDM. Network Information Service (NIS) is not supported and must not be used on the SDM.

WARNING

SDM product support

SDM product support only includes administrative changes that use either the commands or the SDM maintenance interface described in this document. Other administrative changes that are not described in this document are not supported.

This chapter provides introductory information about administering the SDM. The information contained in this chapter describes system administration requirements, specifies limitations and restrictions, and provides recommendations. Refer to the "SDM system administration procedures" section in this document for detailed procedures.

Commissioning SDM software

Initial installation and commissioning of SDM platform software is performed by Nortel, using a detailed installation method (IM). Software installation includes the base software, and the Log Delivery application,

which are included as part of the platform. Software installation can also include optional software applications.

The SDM platform and optional application software is delivered on a digital audio tape (DAT). The tape is accompanied by release notes that describe the software packaging and tape labeling for the platform and applications software.

Information about commissioning and using optional SDM applications software is available in the Northern Telecom publication (NTP) for each application, or in the release notes documents.

Using the SDM commissioning tool

The commissioning tool cannot be accessed from the MAP display or by remote login to the SDM using the SDMRLOGIN command. The commissioning tool must be accessed from the local console to perform the following tasks:

- install the base software
- install optional application software
- configure connectivity to the CM
- configure connectivity to the operating company LAN
- enable or disable file transfer protocol (FTP) and telnet access to the SDM
- configure base line SDM fault-tolerant hardware devices, including disks, tape drives, Ethernet cards, and DS512 controller modules
- configure maintenance (maint) and root userIDs
- set platform security, which includes
  - — file permissions
  - — passwords
  - — enable the restricted shell for maint users
- set the date, time and time zone of the system
- set the console login prompt
- configure DCE
- set remote nodes to be monitored by the SDM

The commissioning tool displays an “SDM Commissioning Complete!” message after all mandatory sections of the commissioning tool are completed successfully. The optional Distributed Computing Environment (DCE) section could fail commissioning and the message “SDM Commissioning Complete!” would still be displayed. If the DCE has not

been successfully commissioned, the “DCE state” is shown as UnEq in the LAN menu level of the RMI. Ensure that the DCE commissioning has completed successfully after entering the DCE commissioning values.

Defining IP addresses for the SDM to CM LAN

The parameters for the SDM to CM LAN are configured when your system is initially commissioned by Nortel, using a detailed installation method. The IP addresses for the CM, the DS512 interface, and the CM side of the SDM are established as part of initial commissioning and do not normally require subsequent modification. The IP addresses must be consistent with the values datafilled in the DMS data schema tables that control CM to SDM connectivity.

Datafill requirements on the DMS switch

The following DMS data schema tables require datafill, in the order listed, to establish connectivity between the CM and the SDM.

- MSCDINV
- IPNETWRK
- IPHOST
- SDMINV

Table MSCDINV defines cards on the DMS message switch, including those that support communication to the DS512 modules on the SDM. Table MSCDINV datafill defines the characteristics of the DS512 link to the message switch (MS). Two ports on each DS512 personality module are defined to each support a subrate of 128.

Table IPNETWRK defines the IP address of the CM, allowing the SDM to communicate with the CM. The SDM cannot communicate with the CM, if the CM IP address is not defined.

Table IPHOST assigns IP addresses to CM end hosts, and in particular, defines the number of transmission control protocol (TCP) endpoints (0 to 50) in the CM. TCP allows virtual connections between a program running on the SDM, and a program running on the CM. A physical connection is not necessary for communication to occur between two such programs.

Table SDMINV contains configuration information specific to the SDM, including MS port definitions, locations, and IP addresses. Table SDMINV defines the DS512 communication between the SDM and the CM. DS512 communication cannot occur without datafilling table SDMINV.

For detailed information on SDM-related datafill of these tables, refer to the customer data schema NTP for your switching system.

Log Delivery commissioning parameters

Log Delivery operating parameters are controlled by an online SDM commissioning tool (Logroute) that is used at initial installation to set up the application, and thereafter to view or modify the parameter values.

The Log Delivery commissioning tool is used to customize the following:

- global application parameters, including
  - buffer size
  - reconnect timeout value
  - lost logs threshold (the number of lost logs before a system log is generated)
  - ASCII line delimiter and log delimeter characters
  - the number of days to keep log files
- the incoming log stream from the CM, to add or delete individual logs
- per-device list, including
  - device type (UNIX file or TCP/IP link)
  - parameters specific to the device type
  - log output format (standard [STD], switching control centre 2 [SCC2] or internal)
  - logs to be sent to the device

For additional information on commissioning the Log Delivery application, see page 2-82.

Administering the SDM using the remote maintenance interface

The following maintenance tasks can be performed using the SDM remote maintenance interface (RMI):

- change the CM connectivity configuration
- change the LAN connectivity configuration
- add, delete or change LAN nodes monitored by the SDM
- change operating system alarm thresholds
- add logical volumes and change their sizes
- add and delete hardware modules

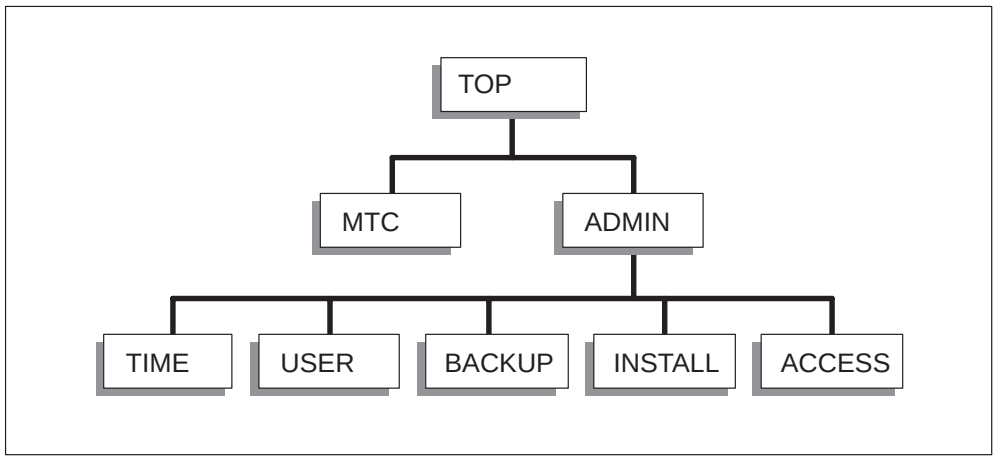
For information about maintenance tasks performed using the RMI, see the “SDM maintenance overview” chapter of this document.

The following administrative tasks can be performed using the administrative level of the SDM remote maintenance interface (RMI):

- change the time zone, time and date
- add and remove users
- password administration
- perform system backup and restore
- enable and disable FTP and telnet access
- install and update software

Figure 3-1 shows the location of the administration level menu items within the RMI. The top menu level is the starting point for all RMI functions. The administration and access menu levels of the RMI are similar to MAP display screens. These screens contain an alarm banner, command list, input and output areas, and a clock. (See the figure 2-8 on page 2-42 in the "SDM maintenance overview" chapter for more information.) The time, user, backup, and install menu options take you to screens that do not resemble the MAP display. These screens display separate entry fields for user input.

Figure 3-1
RMI administration levels



See the “SDM maintenance overview” chapter in this document for an overview of the RMI which includes how to log in to the RMI and a description of the maintenance functionality.

Administration menu level of the RMI

Figure 3-2 shows the administration menu level of the SDM Remote Maintenance Interface menu. Select option 3 from the top level of the RMI to access the administration level. You can also type ADMIN from any level of the RMI to access administration functions.

Figure 3-2
Administration menu level of the RMI

```
                        SDM Remote Maintenance Interface
               SDM      CON     LAN      APPL      SYS      HW            CM : FCC1
                .         .       .         .         .       .            SDM: SDM1

Admin
 0 Quit
 2 Time
 3 User
 4
 5 Backup
 6 Install
 7 Access
 8
 9
10
11
12
13
14
15
16
17 Help
18 Refresh

   root
Time  19:48  >
```

The administration menu level of the RMI has an alarm banner which dynamically updates the overall state of the SDM and the state of its major components. The alarm banner is displayed at the administration and access menu levels of the RMI. For more information on monitoring SDM status and alarms at the RMI, refer to page 2-43 in the “SDM maintenance overview” chapter of this document.

The following set of navigation and interface commands is available at the administration level of the RMI:

- Quit exits the administration level of the RMI. Type QUIT or select option 0 to use this command.

- Time changes the time zone, time and date on the SDM. Type TIME or select option 2 to access this menu.
- User adds and removes users, and administers users and passwords. Type USER or select option 3 to access the User menu.
- Backup accesses the system backup and restore menus. Type BACKUP or select option 5 to access the Backup and Restore Main Menu.
- Install upgrades or installs SDM software. Type INSTALL or select option 6 to install or upgrade software.
- Access changes FTP and telnet settings. Type ACCESS or select option 7 to enable or disable FTP access and telnet access settings.
- Help provides information about the administration menu options. Help messages are also displayed when incorrect information is entered. To use the Help command, type HELP or selecting option 17 to get information about the administration menu options.
- The Refresh command refreshes the screen. Type REFRESH or select option 18 to use this command.

Time and date administration

Time and date administration allows the time zone, date and time of day on the SDM to be changed. Changes between daylight saving and standard time are automatically accommodated on the SDM without a need for manual time and date adjustment. Refer to the procedure ”Setting the time zone, date and time” on page 6-18 for more information.

User and class administration

Two user classes are provisioned on the SDM: administrative users and maintenance users. The administrative class consists of the root user. The maintenance class consists of the maintenance user by default, but additional maintenance class users can be added. The capabilities available to each class are listed in table 3-1.

Table 3-1
User class profiles

Class	Responsibilities	Capabilities
Administration	SDM system administration	user and group administration • adding and removing users • assigning and restricting user access • password administration system image backup and restore unrestricted shell access local console access from LAN setting the time zone, and the date and time all maintenance capabilities
Maintenance	SDM maintenance	maintenance commands (for example, busy, return to service, and offline) monitoring system performance restricted shell access changing system alarm thresholds password update application-specific configuration tools

Password administration

The root user can change any password on the system at any time. Maintenance class users can only change their own passwords. The following conditions apply to user passwords:

- The maximum duration for passwords is four weeks for root users and nine weeks for maintenance class users.
- Warnings are issued 7 days before the password expires, and are repeated at each login until the password is changed.
- A user cannot reuse a passwords for 26 weeks after their assignment.
- If a maintenance class user's password expires, the user has up to 2 weeks after the expiry date to change the password. During this period, the user is forced to enter a new password before they can log in. If it is not changed by the end of this 2-week period, the user must reset it before logging in again.
- The minimum length of passwords is six characters. The password must contain a minimum of one alphabetic character, and a minimum of one numeric or special character. (Although more than eight characters can be entered, only the first eight characters of a password are considered.)

Note: Although passwords beginning with a number are valid, they cannot currently be accepted following the SDMRLogin command.

Idle logins

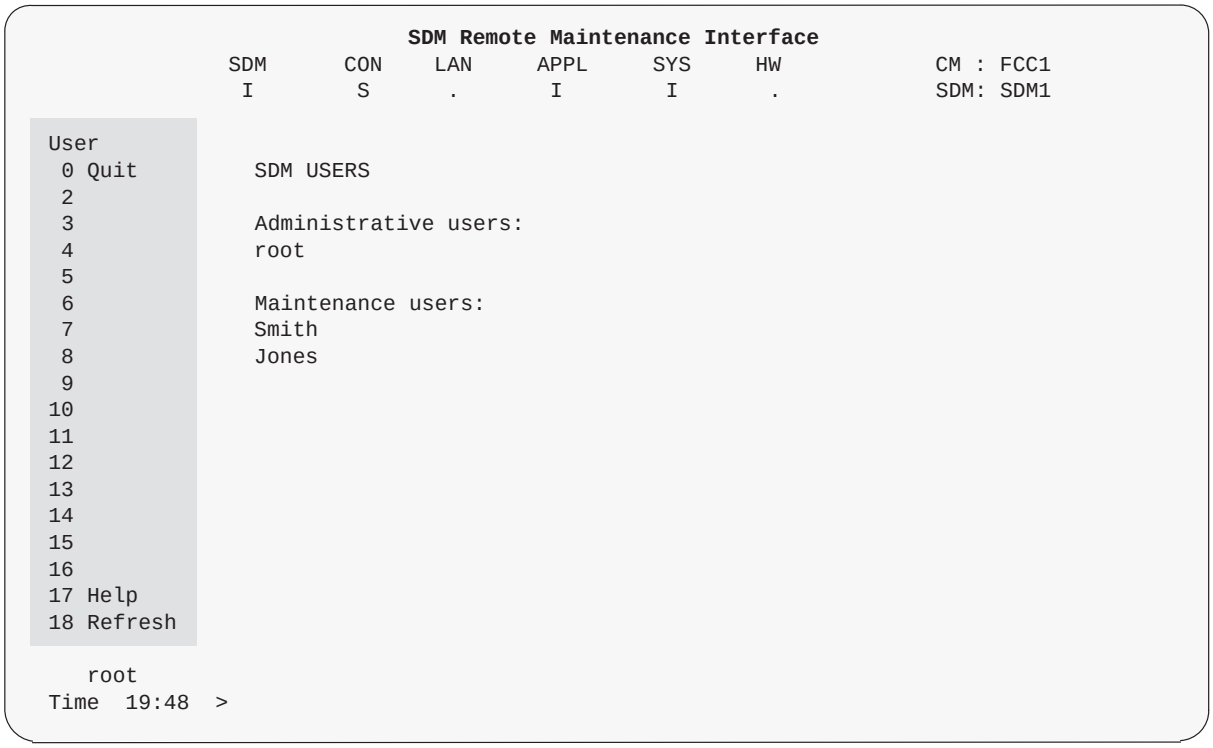
All users are logged out automatically after 10 min of inactivity.

User menu of the RMI

The user option at the RMI is the starting point for administering user passwords, and adding and removing maintenance class users. Figure 3-3 shows the User menu. The user administration tasks that can be done from the User menu include adding a user, removing a user, and changing a password. This screen shows all users on the system.

To access the User menu, select option 3 from the administration menu level of the RMI or type USER from any RMI menu level.

Figure 3-3
User menu



Adding users to the maintenance class

Refer to the procedure ”SDM users class – Adding or removing a maintenance user” on page 6-10 in the “SDM system administration procedures” chapter of this document for more information on how to add new users. Only the root user may execute this procedure.

Changing a user’s password

You must know the user’s old password or be the root user to change a user’s password. See ”Password administration” on page 3-9 for restrictions on defining and changing user passwords. User passwords are changed directly at the User menu.

Refer to the procedure ”Changing user passwords” on page 6-3 in the “SDM maintenance procedures” chapter of this document for more information on how to change passwords.

Removing users from the maintenance class

Removing a maintenance class user is done directly from the User menu.

Refer to the procedure ”SDM users class – Adding or removing a maintenance user” on page 6-10 in the “SDM system administration procedures” chapter of this document for more information on how to remove users. Only the root user may execute this procedure.

Software and data backups

There are two types of backups on the SDM: a system image backup and incremental backups (including automated incremental backups). The following sections describe these types of backups. SDM software and data backups must be performed by the root user. Software backups are stored on 4-mm digital data storage (DDS) tapes with lengths of either 90 m or 120 m.

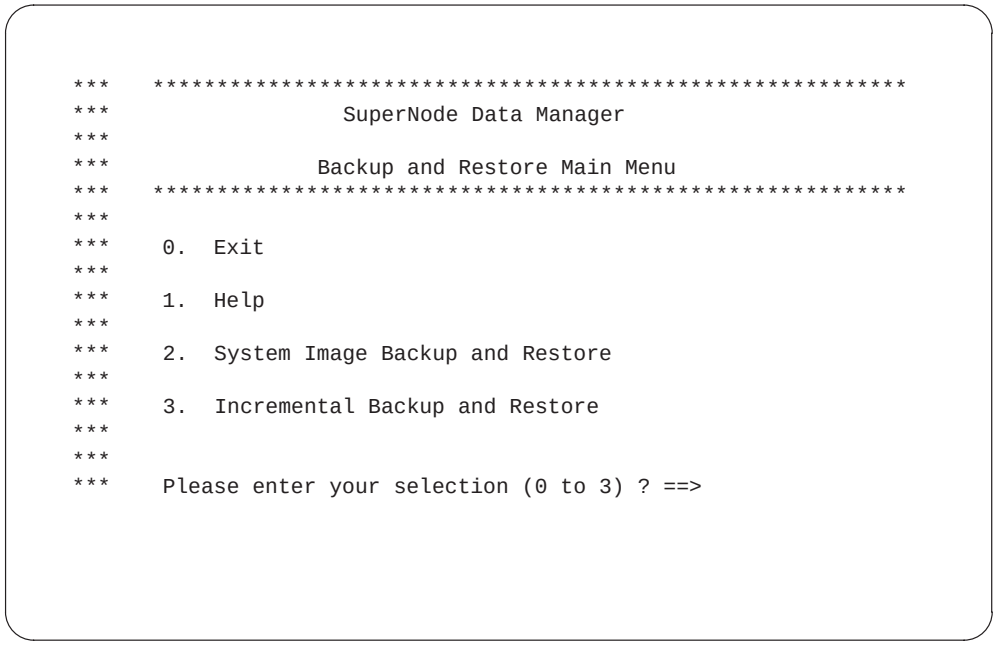
Backups are performed using the SDM backup and restore online utility, which the root user can access in two ways:

- by logging in to the local or remote VT100 console and typing “sdmbkup”
- by typing “sdmmtc” after logging in to the SDM to access the RMI. Select option 3 at the Top level of the RMI, or type ADMIN at any level to go to the administration menu level of the RMI, then select option 5 or type BACKUP.

All volume groups must be fully mirrored before an incremental backup can be performed. Nortel also recommends that tape drive DAT0 is used to perform software and data backups if your system includes the SuperNode Billing Application (SBA).

Figure 3-4 shows the Backup and Restore Main Menu. This is the starting point for performing backup and restore functions.

Figure 3-4
Backup and Restore Main Menu



For detailed instructions on performing software backups, refer to the following procedures in the “SDM system administration procedures” chapter of this document:

- ”Creating SDM backup tapes – system image backup (S–tape)” on page 6-26
- ”Creating SDM backup tapes – Manual incremental backup (I-tape)” on page 6-39
- ”Creating SDM backup tapes – Automated incremental backups” on page 6-50

System image backup

The system image backup is used to back up all files in the root volume group to a tape called an S-tape. The system image backup includes the following:

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

Figure 3-5 shows the System Image Backup and Restore Menu. This menu is used to perform a system image backup, restore files, and list the contents of the system image tape (S-tape).

To access this menu, select option 2, System Image Backup and Restore, from the Backup and Restore Main Menu.

Figure 3-5
System Image Backup and Restore Menu

```
***    ********************************************************
***                  SuperNode Data Manager
***
***           System Image Backup and Restore Menu
***    ********************************************************
***
***     0.  Return to the Previous Menu
***
***     1.  Help
***
***     2.  Create a System Image on Tape (S-tape)
***
***     3.  List Contents of the System Image Tape (S-tape)
***
***     4.  Restore Files from the System Image Tape (S-tape)
***
***
***     Please enter your selection (0 to 4) ? ==>
```

When to perform a system image backup

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

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

Incremental backups

Incremental backups are used to back up files that have been updated or created since the last system image backup was performed. They record all file changes since the last system image backup, so when an incremental backup is performed, the results of any previous incremental backup will no longer be needed. Incremental backups are stored on an incremental backup tape (I-tape). Nortel recommends that you perform regularly scheduled incremental backups to minimize the risk of lost data.

Figure 3-6 shows the Incremental Backup and Restore Menu. This menu is used to perform incremental backups, restore files, create, view or clear an automated incremental backup schedule, and list the contents of the incremental backup tape (I-tape).

To access this menu, select option 3, Incremental Backup and Restore, from the Backup and Restore Main Menu.

Figure 3-6
Incremental Backup and Restore Menu

```
***   ************************************************************
***                  SuperNode Data Manager
***
***            Incremental Backup and Restore Menu
***   ************************************************************
***
***    0.  Return to the Previous Menu
***    1.  Help
***    2.  Automated Incremental Backup Menu
***    3.  Create an Incremental Backup Tape Now (I-tape)
***    4.  List Contents of an Incremental Backup Tape (I–tape)
***    5.  Restore All Files from an I-tape
***    6.  Restore Selective Files from an I-tape
***
***
***    Please enter your selection (0 to 6) ? ==>
```

When to perform incremental backups

An incremental backup can be performed while the system is in service. However, if any files are open when the incremental backup begins, the last closed (saved) versions of these files are backed up. To minimize inconsistency between current and backed up versions of files, perform incremental backups during a low-usage period.

Incremental backups can be performed manually or automatically. The scheduling of incremental backups is at the discretion of the SDM system administrator.

Using the automated incremental backup utility

The root user can enter a scheduled time for automated incremental backups in the Set Date and Time for SDM Incremental Backup menu. Incremental backups can be scheduled to occur daily, weekly, monthly or on a specific date. All SDM software files that have been changed or created since the

most recent system image tape (S-tape) was created are backed up automatically according to the backup schedule that is created.

Files that are open when the automated incremental backup begins will not be backed up. Instead, the most recent saved version of the file is backed up. This may result in inconsistency between the current and backed up versions of files. Automated backups should, therefore, be scheduled during low usage periods to minimize this inconsistency.

Figure 3-7 shows the Automated Incremental Backup Menu, the starting point for creating, viewing or clearing an incremental backup schedule. This menu is used to perform the following tasks:

- create an automated incremental backup schedule
- view the automated incremental backup schedule
- clear the automated incremental backup schedule

To access this menu, select option 2, Automated Incremental Backup Menu, from the Incremental Backup and Restore Menu.

Figure 3-7
Automated Incremental Backup Menu

```
***    ************************************************************
***                    SuperNode Data Manager
***
***              Automated Incremental Backup Menu
***    ************************************************************
***
***     0.  Return to the Previous Menu
***     1.  Help
***     2.  Create Automated Incremental Backup Schedule
***     3.  View Automated Incremental Backup Schedule
***     4.  Clear Automated Incremental Backup Schedule
***
***
***     Please enter your selection (0 to 4) ? ==>
```

Note: Clearing the automated incremental backup schedule erases the stored scheduled data. If you wish to use the same schedule at a later date, make note of the schedule data for future reference before clearing.

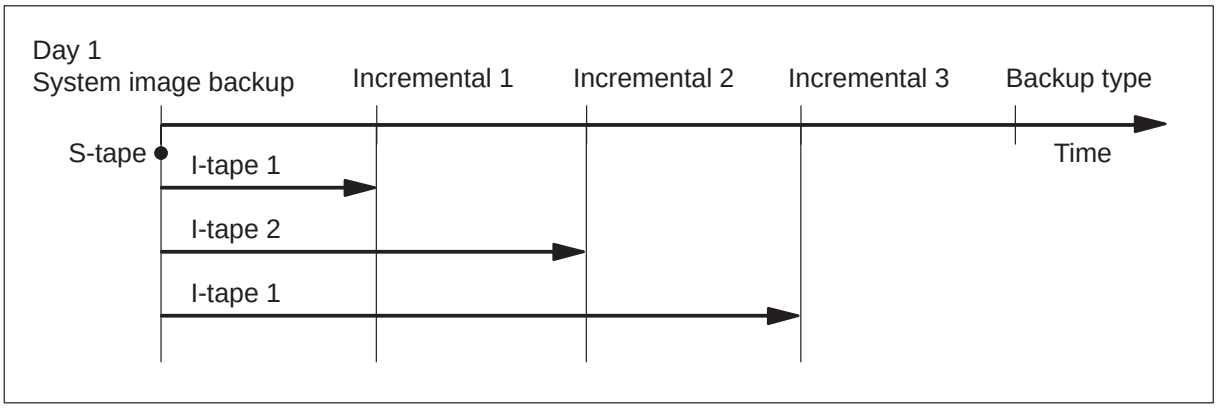
Replacing incremental backup tapes

Replace the tapes that are used for incremental backup after six months to ensure integrity of the data. Nortel recommends using two tapes for incremental backups (I-tapes) and alternating them on a weekly basis. This ensures that a second incremental backup tape is available in the event that the most recent incremental backup fails, or the most recent I-tape is misplaced, damaged, corrupted, or unavailable for any reason.

Software backups are stored on 4-mm DDS tapes, in either 90 m or 120 m lengths. Nortel also recommends periodic cleaning of the tape drive. Refer to the procedure ”Cleaning the SDM DAT drive” on page 4-55 in the “SDM maintenance procedures” chapter of this document for more information.

Figure 3-8 illustrates the use of one S-tape and two I-tapes for SDM backups. The system image backup is performed when the system was installed, and is not repeated until new software is installed, or until there are configuration changes to the disk or the logical volumes. Two I-tapes are rotated on a weekly basis to perform manual incremental backups or automated incremental backups.

Figure 3-8
Using one S-tape and two I-tapes for incremental backups



Restoring SDM software and data

This section provides an overview of SDM software restore capabilities and methods. For detailed instructions on restoring SDM software, refer to the following procedures in the "SDM system administration procedures" chapter in this document:

- "Restoring the SDM – Full restore from S-tape and I-tape" on page 6-61
- "Restoring the SDM – Partial restore from the system image tape (S-tape)" on page 6-75
- "Restoring the SDM – Partial restore from an incremental backup tape (I-tape)" on page 6-84

SDM restore operations must be performed by the root user. The root user must be a trained UNIX system administrator who is capable of correctly identifying files or directories to be restored, and who fully understands the impact of restoring or overwriting software files.

The SDM is restored by using backup tapes. See "Software and data backups" on page 3-11 for information on performing software backups.

Software restores are performed by using the SDM backup and restore online utility, which the root user can access in two ways:

- by logging in to the local or remote VT100 console and typing "sdmbkup"
- by typing "sdmmtc" after logging in to the SDM to access the RMI. Select option 3 or type ADMIN to go to the administration menu level of the RMI, then select option 5 or type BACKUP.

Note: The full restore must be done at the local VT100 terminal, connected to the SDM.

Performing a full SDM restore

A full SDM restore is required if SDM software becomes corrupted, or the disk drive unit is replaced. A full restore consists of loading the full contents of the system image tape (S-tape), followed by loading the full contents of the most recent incremental backup tape (I-tape), if any such tape has been made since the last system image backup.

Full SDM restores require rebooting the SDM. The SDM reboots automatically after the S-tape is restored. Reboot the SDM, if required, after the I-tape is restored.

ATTENTION

After a full SDM restore is performed you must verify the state of DCE and any DCE-based application servers. It may be necessary to perform additional DCE procedures. See the section ”DCE application servers after an SDM restore” on page 3-30 for more information. Also, refer to the procedure ”Restoring the SDM – Full restore from S-tape and I-tape” on page 6-61 for detailed instructions of the steps required.

Performing partial software and data restores

The root user can restore individual files or directories from the system image tape or from an incremental backup tape. Use of these procedures is at the discretion of the root user. Only a trained AIX system administrator who is familiar with the files and knows exactly which files to restore should perform a partial restore procedure. SDM software could inadvertently be corrupted if the wrong files are restored.

Listing the contents of a backup tape

The root user can list the contents of a backup tape by inserting it into the tape drive and accessing the SDM Backup and Restore Main Menu.

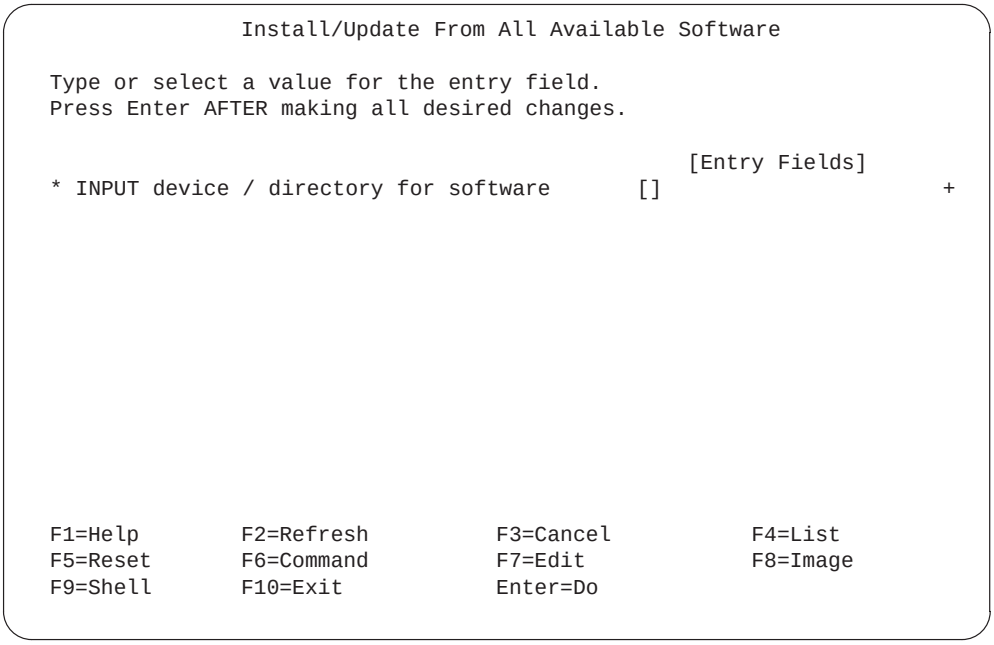
To view the contents of the S-tape, select “System Image Backup and Restore”, then select “List Contents of the System Image Tape (S-tape)”.

To view the contents of an I-tape, select “Incremental Backup and Restore”, then select “List Contents of an Incremental Backup Tape (I-tape)”.

Installing and updating software

To install or update software on the SDM select option 6 or type INSTALL at the administration menu level of the RMI. Use this menu to install or update SDM base or application software packages, as instructed by the release notes or NTPs that accompany the software product. Figure 3-9 shows the software installation and update menu and display.

Figure 3-9
Install menu



Enabling and disabling FTP and telnet access

To view or modify FTP and telnet access to the SDM, select option 7 or type ACCESS at the administration menu level of the RMI or type ACCESS at any level. Figure 3-10 shows the Access menu level of the RMI. In the example shown, telnet access is enabled, file transfer protocol (FTP) access is disabled and Secure File Transfer (SFT) is in Distributed Computing Environment (DCE) mode.

Note: SFT Access is only displayed on the Access menu if the SFT package is installed. If SFT is not installed, only Telnet and FTP access are displayed.

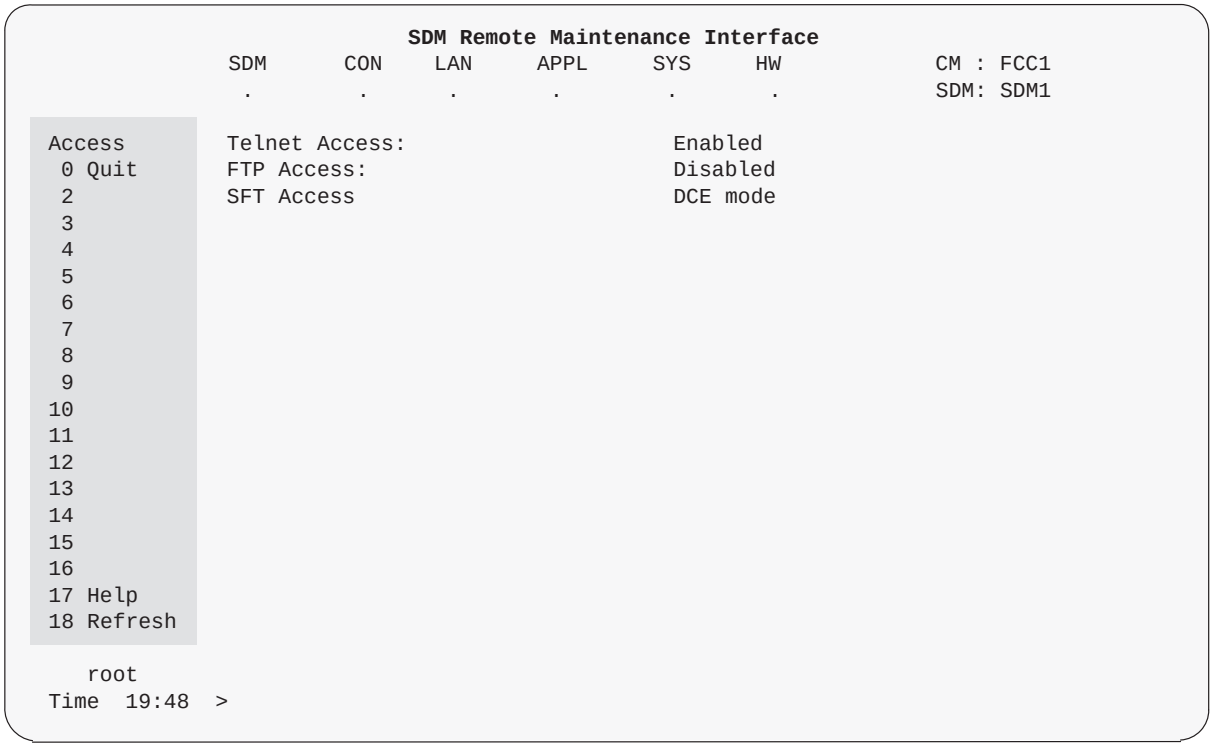
When SFT is in DCE mode:

- the security encryption is enabled

When SFT is in FTP (non-DCE) mode:

- DCE security is disabled for SFT
- the standard FTP server is disabled
- SFT client cannot connect in this mode, users must use a standard FTP client

Figure 3-10
Enabling and disabling FTP and Telnet



Commands at the access menu level

Change is a hidden command used to modify FTP and telnet access to the SDM. The parameters are SFT, TELNET, or FTP. Use the change command as follows:

Note: The parameter SFT only applies if the SFT package is installed. If the SFT package is not installed, the parameters are FTP and TELNET.

- Type CHANGE to change SFT and TELNET access.
- Type CHANGE SFT to change only SFT status (DCE or FTP (non-DCE)).
- Type CHANGE FTP to change only FTP access (enabled or disabled).

- Type CHANGE TELNET to change only telnet access (enabled or disabled).

If no parameters are supplied after the change command, the user is prompted to change both the Telnet and SFT status. The default status of FTP is Disabled. To change the FTP status to enabled, type change FTP after changing SFT to DCE mode.

After you enter the change command, you are prompted to confirm your request.

Hardware upgrades

The CPU controller modules can be upgraded, and are available in the two versions:

- NTRX50FL – 256 MByte DRAM
- NTRX50FM – 512 MByte DRAM

The CPU controller modules can be upgraded from:

- NTRX50FK (128 MByte DRAM) to NTRX50FL (256 MByte DRAM)
- NTRX50FK (128 MByte DRAM) to NTRX50FM (512 MByte DRAM)
- NTRX50FL (256 MByte DRAM) to NTRX50FM (512 MByte DRAM)

For detailed instructions on performing these upgrades, refer to the “SDM hardware upgrade procedures” chapter of this document.

In addition to the required I/O controller module (NTRX50FQ), you may wish to add the following I/O controller module to increase disk capacity:

- NTRX50FU - 2-Gbyte disk drives and Ethernet

ATTENTION

Adding an I/O controller module (NTRX50FU) does not provide functionality in this product release. Functionality is provided in the next product release. Modules can be added now, if desired, to prepare for the new functionality.

For detailed instructions on adding an I/O controller module, refer to the procedure ”Adding I/O controller modules” on page 4-160 in the “SDM maintenance procedures” chapter of this document.

DCE overview

Distributed Computing Environment (DCE) allows graphical user interface (GUI) applications running on remote workstations to communicate securely with the SDM. These GUI application control operations run on the SDM and the DMS switch. They run as clients of application servers running on the SDM, and communicate securely with the SDM by remote procedure calls (RPCs) supported by DCE.

ATTENTION

The DCE overview section is written for experienced DCE system administrators who are knowledgeable about DCE and its required administration procedures.

DCE cell configuration and maintenance

For an SDM to communicate securely with its remote workstations by DCE, the SDM and the workstations must be configured in the same DCE cell. A DCE cell consists of all systems having a common DCE realm. In the SDM context, a DCE cell must contain the following:

- one or more SDMs
- all workstations running GUI applications that will communicate with those SDMs
- DCE servers that provide DCE services to those SDMs and workstations:
  - — security servers that store security information and authenticate users of the GUI applications
  - — cell directory servers (CDSs) that store naming information from the application servers on the SDM and allow GUI application clients to locate the application servers
  - — distributed time servers (DTSs) that allow all machines in the DCE cell to maintain synchronized clocks

Typically there can be more than one replica of each type of server. For security servers and CDS servers, one replica is the primary (or master) replica and all others are slave replicas. For DTS servers, one particular replica is the time provider.

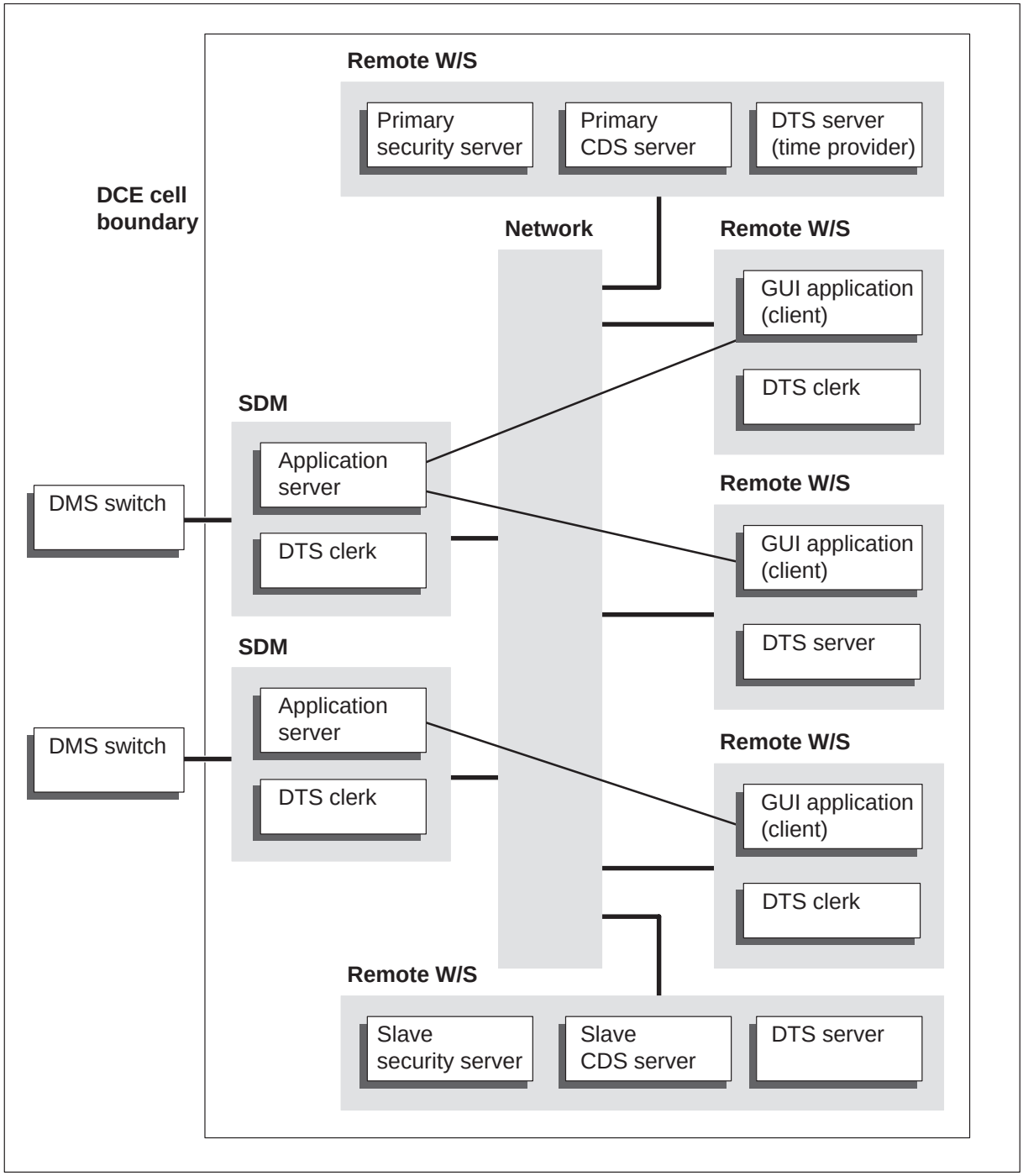
The following workstations may be used to run GUI applications:

- HP 700/800 workstations with HP-UX 9.05 or later
- Sun SPARC workstations with Solaris 2.4 or later

The DCE servers can, in principle, be located on any workstation in the DCE cell. In practice, however, Nortel strongly recommends that all security servers and, if possible, all CDS servers, be located on dedicated and physically-secured workstations that are separate from all GUI-application workstations that use their services. (Other configurations risk compromising the security arrangements offered by DCE.) The primary security and CDS servers and the DTS time provider, can all be on the same workstations, or one/all may be on separate workstations. If a slave security server is present, it must be on a separate workstation.

Each of the SDMs and GUI-application workstations that use the services of the DCE servers must run a DTS clerk that interacts with the DTS servers. If a DTS server is located on a GUI-application workstation, it provides the DTS clerk the functionality required by that workstation. Figure 3-11 shows a typical configuration of a DCE cell.

Figure 3-11
DCE cell configuration



Setting up a DCE installation

The following steps are required before secure network communication between GUI-application workstations and SDMs can be established using DCE:

- DCE software must be installed and configured on all the systems that will be part of the cell, as outlined in the DCE software vendor's installation notes.
- The DCE cell must be configured, including its DCE servers and remote (GUI application) workstations.
- DCE accounts must be created to accommodate the users of the GUI applications.
- Each SDM must be added to the DCE cell.
- Application-server software for each GUI application must be installed on each of the appropriate SDMs within the DCE cell, and registered with the DCE security and CDS servers.
- Each GUI application must be installed on each of the appropriate workstations within the DCE cell.

DCE accounts must also be modified to reflect changes in the user community of the GUI applications.

The following items are covered in the next three sections:

- recommendations on creating the DCE cell
- adding an SDM to the DCE cell
- registering application servers and creating DCE accounts on the DCE security server

Creating the DCE cell and adding nodes to a cell

The DCE cell must be created using a machine on which one or more of the DCE servers will reside. Each vendor of DCE software provides a program that carries out cell creation, and is used to add machines to a DCE cell. The following is a partial list:

MACHINE	DCE CELL-CREATION PROGRAM NAME
HP9000	dce_config
IBM RS-6000	mkdce
Motorola PowerStack	mkdce
Sun SPARC	dcesetup

These programs are invoked from the machine's UNIX prompt. For more information on creating DCE cells and configuring DCE and client servers, refer to "OSF DCE Administration Guide – Core Components" or your DCE vendor's installation/configuration information.

Adding an SDM to the DCE cell

Add an SDM into a DCE cell by invoking the SDM commissioning tool from the local console of that SDM. (No other machines in the DCE cell can be used to perform this task.)

The SDM can be added to the cell using two different methods:

- full configuration, when you know both the root password of the SDM, and a DCE administrative account password
- local configuration, when you know only the root password of the SDM

To use full configuration, you must also know the following:

- the name of the DCE cell
- the IP address of each machine hosting the primary DCE security server
- the IP address of the CDS server
- the name of the SDM LAN profile
- the password of the DCE cell administrator

To use local configuration, a user with a DCE administrative account password must have already executed an enabling administrative procedure from another AIX-based machine within the DCE cell. You must then know the following:

- the name of the DCE cell
- the IP address of each machine hosting the primary DCE security and DTS servers

For more information, see the procedures "Distributed Computing Environment – Configuring an SDM in a DCE cell" and in the "SDM system administration procedures" chapter of this document.

Registering application servers and creating user accounts

All application servers on SDMs within the DCE cell, and GUI applications users that communicate with an application server using DCE, must have properly configured accounts registered in the DCE security database associated with the DCE security server. A DCE administrative account password is required to perform all registration activities.

Registration can be done from any machine in the DCE cell. Commands to perform registration activity are available from the UNIX prompts on the

DCE cell machines. For security reasons, however, Nortel does not recommend that telnet and Enhanced Terminal Access (ETA) be used when establishing a registration session.

Note: ETA is an optional SDM application that provides secure remote access to the SDM across the operating company TCP/IP wide area network (WAN). For more information on the ETA application, refer to the NTP, *SuperNode Data Manager Enhanced Terminal Access User Guide*.

As part of the SDM application-server software installation, a key table (keytab) file is created to store the application server DCE password (for presentation whenever DCE communication with the application server is required). To preserve security, each application keytab file provides read-only file permissions to the application server, and must deny access to all other UNIX users.

Note: It is very important that these permissions are not changed, as DCE security will be compromised.

When an application server on a particular SDM is registered to the DCE application server, an entry is created in a CDS directory called

- /.:/subsys/NT/SDM/*clli*

where

clli is the CLLI of the DMS switch to which the SDM is connected.

The CDS directory is created automatically when the first application-server registration to the DCE security database from that SDM takes place.

For more information on registrations to the DCE security database, refer to *OSF DCE Administration Guide – Core Components* or your DCE vendor's installation/configuration information.

DCE commands and status

Various DCE commands are available on any machine that has been included in a DCE cell. To access these commands, type "dcecp" at the UNIX prompt.

Each SDM that has been included in a DCE cell is equipped with a DCE monitoring tool called dcemonitor, that determines status and checks for error conditions. Most DCE troubleshooting activities for an SDM must be carried out from the SDM itself.

Access to DCE-based applications across a firewall

Special measures must be taken for DCE-based applications to work when the SDM is separated from

- the DCE cell's security and CDS servers, by a firewall (or some other filtering device
- a workstation that runs an SDM client program

The SDM restricts the TCP and universal datagram protocol (UDP) ports that it uses for accepting DCE RPCs. These RPCs communicate between application client programs, or DCE management utilities, and DCE-based programs running on the SDM.

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

Adding and removing port restrictions

DCE port ranges can be restricted to a range that is predefined by SDM software or to a specified range determined by a system administrator. When port restrictions are removed, the SDM returns to the default values for the DCE ports. This allows the DCE ports to be randomly assigned.

For detailed instructions on adding and removing port restrictions, refer to the following procedures in the "SDM system administration procedures" chapter in this document:

- "Restricting ports to an SDM defined range" on page 6-140
- "Restricting ports to a specific range" on page 6-145
- "Removing port restrictions" on page 6-150

Executing SDM-specific DCE commands on other machines

Many DCE commands described in this document, that pertain to a specific SDM, can be executed on any machine configured as a DCE node in the DCE cell of which that SDM is a member. The exceptions are described in table 3-2. An administrator DCE login is usually required. For security reasons, Nortel recommends that, whenever possible, you do not execute DCE commands from a remote terminal that uses Enhanced Terminal Access (ETA) or telnet to connect to the SDM. The DCE login is risky in such cases because the administrator's userID and password are passed unprotected over the network.

Interactions between the dcecp program and the DCE security server are protected by encryption and cannot be compromised. It is not necessary, and not advised, to run the commands on the same machine as the security server.

Table 3-2
DCE commands – SDM vs remote node

Procedures that must be executed from the SDM	Procedures that can be executed on any node that is part of the DCE cell
configuring an SDM in a DCE cell using full configuration configuring an SDM in a DCE cell using local configuration adding an SDM application server (as described in the SDM application NTPs) removing an SDM application server enabling, disabling or viewing dcemonitor data most DCE troubleshooting problems	configuring an SDM in a DCE cell (administrative portion only). The administrative portion consists of: • logging in as any user that can execute UNIX commands to a machine other than the SDM being configured • invoking the “mkdce -o admin” command adding an SDM user creating or modifying SDM application network data (for example, assigning the ETA CM and SDM userIDs to a user)

Invoking DCE-based applications

Users of DCE-based GUI applications at remote workstations must provide a userID and password to DCE. This is done in one of three ways, depending on how the remote workstation has been configured:

- If the workstation has been configured to use integrated DCE login, the userID and password are provided to DCE automatically each day, whenever UNIX usage or UNIX login first occurs.
- If the workstation has not been configured to use integrated DCE login, but a dce_login command is contained in the user’s profile, a dce_login prompt will be issued when the user logs in to the workstation. All DCE-usage credentials are valid for several hours, and another dce_login prompt is issued shortly before their expiry.
- If the workstation has not been configured to use integrated DCE login, and the user’s profile does not contain a dce_login command, the user must log in each time a DCE-based application is invoked. (A DCE login dialog is issued whenever a user tries to invoke such an application without invoking the dce_login command.) The DCE-usage credentials must be renewed every few hours; a renewal dialog is issued prior to their expiry, although renewal can occur after expiry without adverse impacts.

DCE application servers after an SDM restore

As with a human user, the DCE-based application servers running on the SDM must log in to DCE to obtain credentials necessary to decrypt the authentication data coming from GUI clients, and to register in the DCE cell directory service. Application servers log in to DCE by getting keys, the equivalent of passwords, from keytab files stored in the non-volatile storage area of the SDM. Application servers may also need to change their keys to reinforce security.

The time period after which an application server needs to change its key is the shorter value of the pwdlife attribute of the server's account in the DCE security registry, and the value of the pwdlife attribute for the organization to which the server belongs. (By default, the SDM servers belong to the sdm-servers organization.) The default values of both pwdlife attributes are "forever", which (if retained) means that the key never gets changed. However, if the value for either attribute is changed by the DCE administrator, the SDM servers will automatically modify their keys in the keytab files before they expire.

If an SDM application server automatically modifies its key between the time the SDM disk was backed up and the time the SDM was restored from tape, restoring the SDM from tape will cause the application server to revert back to an obsolete key. If this occurs, the DCE-based application state is displayed as failed (Fail) at the application menu level of the RMI. The same situation occurs if the restore occurs from a tape other than the most recent one, and the key has been modified at any time since that tape's creation. To restore a server that has failed for this reason, it is necessary to re-execute the command to create the application server's account in DCE, as documented in the NTP for the application.

The SDM DCE software which is responsible for the core DCE servers, also uses a keytab file. If this software gets an obsolete key after a system restore, DCE will fail on the SDM. The state of DCE is then displayed as SysB at the LAN menu level of the RMI.

To recover from this situation, the SDM must be removed and reconfigured in the DCE cell, as documented in the following procedures in the "SDM system administration procedures" chapter in this document:

- "Distributed Computing Environment – Removing an SDM from a DCE cell"
- "Distributed Computing Environment – Configuring an SDM in a DCE cell"

DCE problems requiring manual intervention

ATTENTION

This section contains technical material addressed to experienced DCE system administrators only. Other users who suspect DCE problems must contact an experienced DCE administrator, or their next level of support.

The SDM detects common DCE failure conditions, reports them to the SDM node control facility, and automatically takes the appropriate recovery action to clear the problem. Dcemonitor dumps its current status, problems found, and the recovery action in a file that is regularly rewritten. The status of DCE, reported by dcemonitor, is displayed under the connectivity level of the remote maintenance interface (RMI). To view the status file, refer to the "SDM system administration procedures" chapter in this document.

Table 3-3 lists examples of problem text that is displayed under the LAN menu level of the RMI, and describes the triggers and solutions for each problem. Table 3-3 is not representative of all DCE failure conditions, as it is impossible to predict all failures that may occur.

Table 3-3
DCE problem text at RMI Con menu level

Problem text	Trigger	Action
`/etc/rc.dce file cannot be read`	DCE software is not installed or was removed from the SDM.	Type "lslpp -L grep dce" to verify fileset installation. (There are about 20 filesets).
	The /etc/rc.dce file was accidentally removed.	Reinstall the SDM operating system software.
`DCE has not been commissioned - daemon not enabled`	DCE is not commissioned on the SDM.	Configure DCE on the SDM. Refer to the procedure, "Distributed Computing Environment – Configuring an SDM in a DCE cell" on page 6-97 in the "SDM system administration procedures" chapter of this document.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
daemon `is not running` or *daemon error message from rc.dce* ***Note:*** *daemon* can be: • dced • sec-client service • cdsadv • dtsd	The specified daemon is not running. It may be crashing after /etc/rc.dce has started it.	Execute the daemon manually as the root user from a UNIX shell. Check the DCE command reference manual for the debug syntax options for more error information. Depending on the daemon that is reported as failing, check for log files under: • /opt/dcelocal/var/dced • /opt/dcelocal/var/adm/directory/cds • /opt/dcelocal/var/security • /opt/dcelocal/var/time/adm/dtsd • /opt/dcelocal/var/adm/time • /opt/dcelocal/var/svc/error.log • /opt/dcelocal/var/svc/fatal.log
	The cell security service or the CDS are malfunctioning.	Ensure that the cell security service and the CDS server are both functioning properly.
	The time on the SDM and the security server in the DCE cell are not within 5 min of each other.	Use the UNIX date command to check SDM time. Ensure that the SDM time is within 5 minutes of the cell security server time. SDMs and security servers can be on different time zones if their times are within 5 minutes of each other when they are converted to universal time clock (UTC).

`cannot find telcolan entry in /etc/hosts file`
or
`cannot extract sdm IP addr and hostname from /etc/hosts`
	The /etc/hosts file is damaged, and dcemonitor cannot compute the operating company LAN IP address of the SDM.	Check that the /etc/hosts file contains a line formatted as: xxx.xx.xx.xx *hostname* telcolan. Fix the /etc/hosts file by setting the SDM IP address using the RMI.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`cannot get the host_name from the config hostdata database`	Dcemonitor cannot read the DCE hostname from the hostdata configuration information.	From dcecp, type “hostdata catalog”. One of the listed entries ends with host_name. Then type “hostdata show host_name”. Ensure the hostdata output contains a line formatted as hostdata/data hosts/*hostname*. The hostname is the same as the UNIX hostname. If you cannot display hostdata information, remove and reconfigure DCE on the SDM. Refer to the procedures, ”Distributed Computing Environment – Removing an SDM from a DCE cell” on page 6-110 and ”Distributed Computing Environment – Configuring an SDM in a DCE cell” on page 6-97 in the “SDM system administration procedures” chapter of this document.
	CDS is malfunctioning.	Ensure that CDS server is functioning properly.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`cannot list /.:/hosts/`*`hostname`*	CDS is malfunctioning.	Ensure that the CDS server is functioning properly.
	The machine “self” principal does not have all its permissions set.	Check that the ACL on this directory. The machine “self” principal must have all permissions set. Check that CDS contains a /.:/hosts/*hostname* directory. Reconfigure DCE on the SDM. Refer to the procedure, ”Distributed Computing Environment – Configuring an SDM in a DCE cell” on page 6-97 in the “SDM system administration procedures” chapter of this document.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`cannot unexport bad IP address from /.:/hosts/`*`hostname/server entry`* or `/.:hosts/`*`hostname/server entry`* `contains a bad IP address, and a good binding cannot be computed` or `cannot re-export I/F`*`interface UUID`* `to /.:/hosts/`*`hostname/server entry`*	The SDM has IP addresses for the operating company LAN, and the switch. DCE daemons export these addresses in bindings stored in CDS. Because the switch-side IP address cannot be reached from any client from the operating company LAN, dcemonitor looks for these bindings, and removes or replaces them with equivalent bindings containing the operating company IP address only. This error message indicates that this substitution cannot be done.	Check the bindings for the faulty / .:/hosts/*hostname*/*server entry* to make sure it does not contain the IP address of the SDM as seen from the CM side.
	CDS is malfunctioning. The machine “self” principal does not have all its permissions set.	Ensure that the CDS server is functioning properly. Check the ACL on the CDS server entry. The machine “self” principal must have all permissions set. Reconfigure DCE on the SDM. Refer to the procedure, ”Distributed Computing Environment – Configuring an SDM in a DCE cell” on page 6-97 in the “SDM system administration procedures” chapter of this document.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
The DCE hostname ($dce_hostname) doesn't match the SDM unix hostname: (*hostname*). DCE re-configuration is required.	The SDM UNIX hostname (defined in the /etc/hosts file) does not match the DCE hostname of the SDM that was defined when DCE was commissioned. The /etc/hosts file is formatted incorrectly.	Check the DCE hostname in the file /opt/dcelocal/dce_cf.db. Check that the /etc/hosts file contains a line formatted as xxx.xx.xx.xx *hostname* telcolan. If the line is incorrect, correct it using the RMI. Reconfigure DCE on the SDM. Refer to the procedure, "Distributed Computing Environment – Configuring an SDM in a DCE cell" on page 6-97 in the "SDM system administration procedures" chapter of this document.
cannot find CLLI (cm alias) entry in /etc/hosts file	Dcemonitor cannot identify the CLLI of the switch.	The CLLI is dynamically transmitted from the CM to the SDM and stored in the /etc/hosts file. Check the file for a line formatted as xxx.xx.xx.xx cm *clli*. If the file does not contain this line, execute the Change command at the connectivity (Con) menu level of the RMI, and accept the default values. See the "SDM maintenance overview" chapter for more information.
cannot get the list of keytabs from the config hostdata database	Dcemonitor cannot list the key tables for the machine.	At the dcecp prompt, execute the dcecp command manually as the root user by typing "keytab catalog". Note the error message. You may have to reconfigure DCE on the SDM. If required, refer to the procedure, "Distributed Computing Environment – Configuring an SDM in a DCE cell" on page 6-97 in the "SDM system administration procedures" chapter of this document.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`self keytab cannot be shown`	Dcemonitor cannot list the keys for the machine “self” principal, the principal name that the DCE daemon uses.	At the dcecp prompt, execute the dcecp command manually as the root user by typing “keytab show self”. Note the error message. You may have to reconfigure DCE on the SDM. If required, refer to the procedure, ”Distributed Computing Environment – Configuring an SDM in a DCE cell” on page 6-97 in the “SDM system administration procedures” chapter of this document.
`host data cannot be shown`	Dcemonitor cannot list local host data information.	At the dcecp prompt, execute the dcecp command manually as the root user by typing “show hostdata cell_name”. Note the error message. You may have to reconfigure DCE on the SDM. If required, refer to the procedure, ”Distributed Computing Environment – Configuring an SDM in a DCE cell” on page 6-97 in the “SDM system administration procedures” chapter of this document.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`Detected a CLLI mismatch between` *`principal`* `and the SDM's CLLI:` *`clli`*`. Server reconfiguration is required.`	Dcemonitor has detected that the CLLI portion of one of the application server names is different from the CLLI of the switch stored in the /etc/hosts file because of a recent change in the switch CLLI. The format in the /etc/hosts file may also be incorrect.	Check that the /etc/hosts file contains a line formatted xxx.xx.xx.xx cm *clli*. If the CLLI is incorrect, correct it on the CM. If the problem is with the application server principal name, remove each application server, and recreate. To identify all application servers on an SDM, type "key show [key catalog]" at the dcecp prompt. Refer to the procedures,"Distributed Computing Environment – Removing a DCE based SDM application server" on page 6-110 and "Distributed Computing Environment – Configuring an SDM in a DCE cell" on page 6-97 in the "SDM system administration procedures" chapter of this document.
`endpoint cannot be shown`	Dcemonitor cannot list the remote procedure call (RPC) endpoint information.	From the dcecp prompt, execute the dcecp command manually as the root user by typing "show endpoint". Note the error message. You may have to reconfigure DCE on the SDM. If required, refer to the procedure, "Distributed Computing Environment – Configuring an SDM in a DCE cell" on page 6-97 in the "SDM system administration procedures" chapter of this document.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`could not get clearing house information`	Dcemonitor cannot list the CDS clearing houses.	From the dcecp prompt, execute the dcecp command manually as the root user by typing “clearinghouse catalog”. Note the error message.
	CDS is malfunctioning.	Ensure that the CDS server is functioning properly.
	The IP address of the CDS server may have changed. Cdsadv cannot find the server because its broadcasts are blocked by a router.	Check the IP address of the CDS server. You may have to reconfigure DCE on the SDM. If required, refer to the procedure, ”Distributed Computing Environment – Configuring an SDM in a DCE cell” on page 6-97 in the “SDM system administration procedures” chapter of this document.
`Cdscache cannot be dumped`	Dcemonitor cannot dump the contents of its local directory cache.	At the dcecp prompt, execute the dcecp command manually as the root user by typing “cdscache show *clearinghouse*”. Note the error message.
	The IP address of the CDS server may have changed.	Check the IP address of the CDS server.
	Cdsadv is unable to find the server because its broadcasts are blocked by a router. CDS is malfunctioning. The IP address does not match the IP address of the CDS server.	If the SDM is separated by a router from the CDS server, it depends on defined cached server information stored in the cache. As root user on the SDM, check the IP addresses by typing: • “cd /opt/dcelocal/var/adm/ directory/cds” • “cat cds_cache.wan”

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
	The number of the current cache dump does not match the number contained in cds_cache.version.	Check that the current cache dump which corresponds to the cds_cache.0000xxxx file, matches the number contained in the cds_cache.version by typing • "ls cds_cache*" • "cat cds_cache.version" If the cds_cache.0000xxxx file does not match the number contained in the cds_cache.version, rename the cds_cache.0000xxxxfile and the cds_cache.version files to a temporary name, and restart the daemons by typing • "/etc/dce.clean" • "/sdm/mtce/dce/dcestart" Ensure that the CDS server is functioning properly.
`directory cannot be shown`	Dcemonitor cannot perform a basic CDS command. CDS is malfunctioning.	At the dcecp prompt, execute the dcecp command manually as the root user by typing "show dir / .: " Ensure that the CDS server is functioning correctly.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
`could not get dts synchronization information` or `clock cannot be shown`	Dcemonitor cannot get status information from the DTS daemon.	At the dcecp prompt, execute the dcecp command manually as the root user by typing • "dta show -all" • "clock show"
	The cell security service or CDS are malfunctioning.	Ensure that the cell security service and the CDS server are functioning properly.
	The time on the SDM is not within 5 min of the security server in the DCE cell.	Use the UNIX date command to check the SDM time. Ensure that the SDM time is within 5 min of the cell's security server. SDMs and security servers can be on different time zones if their times are within 5 min of each other when they are converted to universal time clock (UTC).
`DTS clock not synchronized, undetermined drift` or `DTS drifting, more than 2 minutes off` or `DTS drifting, more than 4 minutes off, DCE will fail soon`	The SDM internal clock is not properly synchronized to the DTS time servers on the network.	At the dcecp prompt, type "clock show" to determine if the synchronization is improving or deteriorating. The output of the command is `1997-01-31-13:52:23.818-05:00I0.751 [-----] imprecision`. The value after the "I" is the imprecision. Repeat the command over time, and look at the imprecision. If the imprecision is decreasing, wait for the clocks to synchronize themselves. If the imprecision is increasing, or is undetermined (as indicated by a set of dashes), the problem must be corrected before the SDM clock differs over 5 min with the security server clock. If the time difference exceeds 5 min, the DCE server to the SDM will terminate.

—continued—

Table 3-3
DCE problem text at RMI Con menu level (continued)

Problem text	Trigger	Action
	The SDM cannot find enough DTS time servers to synchronize with.	Determine if the SDM is finding enough DTS time servers to synchronize with by typing “dts show -all” at the dcecp prompt. Look at the value for `toofewservers` and `nointersections` counters. Check to see if the value is anything but zero, and whether it is increasing each time the DTS attempts to resynchronize.
	The SDM does not have access to enough local or global servers.	Determine if the SDM has access to enough local or global servers. The minimum number of servers is indicated by the minservers attribute . Display the minservers attribute by typing “dts show -all” at the dcecp prompt.
	The LAN profile does not contain machines that are running as DTS local servers.	At the dcecp prompt, check the LAN profile by listing the LAN that the SDM was commissioned on by typing • “profile show / . :/hosts/*SDM hostname/*profile” • “rpcprofile list *profile obtained above*” Ensure the profile contains enough machines that are running as DTS local servers. (There must be at least three DTS servers per LAN). Review *OSF DCE Administration Guide – Core Components* for more guidelines on how to administer DTS.
	—end—	

SDM maintenance procedures

Introduction to SDM maintenance procedures

This chapter contains SDM maintenance procedures that can be performed by operating company personnel who have maintenance user (or root user) permissions for accessing the SDM. Each procedure contains the following:

- explanatory and context-setting information
- summary flowchart
- step-action instructions

Explanatory and context-setting information

Depending on the type of procedure, the first page of each procedure may contain the following headings:

- Indication (where an alarm appears on the MAP display)
- Meaning (what the alarm means)
- Impact (how the alarm affects service)
- Application (why you would perform the procedure)
- Action (how to use the flowchart and step-action instructions)

Summary flowchart

The flowchart is only a summary of the main actions, decision points, and possible paths you may take. Do not use the summary flowchart to perform the procedure. Instead, use it to preview what you will be doing and to prepare for it. For example, if you see that the procedure involves actions at the SDM site, you will know to advise that office before you begin the step-action instructions.

Step-action instructions

The step-action instructions tell you how to perform the procedure. Normally you will perform the steps in order, but you may be directed to return to a previous step and repeat a sequence. The successful completion of a step may depend on previous steps; therefore, always perform the steps in the order specified.

The step-action instructions provide the command syntax and system information you use or see while performing the procedure. For help on DMS and SDM commands or output, see the "About this document" chapter at the beginning of this document.

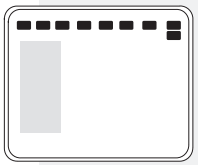
Return key and Enter key

The carriage return key is identified in different ways (such as Enter, Return or Carriage Return) on various types of terminals. It is always used to enter commands and parameters into the system.

The procedures contained in this book and in other NTPs instruct you to press the Enter key after each step. If your terminal has a Return key, press the Return key instead. Do not press the Enter key located beside the numeric key pad.

Clearing MAP alarms triggered by the SDM APPL SDM minor

Application



CM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	**APPL SDM**
.	.	.	.		.	.	.	.	

Use this procedure to clear an APPL SDM minor MAP alarm that has been triggered by the SDM.

Indication

At the MTC level of the MAP display, SDM appears under the APPL header of the alarm banner. This appearance indicates an SDM minor alarm.

Meaning

An SDM minor alarm indicates that the SDM is in manual-busy (ManB) or in-service trouble (ISTb) state.

Impact

If the SDM state at the MAP display is ManB, the SDM was set to that state by the MAP command.

If the SDM state at the MAP display is ISTb, the computing module (CM) is receiving ISTb status from the SDM. One or more of the following conditions exist:

- One or more SDM applications have failed, but at least one application has not failed.
- A system software resource has exceeded its alarm threshold.
- An automated incremental software backup has failed.
- The SDM is cannot communicate with one or more defined nodes on the local area network (LAN) of the operating company
- The Distributed Computing Environment (DCE) is not in service
- An SDM application is reporting an in-service trouble condition.
- A hardware device failure has been reported.
- Disk mirroring is in progress or has failed.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

- There is an Internet protocol (IP) mismatch between the CM and the SDM.

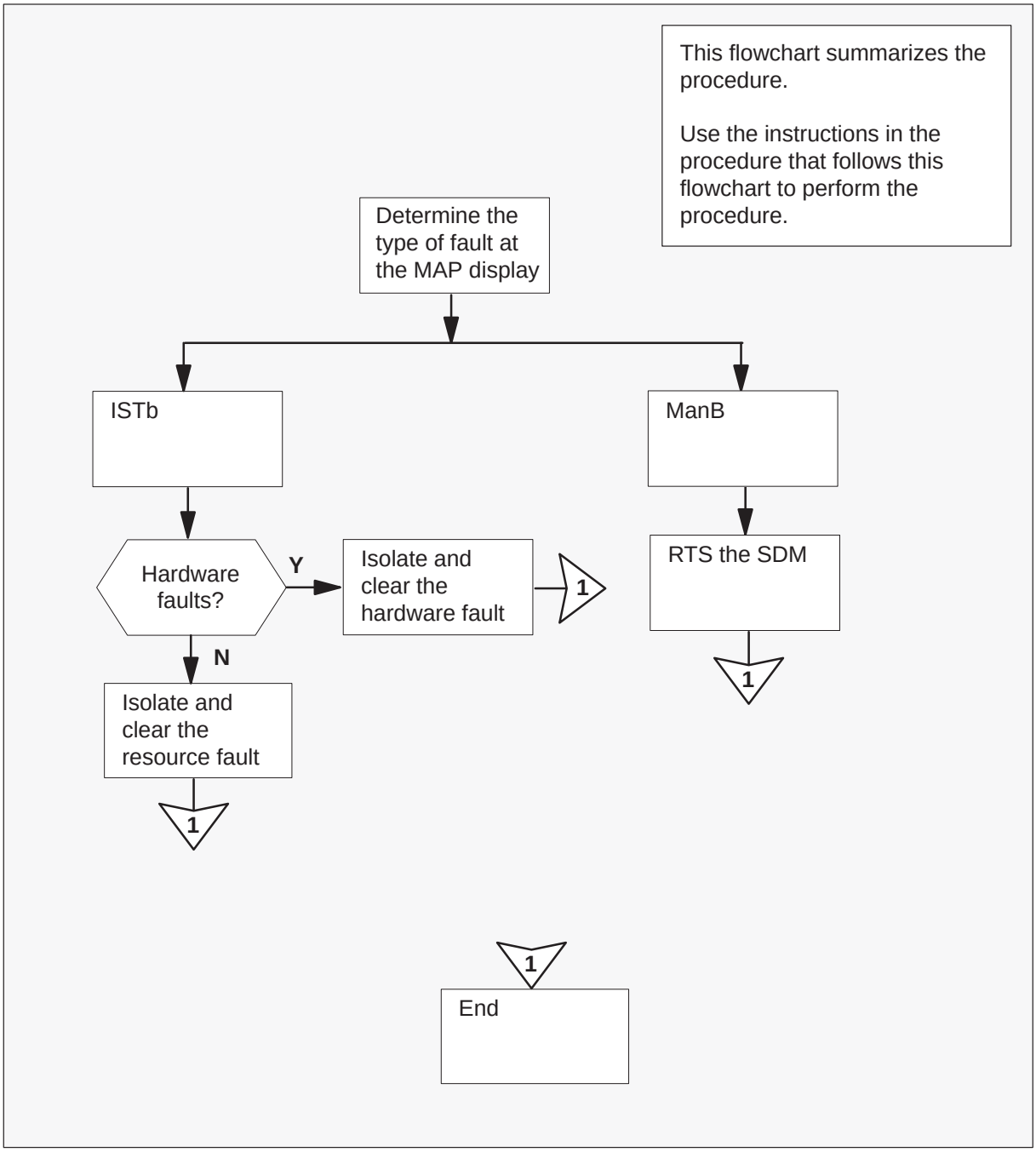
Note: If all SDM applications fail, the SDM node state is system busy (SysB). The system generates an APPL SDM critical or APPL SysB critical alarm.

Action

The following flowchart is only a summary of the procedure. Use the instructions in the step-action procedure that follows the flowchart to clear the alarm.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

Summary of Clearing MAP alarms triggered by the SDM–APPL SDM minor



Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

Clearing MAP alarms triggered by the SDM – APPL SDM minor

At the MAP display

1 Access the SDM level of the MAP display by typing

>MAPCI; MTC; APPL;SDM
and pressing the Enter key.

Example response:

```
SDM 0  ISTb    Links_OOS: 2
```

2 Check the node state of the SDM at the MAP display.

If the SDM is	Do
ManB	step 3
ISTb	step 4

3 If applicable, determine from office records or other personnel why the SDM was set to manual busy state. When permissible, return the SDM to service by typing

>RTS
and pressing the Enter key.

Response:

```
SDM RTS initiated.
SDM RTS completed.
```

Go to step 88.

4 Obtain fault status information from the SDM by typing

>QUERYSDM FLT
and pressing the Enter key.

5 Determine if the response indicates a hardware device fault.

If a hardware device fault is	Do
not indicated	step 6
indicated	step 66

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

6 Determine the type of fault. Note the log fault type for use in later steps.

If the fault is	Do
an exceeded resource threshold	step 7
a logical volume is integrating	step 15
a DCE problem	step 16
an automated incremental backup	step 30
anything else	step 17

7 From the response to the QuerySDM FLT command, determine the type of system resource that has exceeded its alarm threshold.

If the resource exceeded is	Do
swap space	step 8
number of processes	step 8
number of swap queue entries	step 8
number of zombie processes	step 8
CPU (number of run queue entries)	step 8
logical volume (% full)	step 12

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

8 Access the System (Sys) menu level of the RMI by typing

>SYS

and pressing the Enter key.

Example response:

```
SDM Node State:               ISTb
SDM System State:             ISTb
SDM Storage State:            InSv
Automated Incremental Backup:  Completed on 11/16/97

# Description                              Current/Threshold
1 CPU (run queue entries):                      1/  5
2 Number of Processes:                         63/250
3 Number of Zombies:                            0/  3
4 Swap Space (% full):                         72/ 70*
5 Number of Swap Queue Entries:                 0/  2
```

9 Check the current level of the software resource by locating the resource on the screen.

Note: A pair of numbers is located in the column next to the software resource. The first number is the current level of the resource. The second number is the alarm threshold. In the example response in step 12, the current level of "Swap Space" is 72. This level exceeded the threshold of 70.

10 If the current level of the software resource is acceptable, increase the size of the threshold to clear the alarm. Complete the procedure, "Changing system thresholds," in this chapter, and return to this point.

Note: If you are not sure of the acceptability of the software resource level, go to step 91.

If the current level of the software resource is not acceptable, go to step 87.

11 Wait 5 minutes. Check to see if the alarm has cleared.

If the	Do
alarm has not cleared	step 87
alarm has cleared	step 88

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

12

CAUTION
Potential Service Interruption
A logical volume on the SDM must never reach 100% disk full. The system enters into abnormal conditions when a logical volume reaches 100% disk full.

If a logical volume exceeds its alarm threshold, contact your system administrator. The system administrator must assess the current condition of the logical volume and take appropriate action immediately. If required, contact Nortel for assistance.

The usage level of the specified logical volume has exceeded its alarm threshold.

Access the storage menu level of the RMI by typing

>STORAGE
and pressing the Enter key.

Example response:

```
SDM Node State:            ISTb
SDM System State:          ISTb
SDM Storage State:         ISTb

Disk mirroring (rootvg):                        Mirrored
   Volume             Size (MB)        (% full/ threshold)
 1 /                     240                     52/ 80
 2 /usr                  204                     82/ 90
 3 /var                  40                      35/ 70
 4 /tmp                  24                      21/ 90
 5 /home                 304                     75/ 70*
 6 /sdm                  304                     47/ 90
 7 /home/sba              16                      7/ 80
(unallocated)            608
```

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

13 If the current usage level of the logical volume is acceptable, increase the size of the logical volume threshold. Complete the procedure, “Changing logical volume thresholds,” in this chapter, and return to this point.

Note: Do not change the system threshold if the current usage of the logical volume is greater than 95%.

If the current usage level of the logical volume is not acceptable, complete the procedure, “Increasing the size of a file system,” in this chapter. If you require assistance to help you determine if the current resource is acceptable, go to step 87.

14 Wait 5 minutes. Check to see if the alarm has cleared.

If the	Do
alarm has not cleared	step 87
alarm has cleared	step 88

15 Allow the logical volume reintegration process to complete without intervention. This process is initiated automatically whenever an I/O controller module is returned to service, and synchronizes (mirrors) data on the two hard disks.

Note: Depending on the amount of data that is stored in the affected volume group, the reintegration process can take about 30 min to complete. The status of the root volume group (rootvg) reintegration can be monitored by selecting the storage option from the system (Sys) menu level of the RMI.

Go to step 88.

16 Have your system administrator isolate and clear the DCE problem.

Note: DCE troubleshooting information is provided in the “SDM system administration overview” chapter of this document.

Go to step 88.

At the local or remote VT100 console

17 Log in to the SDM as the root user or the maint user.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

18 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

19 Access the maintenance (Mtc) menu level of the RMI by typing

>2
and pressing the Enter key.

20 Proceed according to the type of fault defined in step 10 as “anything else.”

If the fault is	Do
an application software problem (package/process fault)	step 21
an automated incremental backup failure	step 30
a logical volume is not mirrored	step 39
a CM connectivity problem (fault type CM)	step 41
an operating company LAN connectivity problem (fault type LAN)	step 57

21 Access the application (Appl) menu level of the RMI by typing

>4
and pressing the Enter key.

Example response:

```
SDM Node State:                 InSv
SDM Application State:          InSv

 # Package Description          Version       State
 1 Table Access Service         9.0.21.0      InSv
 2 OM Access Service            9.0.21.0      ManB
 3 Log Delivery Service         9.0.21.0      InSv
```

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

22 Determine the affected application from the display and note its key number, shown under the header "#".

If the package is	Do
Table Access Service	step 27
Operation Measurements	step 27
Log Delivery Service	step 27
anything else	step 29

23 Proceed depending on the state of the out-of-service application software package.

If the package state is	Do
ManB	step 24
ISTb or SysB	step 26
Fail	step 27

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

24 The application software package is in manual-busy state. Determine from office records or other personnel why the application was manually removed from service. When permissible, return the application software package to service by typing

>RTS key

and pressing the Enter key.

where

key is the key number of the application, shown under the header "#".

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

Go to step 88.

25 The specified application software package has been set to in-service trouble (ISTb) state during initialization. Allow 10 min for the packages to complete initialization.

If the package	Do
remains ISTb	step 87
changes to InSv state	step 88

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

26 The specified application software package was set to system-busy (SysB) or in-service trouble (ISTb) state because it failed for one of the following reasons:

- The system cannot restart the package.
- The application has restarted and failed three times within its designated failure threshold (10 min).

At the application menu level of the RMI, manually busy the affected application software package by typing

>BSY key

and pressing the Enter key.

where

key is the key number of the application, shown under the header "#"

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

27 Return the application to service by typing

>RTS *key*
and pressing the Enter key.

where

key is the key number of the application, shown under the header "#"

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

28 Proceed depending on the state of the application software package.

If the package	Do
remains ISTb	step 87
changes to InSv state	step 88

29 Consult the documentation for the specified application software package to diagnose and clear the problem.

Go to step 88.

30 Note the affected tape drive (RMT0 or RMT1) from the QuerySDM FLT response, and the timestamp at which the automated incremental backup failed.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

31 Determine from office records and log reports if the affected digital audio tape (DAT) drive was out of service at the schedule time for the backup.

Note: If the affected DAT drive is still out of service, the alternate DAT drive can be specified as the target device for manual or automated backup scheduling, or both. Use the Backup utility that is available at the administration (Admin) menu level of the RMI to specify the target device.

If the DAT drive was	Do
in service	step 32
out of service (and has since been returned to service)	step 36

At the SDM

32 Physically verify that the tape used to store incremental backups is in the appropriate tape drive (RMT0 or RMT1).

If the tape is	Do
absent	step 33
present	step 34

33 Insert the tape used for automated incremental backups into the tape drive.

Go to step 36.

34 Eject the tape from the tape drive and inspect it for physical damage.

If the tape is	Do
damaged	step 35
appears undamaged	step 37

35 Insert a new tape to store automated incremental backups.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

At the local or remote VT100 console

36 Perform manual incremental backup using the procedure, “Creating SDM backup tapes – Manual incremental backup (I–tape),” on page 6-39 in the System Administration Procedures section of this document.

Go to step 88.

37 Verify the operation of the tape drive as follows:

- Use the Backup utility at the administration (Admin) menu level of the RMI to perform a manual incremental backup. See the procedure, “Creating SDM backup tapes – Manual incremental backup (I–tape),” on page 6-39 in the System Administration Procedures section of this document.
- When the backup is complete, list the contents of the tape to verify that the DAT drive can successfully write to and read from the tape.

If the DAT drive	Do
is not working	step 38
appears to be functional	step 87

38 Replace the affected NTRX50FQ I/O controller module using the procedure in the hardware replacement procedures section of this document. When you have completed that procedure, continue this procedure at step 36.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

39 Logical volumes are not mirrored under the following circumstances:

- an I/O controller module is out of service
- a hard disk drive is out of service
- a hard disk has just returned to service and the reintegration process is just about to start (as described in step 19)

In rare cases, the system cannot start or complete automatic volume group reintegration. For example, the reintegration process is interrupted due to a power failure or system reboot.

Proceed depending on the reason for the mirroring problem, as stated in the reported log (noted in step 6).

If the mirroring problem is	Do
due to an abnormal reintegration process interruption or failure	step 40
due to recently returned-to-service hardware	step 15
due to out-of-service hardware	step 69

40 Contact Nortel to take the necessary corrective action, identifying the volume group reintegration problem.

Go to step 88.

41 Determine if the response indicates an IP address mismatch.

If the response indicates	Do
an SDM IP address mismatch	step 42
a CM IP address mismatch	step 43
anything else	step 87

At the MAP display

42 Access table SDMINV, and record the datafilled value for the SDM CM-side IP address (field IPADDR), by typing

>TABLE SDMINV; LIST ALL
and pressing the Enter key.

Go to step 44.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

At the MAP display

43 Access table IPNETWRK and record the datafilled value for the CM IP address (field CMIPADDR), by typing

>TABLE IPNETWRK; LIST ALL
and pressing the Enter key.

At the local or remote VT100 console

44 Access the CM-to-SDM connectivity (Con) menu level by typing

>CON
and pressing the Enter key.

45 Determine how the CM IP address, SDM CM-side IP address, and CM/SDM netmask are commissioned on the SDM by typing

>QUERYSDM
and pressing the Enter key.

Example response:

```
CM IP Address:          47.105.155.1
SDM IP Address:         47.105.155.6
CM/SDM Netmask:         255.255.255.240
```

46 Using office records, have your system administrator review the IP address information to determine the correct values for the system.

If	Do
the CM IP address datafill is incorrect	step 47
the SDM CM-side IP address datafill is incorrect	step 48
any of the IP address parameters are commissioned incorrectly on the SDM	step 49
all values appear to be correct	step 87

At the MAP display

47 Correct the datafill for the CM IP address in table IPNETWRK by typing

>TABLE IPNETWRK; CHA CMIPADDR
and pressing the Enter key.

Go to step 88.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

48 Correct the datafill for the SDM CM-side IP address in table SDMINV by typing

>TABLE SDMINV; CHA IPADDR
and pressing the Enter key.

Go to step 88.

At the MAP display

49 Manually busy the SDM by typing

>BSY
and pressing the Enter key.

Response:

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

At the local or remote VT100 console

50 At the connectivity (Con) menu level of the RMI, access the change editor for the CM side IP parameters by typing

>CHANGE
and pressing the Enter key.

51 Each editable parameter is displayed in turn. Press the Enter key until the parameter you wish to correct is displayed.

52 At the command line, type the correct value and press the Enter key.

Example response:

```
Values to be changed:
   CM IP address:       47.105.145.1
   SDM IP address:      47.105.145.6
   SDM-SDM LAN netmask: 255.255.255.248

Enter Y to confirm, N to reject or E to edit.
```

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

53 Determine if the displayed values are correct.

If the displayed values are	Do
incorrect	step 54
correct	step 55

54 Edit the values by typing

>E
and pressing the Enter key.

Go to step 51.

55 Save the change and exit the change editor by typing

>Y
and pressing the Enter key.

At the SDM level of the MAP display

56 Return the SDM to service by typing

>RTS
and pressing the Enter key.

Response:

```
SDM RTS initiated.
SDM RTS completed.
```

Go to step 88.

57 Contact your LAN network administrator to determine if the communications problem is external to the SDM. That is, the communications problem is due to other problems on the operating company LAN. (For example, the LAN host is out of service.)

If the fault is	Do
not on the operating company LAN	step 58
on the operating company LAN	step 88

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

At the local or remote VT100 console

58 Access the LAN menu level of the RMI by typing

>LAN
and pressing the Enter key.

Example response:

```
# DESCRIPTION       HOSTNAME    ADDRESS          STATE
1 626 FT Machine    bnode7c8    47.18.32.25      SysB
```

59 Determine if the IP address shown for the affected LAN hostname is correct.

If the IP address is	Do
incorrect	step 60
correct	step 87

60 Access the change editor by typing

>CHANGE n
and pressing the Enter key.

where

n is the numeric key for the hostname entry, shown under the "#" header

61 Each editable parameter is displayed in turn. Press the Enter key until the IP address is displayed.

62 Type the correct IP address for the LAN node at the command line and press the Enter key.

Example response:

```
Values to be changed for Telco Node 1:
   Telco Node Description: 626 FT Machine
   Telco Node Hostname: bnode7c8
   Telco IP Address: 47.18.32.52

Enter Y to confirm, N to reject or E to edit.
```

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

63 Determine if the displayed values are correct.

If the displayed values are	Do
correct	step 64
incorrect	step 65

64 Save the change and exit the change editor by typing

>Y
and pressing the Enter key.

Note: The node state changes to InSv within 2 min.

Go to step 88.

65 Edit the values by typing

>E
and pressing the Enter key.

Go to step 61.

At the MAP display

66 Determine if the fault reason indicates a cable fault.

If a cable fault is	Do
indicated	step 67
not indicated	step 69

Note: If there is a cable fault, the Ethernet device is the only faulty device on the module.

67 From the QuerySDM FLT response, determine which cable is affected and its location. By physical inspection, determine if the cable has been disconnected or physically damaged.

If a cable	Do
requires reconnection or repair	step 68
appears undamaged and correctly connected	step 87

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

68 Reconnect, repair, or replace the cable as appropriate.

Go to step 88.

69 From the QuerySDM FLT response, determine the affected device type and its state.

If the device state is	Do
ManB	step 70
Failed	step 75

70 Determine from office records or other personnel why the device was manually removed from service. When permissible, return the device to service.

71 Log in to the SDM as the root or maint user.

72 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

73 Access the hardware menu level of the RMI by typing

>HW
and pressing the Enter key.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

74 Return the device to service by typing

>RTS n device
and pressing the Enter key.

where

n is the domain number (0 or 1) of the device that you are returning to service

device is hardware device name that you are returning to service.

Example response:

```
Hardware RTS : Domain 0 Device ETH - Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device ETH – Command submitted.
```

Go to step 88.

75 Determine if the QuerySDM FLT response indicates an interconnect module (ICM) failure.

If an ICM failure is	Do
indicated	step 76
not indicated	step 86

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

76 Have qualified power maintenance personnel verify that power is available from the MSP to the failed ICM.

Note: If the SDM loses one –48V dc power feed, it continues to provide service using the other power feed. The loss of one feed removes one input/output (I/O) domain from service. On the affected modules, the module in-service LEDs are off, and the out-of-service LEDs are on. These modules cannot be returned to service until power is restored.

If	Do
the ICM has failed due to interruption of its power feed	step 77
the ICM power feed is OK	step 86

At the local or remote VT100 console

77 Log in to the SDM as the root user or the maint user.

78 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

79 Access the hardware menu level of the RMI by typing

>HW
and pressing the Enter key.

Clearing MAP alarms triggered by the SDM APPL SDM minor (continued)

80 Determine if one CPU has dropped out of service (indicated by an “F” under its header at the hardware menu level).

If	Do
one CPU is out of service	step 81
both CPUs are in service	step 82

81 Return the out-of-service CPU to service and start CPU reintegration by typing

>RTS n CPU
and pressing the Enter key.

where

n is the domain where the CPU is located (0 or 1)

Note: The domain is 0 if the CPU controller module is in slots 6 and 7, and 1 if it is in slots 10 and 11 of the main chassis.

Example response:

```
Hardware RTS : Domain 0 Device CPU – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS: Domain 0 Device CPU – Command submitted.
```

Note: At the hardware menu level of the RMI, the CPU state changes to “S”, indicating that the CPUs are reintegrating. The reintegration process takes about 2 min to complete. The actual time may vary depending on the processor load. When reintegration is complete, the CPU status changes to in-service, indicated by a dot (.).

82 Have qualified power maintenance personnel restore the power feed to the ICM.

Clearing MAP alarms triggered by the SDM APPL SDM minor (end)

83 At the hardware (Hw) menu level of the RMI, return the main chassis ICM (that has failed due to loss of power) to service by typing

>RTS domain ICM1

and pressing the Enter key.

where

domain is the I/O domain where the ICM is located (0 or 1)

Example response:

```
Hardware RTS : Domain 0 Device ICM1 – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS: Domain 0 Device ICM1 – Command submitted.
```

Note: The out-of-service ICM can be identified by an “F” under its header on the RMI display. It can also be visually identified at the back of the SDM by its in-service LED off, and its out-of-service LED on.

84 After the ICM returns to service, the system automatically returns all the subtending nodes in its I/O domain to service. When each affected I/O controller module has returned to service, it begins to reintegrate with its corresponding I/O controller module in the other I/O domain. During this period, the System In Service light flashes. The disk reintegration period for each affected I/O controller module lasts about 30 min. The actual amount of time may vary depending on the amount of data stored on the disks, and the current processor load.

85 Upon completion of the disk reintegration, check the MAP MTC alarm banner for SDM-related alarms. Use the alarm clearing procedures in this document to clear any remaining faults.

Go to step 88.

86 Replace the failed device using the appropriate procedure in the “SDM hardware replacement procedures” chapter of this document.

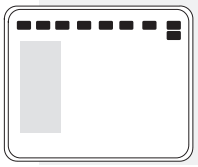
Go to step 88.

87 Contact the personnel responsible for the next level of support.

88 You have completed this procedure.

Clearing MAP alarms triggered by the SDM APPL SDM critical

Application



CM	MS	IOD	Net	PM	CCS	Lns	Trks	Ext	APPL
.	.	.	.		.	.	.	.	SDM *C*

Use this procedure to clear an APPL SDM critical MAP alarm that has been triggered by the SDM.

Indication

At the MTC level of the MAP display, SDM *C* appears under the APPL header of the alarm banner and indicates an SDM critical alarm.

Meaning

An SDM critical alarm indicates that the SDM is sending system busy status to the CM because it is out of service, or the CM has designated the SDM as system busy because it is unable to communicate with the SDM.

Impact

If the SDM is out of service, all SDM applications are unavailable.

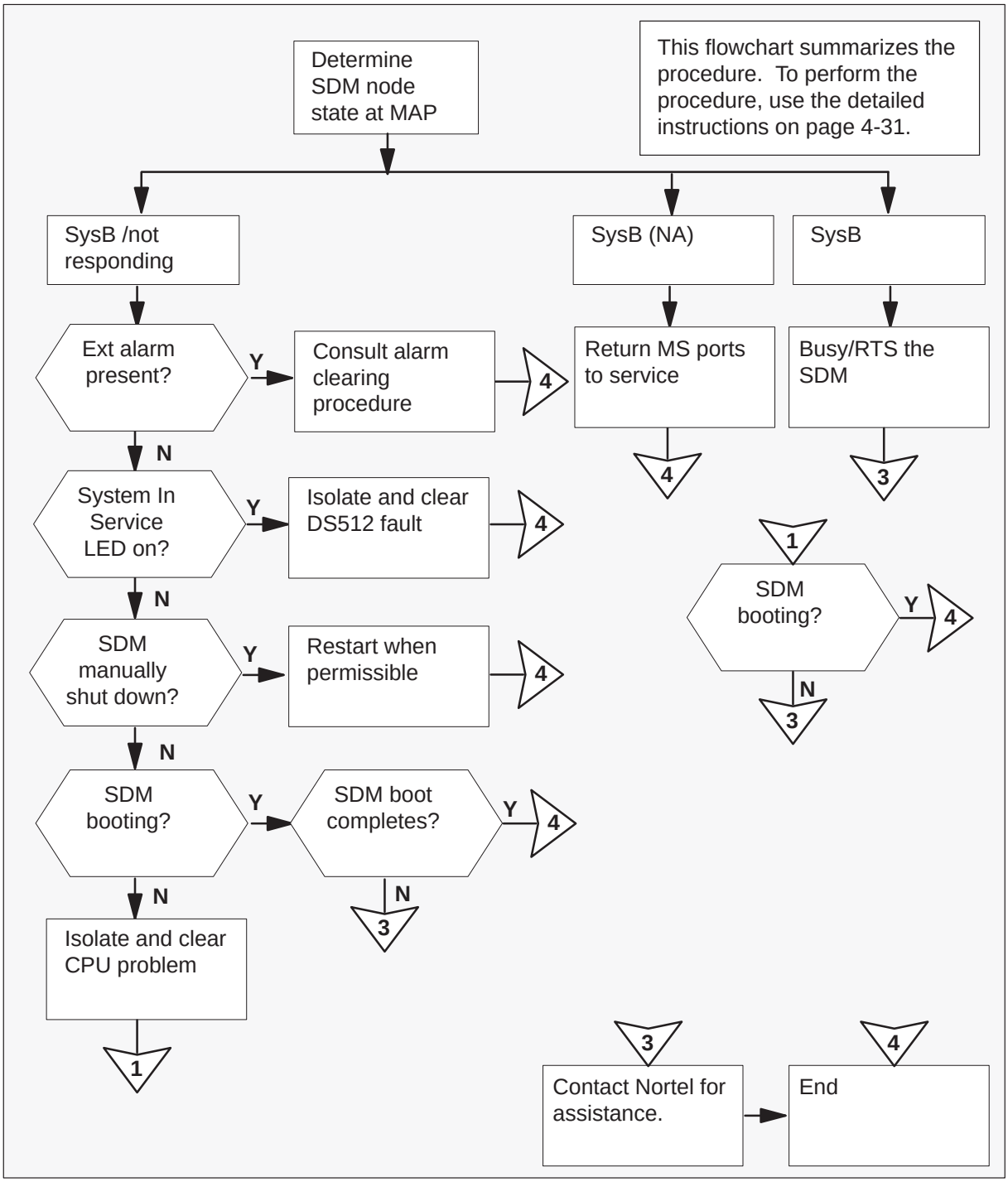
If the CM is unable to communicate with the SDM, the local state and operating condition of the SDM are unknown to the CM. MAP commands requesting state changes to the SDM are not sent to the SDM, and MAP requests for information from the SDM cannot be completed. The SDM remote maintenance interface (RMI) can be used to change the local state of the SDM, or obtain information about the SDM, when the CM-SDM link is not functioning. When communications are restored, the SDM local state aligns itself to the CM view of its state.

Action

The following flowchart is only a summary of the procedure. Use the instructions in the step-action procedure that follows the flowchart to clear the alarm.

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

Summary of Clearing MAP alarms triggered by the SDM — APPL SDM critical



Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

Clearing MAP alarms triggered by the SDM - APPL SDM critical

At the MAP display

1 Access the SDM level of the MAP display by typing

>MAPCI; MTC; APPL;SDM
and pressing the Enter key.

Example response:

```
SDM   SysB(NA)    Links_OOS: 4
```

2 Determine the state of the SDM.

If the state of the SDM is	Do
SysB (NA)	step 4
SysB / The SDM is not responding	step 3
SysB	step 70

3 Determine from the response if any links are out of service, as indicated by "Links_OOS:" (see step 1).

If	Do
any of the links are out of service	step 5
all links are in service	step 15

4 The CM has designated the SDM as system busy because all four message switch (MS) ports that provide the DS512 links to the SDM are unavailable. The SDM may still be operational, but it is unable to communicate with the computing module (CM).

5 Determine the MS hardware that provides the DS512 links to the SDM by typing

>TRNSL
and pressing the Enter key.

Example response:

```
SDM 0 DOMAIN 0 PORT 0 (MS 0:15:0) OK    ,C MsgCnd:Closed
SDM 0 DOMAIN 0 PORT 1 (MS 1:15:0) ManB     MsgCnd:Closed
SDM 0 DOMAIN 1 PORT 0 (MS 0:15:1) OK    ,C MsgCnd:Closed
SDM 0 DOMAIN 1 PORT 1 (MS 1:15:1) ManB     MsgCnd:Closed
```

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

6 Record the MS port card number that is associated with the SDM DS512 links.

Note: In the example response shown in step 5, the port card number is 15.

7 Access the MS level of the MAP display by typing

>MS
and pressing the Enter key.

8 Access the shelf level by typing

>SHELF 0
and pressing the Enter key.

9 Access the MS port card level that is associated with the SDM DS512 links by typing

>CARD cardno
and pressing the Enter key.

where

cardno is the MS card number noted in step 6.

10 Note the status of the MS port card and its ports. If port status indication is P-side busy, then continue with step 11. Otherwise, use the generic MS alarm clearing procedures provided with your DMS switching system to return the ports to service, and then continue this procedure.

11 Access the SDM level of the MAP display by typing

>APPL;SDM
and pressing the Enter key.

Example response:

```
SDM 0 InSv    Links_OOS: .
```

12 Determine the state of the SDM.

If the state of the SDM is	Do
InSv	step 74
SysB (NA)	step 73
SysB	step 70
SysB /The SDm is not responding	step 15
ISTb	step 13

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

13 Allow 2 min for SDM applications to re-establish communications with the CM and return to service. When this is complete, the SDM state automatically changes to InSv, unless another fault exists.

Note: 2 min is an approximate time value. The actual time required for the system to restart all applications varies depending on the number and type of application software packages installed on your SDM.

If the SDM state is	Do
InSv	step 74
remains ISTb after 2 min	step 14

14 Clear the ISTb state using the procedure ”Clearing MAP alarms triggered by the SDM – APPL SDM minor” on page 4-3 of this document.

Go to step 74.

15 Access the EXT level of the MAP display by typing

>EXT
and pressing the Enter key.

16 List all major EXT alarms by typing

>LIST MAJ
and pressing the Enter key.

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

17 Determine if the SDM has triggered an FSP frame fail alarm for the equipment aisle containing the SDM.

If an SDM-related FSP alarm is	Do
present	step 18
not present	step 19

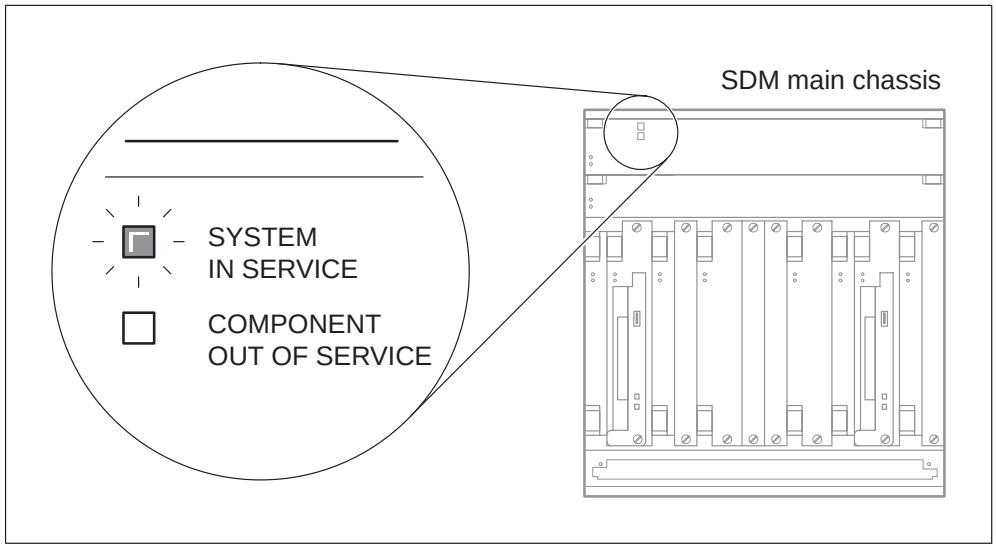
Note: An EXT FSP major alarm triggered by the SDM indicates that one or both -48V dc power inputs to the SDM have failed, or that the SDM has shut down because of thermal failure (overheating).

18 Clear the EXT FSP alarm using the procedure ”Clearing MAP alarms triggered by the SDM – Ext FSP major” on page 4-49 in this document.

Go to step 74.

At the front of the SDM

19 Determine if the System in Service light is on (green).



Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

Note: If the System in Service light is off, but power is available to the system and it has not shut down because of thermal failure (overheating), one or more of the following conditions is present or has occurred:

- System software has crashed.
- The system is booting, or the attempt to boot has failed.
- The system cannot boot because both CPUs or both I/O controller modules containing the root volume group (rootvg) are out of service.
- The system has been manually shut down.

If the System in Service light is	Do
on	step 45
off	step 20

20 Determine from office records or other personnel if the SDM was manually shut down.

If the system was	Do
manually shut down	step 21
not manually shut down	step 22

21 When permissible, restart the SDM by continuing this procedure at step 24.

22 Ensure that the local console is connected to SP0 of the CPU personality module using the designated cable. Ensure that the console is operational and correctly configured for VT100 operation.

At the local VT100 console

23 Determine if the system is booting.

If the system is	Do
booting	step 25
not booting, or the boot has failed	step 24

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

At the front of the MSP

24 Cycle power to the SDM by turning the modular supervisory panel (MSP) breakers off and on. The MSP breakers supply power to the SDM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
contains a main and I/O expansion chassis	turn all four breakers off and on

At the local VT100 console

25 Monitor the boot process at the local console.

If the boot	Do
does not start	step 26
starts but does not complete (returns to the FX-Bug prompt)	step 36
completes normally and the login prompt is displayed	step 35

At the front of the SDM

26 Physically verify that the CPU controller modules (NTRX50FK, FL, or FM) are present in the main chassis (slots 6 and 7, and 10 and 11). Determine if either CPU controller module was accidentally unseated or removed. (This scenario may have occurred if one CPU controller module was in manual busy or system busy state, and the remaining in-service CPU controller module was removed in error.)

If	Do
both CPU controller modules are present	step 31
a CPU controller module was removed or unseated in error	step 27

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

27

WARNING
Static electricity damage
Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Reinsert the CPU controller module that was removed in error.

At the local VT100 console

28 Determine whether the system has begun to boot.

If the system is	Do
booting	step 30
not booting, or the boot has failed	step 29

At the front of the MSP

29 Cycle power to the SDM by turning the MSP breakers off and on. The MSP breakers supply power to the SDM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
contains a main and I/O expansion chassis	turn all four breakers off and on

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

At the local VT100 console

30 Monitor the boot process.

If the boot	Do
does not start	step 31
starts but does not complete (returns to the FX-Bug prompt)	step 36
completes normally and the login prompt is displayed	step 35

At the front of the SDM

31

WARNING
Static electricity damage
Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

32 Verify that each CPU controller module is seated correctly and passes self tests by unseating, and then reseating it. Ensure that both CPU controller modules are seated firmly and the latches are closed snugly. When a CPU controller module is reseated and its latches closed, both LEDs on the CPU controller module turn on solid for a brief period, indicating that the module is powered up, fully seated, and has passed its self tests.

If	Do
one CPU controller module fails its self tests	step 33
both CPU controller modules fail their self tests	step 73
both CPU controller modules pass their self tests	step 34

33 Replace the CPU that failed its self tests. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the top locking lever of the module. (Refer to the appropriate procedure in the “SDM hardware replacement procedures” chapter in this document.)

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

At the local VT100 console

34 Monitor the boot process.

If the boot	Do
does not start	step 73
starts but does not complete (returns to the FX-Bug prompt)	step 36
completes normally and the login prompt is displayed	step 35

At the MAP display

35 Determine the state of the SDM.

If the state of the SDM is	Do
InSv	step 74
SysB (NA)	step 4
SysB	step 70
SysB /The SDM is not responding	step 45
ISTb	step 13

At the front of the SDM

36 Physically verify that the I/O controller modules (NTRX50FQ) that provide root volume group (rootvg) storage for the system, are present in the main chassis (slots 2 and 3, and 13 and 14). Determine if either I/O controller module was accidentally unseated or removed. (This scenario may have occurred if one I/O controller module was in manual-busy or system-busy state, and the remaining in-service I/O controller module was removed in error.)

If	Do
both I/O controller modules are present	step 38
an I/O controller module was removed or unseated in error	step 37

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

37 Reinsert the I/O controller module that was removed in error.

Go to step 39.

38 Unseat and reseat both I/O controller modules in slots 2 and 3, and 13 and 14. Ensure that they are seated firmly and that the latches are closed snugly.

At the front of the MSP

39 Cycle power to the SDM by turning the MSP breakers off and on. The MSP breakers supply power to the SDM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
contains a main and I/O expansion chassis	turn all four breakers off and on

At the local VT100 console

40 Monitor the boot process.

If the boot	Do
does not start	step 41
completes normally and the login prompt is displayed	step 44

41 Perform a system software reinstall using the procedure ”Restoring the SDM – Full restore from S-tape and I-tape” on page 6-61 of this document. When you have restored from the S-tape, and you have begun to reboot the system as instructed by that procedure, return to this point.

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

42 Monitor the boot process.

If the boot	Do
does not complete (returns the FX-Bug prompt)	step 73
completes normally and the login prompt is displayed	step 43

43 Complete the remainder of the procedure ”Restoring the SDM – Full restore from S-tape and I-tape” on page 6-61 of this document and return to this point.

At the MAP display

44 Determine the state of the SDM.

If the state of the SDM is	Do
InSv	step 74
SysB (NA)	step 4
SysB	step 70
SysB /The SDM is not responding	step 45
ISTb	step 13

At the local or remote VT100 console

45 Log in to the SDM as the root or maint user.

46 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

47 Access the connectivity (Con) menu level of the RMI by typing

>CON

and pressing the Enter key.

Example response

```
SDM Node State:                 ISTb
CM Connectivity State:          SysB

Heartbeat status:               SysB
IP address synchronization:     InSv

DS512 Link States:
I/O domain 0, port 0:           Closed
I/O domain 0, port 1:           Closed
I/O domain 1, port 0:           Failed
I/O domain 1, port 1:           Failed
```

48 Determine the DS512 link states.

If	Do
all four links are failed	step 59
any of the links are closed	step 49

49 Note the I/O domain number and port number of each closed link.

At the back of the SDM

50 Physically inspect the fiber link connections to the SDM DS512 personality modules.

If the fiber links	Do
require reconnecting or replacement	step 51
appear undamaged and are correctly connected to the SDM	step 53

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

51

CAUTION
Transmit and receive cables
Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect or replace the fibers on the DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the right.

At the local VT100 console

52 Monitor the link status at the connectivity menu level of the RMI.

If	Do
any of the links are closed	step 53
all four links are InSv	step 74
two links are InSv and two links are failed	step 59

Note: Allow 5 min for the SDM link status to update if one or more fibers were reconnected or replaced.

At the MAP display

53 Determine the MS hardware that provides the DS512 links to the SDM by typing

>TRNSL
and pressing the Enter key.

Example response:

```
SDM 0 DOMAIN 0 PORT 0 (MS 0:15:0) SysB ,P  MsgCnd:Closed
SDM 0 DOMAIN 0 PORT 1 (MS 1:15:0)  OK      MsgCnd:Open
SDM 0 DOMAIN 1 PORT 0 (MS 0:15:1) SysB ,P  MsgCnd:Closed
SDM 0 DOMAIN 1 PORT 1 (MS 1:15:1)  OK      MsgCnd:Open
```

54 Record the MS port card number associated with the system-busy DS512 links identified in step 52.

Note: In the example response shown in step 53, the port card number is 15.

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

At the back of the SDM

55 Physically inspect the fiber link connections to the SDM DS512 personality modules.

If the fiber links	Do
require reconnecting or replacement	step 56
appear undamaged and are correctly connected to the SDM	step 59

56

CAUTION
Transmit and receive cables
Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect or replace the fibers on the DS512 personality module(s) by pressing the fiber cable in, and turning it a 1/4 turn to the right.

At the MAP display

57 Repeat the TRNSL command by typing

>TRNSL
and pressing the Enter key.

Example response:

```
SDM 0 DOMAIN 0 PORT 0 (MS 0:15:0) SysB ,P  MsgCnd:Closed
SDM 0 DOMAIN 0 PORT 1 (MS 1:15:0) OK       MsgCnd:Open
SDM 0 DOMAIN 1 PORT 0 (MS 0:15:1) SysB ,P  MsgCnd:Closed
SDM 0 DOMAIN 1 PORT 1 (MS 1:15:1) OK       MsgCnd:Open
```

58 Determine the state of the DS512 links.

If	Do
any of the links are still closed	step 59
all four links are InSv	step 74

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

Note: Allow 5 min for the SDM link status to update if one or more fibers were reconnected or replaced.

At the local VT100 console

59 Access the hardware (Hw) menu level of the RMI by typing

>HW

and pressing the Enter key.

60 Check the status of the DS512 controller modules, indicated under the “512” header.

If	Do
either DS512 controller module is manual-busy (indicated by an M)	step 61
both DS512 controller modules have failed (indicated by an F)	step 64
one controller is failed and one controller is in service (indicated by a dot)	step 63

61 Determine from office records or other personnel why one or both DS512 controller modules are manually busy. When permissible, return each manual-busy DS512 controller module to service by typing

>RTS n 512

and pressing the Enter key.

where

n is the SDM domain number (0 or 1).

Example response:

```
Hardware RTS : Domain 0 Device 512 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device 512 – Command submitted.
```

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

62 Check the status of the DS512 controller modules, indicated under the “512” header.

If	Do
either DS512 controller module is in service (indicated by a dot)	step 74
both DS512 controller modules have failed (indicated by an F)	step 64
one DS512 controller module is in service, and one DS512 controller module has failed	step 63

63 Return the system-busy DS512 controller modules to service using the procedure ”Clearing MAP alarms triggered by the SDM – APPL SDM minor” on page 4-3.

Go to step 74.

At the front of the SDM

64 Physically verify that the two DS512 controller modules (NTRX50GA, front slots 1 and 12) are present in the main chassis. Determine if either of these modules were accidentally unseated or removed. (This scenario may have occurred if one DS512 controller module was in manual-busy or system-busy state, and the remaining in-service DS512 controller module was removed in error.)

If	Do
both DS512 controller modules are present	step 69
a DS512 controller module was removed or unseated in error	step 65

Note: If both LEDs on the DS512 controller module are off, the module is not seated correctly.

65 Reinsert the DS512 controller module that was removed or unseated in error. Ensure that the module is seated firmly and that the latches are closed snugly.

Clearing MAP alarms triggered by the SDM APPL SDM critical (continued)

At the local VT100 console

66 Return the DS512 controller module to service by typing

>RTS domain 512
and pressing the Enter key.

where

domain is the SDM domain number (0 or 1).

Example response:

```
Hardware RTS : Domain 0 Device 512 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device 512 – Command submitted.
```

67 Check the status of the DS512 controller modules, indicated under the “512” header.

If	Do
both DS512 controller modules have failed (indicated by an F)	step 69
one DS512 controller module is in service, and one DS512 controller module has failed	step 68

68 Return the system-busy DS512 controller module to service using the procedure ”Clearing MAP alarms triggered by the SDM – APPL SDM minor” on page 4-3.

Go to step 74.

At the front of the SDM

69 Replace one DS512 controller module using the appropriate procedure in the “SDM hardware replacement procedures” chapter of this document.

Go to step 72.

Note: You can determine if a DS512 controller module is faulty by viewing the component out-of-service LED and the system in service LED. If the module is faulty, the component out-of-service LED is on (red), and the system in service LED (green) is off.

Clearing MAP alarms triggered by the SDM APPL SDM critical (end)

At the MAP display

70 The SDM state SysB, with no additional qualifier (NA or / not responding) indicates that the SDM is communicating successfully with the CM, but that all SDM applications have failed. Manually busy the SDM by typing

>BSY
and pressing the Enter key.

Response:

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

71 Return the SDM to service by typing

>RTS
and pressing the Enter key.

Response:

```
SDM RTS initiated.
SDM RTS completed.
```

72 Determine the state of the SDM.

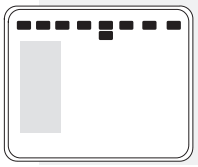
If the state of the SDM is	Do
InSv	step 74
SysB (NA)	step 73
SysB	step 73
SysB /The SDM is not responding	step 73
ISTb	step 13

73 Contact Nortel for assistance.

74 You have completed this procedure.

Clearing MAP alarms triggered by the SDM Ext FSP major

Application



CM	MS	IOD	Net	PM	CCS	Lns	Trks	**Ext FSP M**	APPL
.	.	.	.	.	.	.	.		.

Use this procedure to clear an EXT FSP major MAP alarm that has been triggered by the SDM.

Note: The EXT alarm FSP is used to report fault conditions on frame supervisory panels (FSP) and modular supervisory panels in various types of cabinets in a DMS switching. This procedure assumes that you have isolated the SDM as the cause of the FSP alarm. To clear an FSP alarm generated by another cabinet or frame, or by equipment other than the SDM, use the EXT FSP alarm clearing procedure in the generic alarm clearing manual for your DMS switch.

Indication

At the MTC level of the MAP display, FSP preceded by a number appears under the Ext header of the alarm banner and indicates an external FSP major alarm.

Meaning

An EXT FSP alarm triggered by the SDM means that one of the following faults has occurred:

- Input power to the SDM has failed.
- The SDM has shut down because it has reached its maximum allowable operating temperature threshold.
- The SDM power supply has failed.

Impact

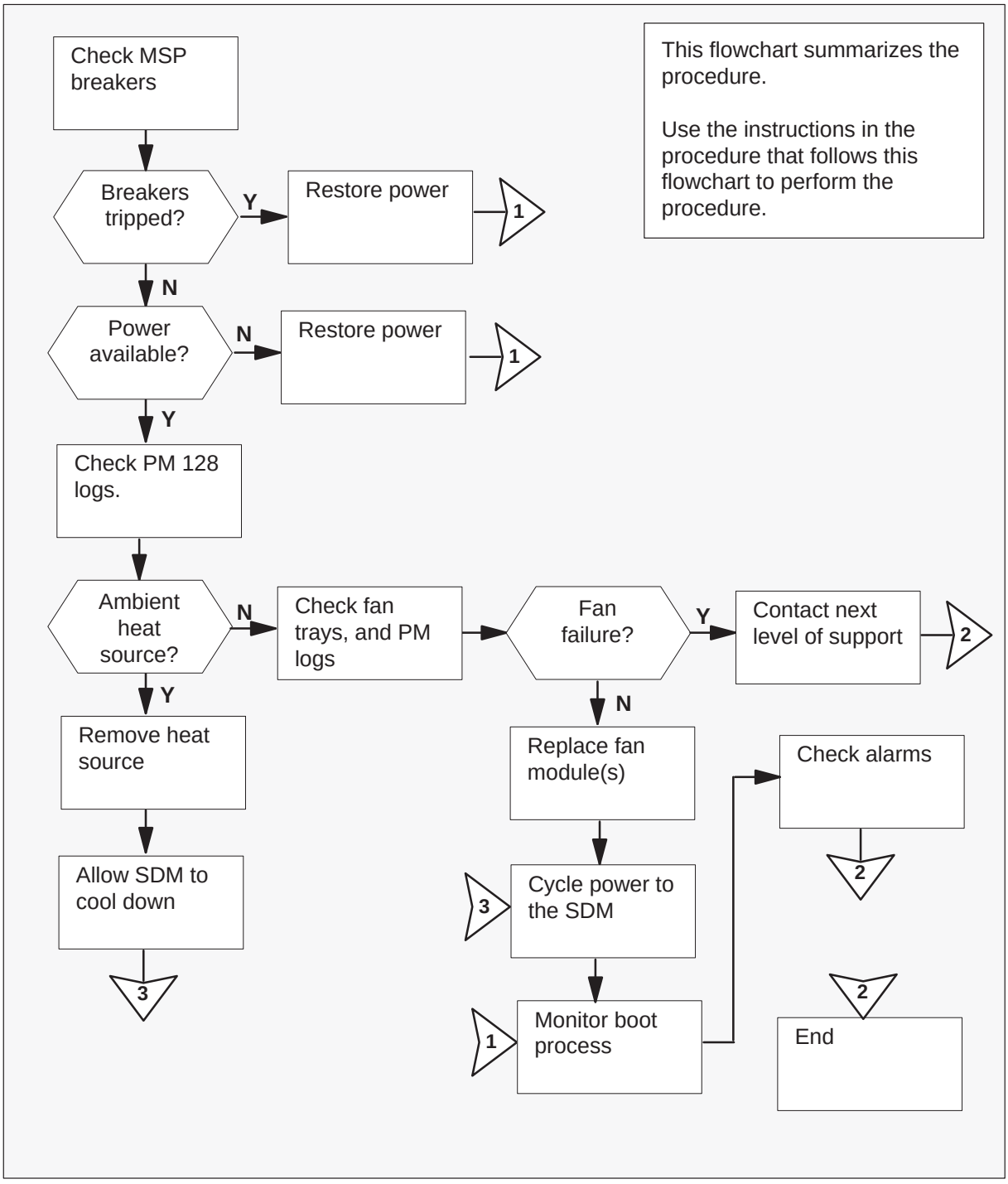
The SDM is out of service and no applications can run.

Action

The following flowchart is only a summary of the procedure. Use the instructions in the step-action procedure that follows the flowchart to clear the alarm.

Clearing MAP alarms triggered by the SDM Ext FSP major (continued)

Summary of Clearing MAP alarms triggered by the SDM - Ext FSP major



Clearing MAP alarms triggered by the SDM Ext FSP major (continued)

Clearing MAP alarms triggered by the SDM - Ext FSP major

At the MSP

1 Check the modular supervisory panel (MSP) breakers that supply -48V dv power to the SDM.

If the breakers have	Do
tripped	step 2
not tripped	step 3

2 The breakers have tripped due to an over-current condition. Have qualified maintenance personnel inspect the problem. If required, contact Nortel for assistance. When power is restored, continue this procedure at step 17.

Note: The MSP frame fail LED is lit when a breaker has tripped.

3 Have qualified power maintenance personnel determine if power is available from the MSP to the SDM.

If power to the SDM is	Do
available	step 5
not available	step 4

4 Have qualified power maintenance personnel restore power. Contact Nortel for assistance, if required. When power has been restored, continue this procedure at step 17.

At the local VT100 console

5 The SDM has shut down due to thermal failure (overheating). Verify this by checking for recent SDM-related PM128 logs. If the SDM shut down is due to thermal failure, then two logs were generated. The first log was generated when the SDM reached its thermal warning threshold (60° C or 140° F). The second log was generated to indicate that shutdown will occur in 1 min because its shutdown thermal threshold has been reached (80° C or 177° F)

At the C28B cabinet containing the SDM

6 Determine if an ambient heat source has caused the thermal shutdown.

Clearing MAP alarms triggered by the SDM Ext FSP major (continued)

Note: An ambient heat source may consist of an excessively high air temperature in the vicinity of the SDM, excessive heat from an adjacent frame, or a combination of these factors.

If	Do
an ambient heat source is present	step 14
the temperature in the vicinity of the SDM seems normal	step 7

At the front of the SDM

7 Verify that both fan trays are present, and fully seated in the main chassis.

At the local VT100 console

8 Check for recent SDM-related PM128 logs indicating failure of one or both fan tray units.

If a fan failure log is	Do
generated	step 13
not generated	step 9

9 Ensure that the local VT100 console is connected to the SDM with the designated cable, and that the VT100 console is operational.

At the MSP

10 Cycle power to the SDM by turning both MSP breakers, located at the front of the MSP, off and on. The MSP breakers supply power to the SDM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
contains a main and I/O expansion chassis	turn all four breakers off and on

Clearing MAP alarms triggered by the SDM Ext FSP major (continued)

At the local VT100 console

11 The SDM begins to reboot. Monitor the boot process. When you see the following prompt,

```
Self Test/Boots about to Begin... Press <BREAK> at any time to Abort ALL.
```

press the Break key repeatedly to interrupt the boot process. The FX-Bug prompt is then displayed.

At the front of the SDM

12 Check the operation of the three fans in each fan tray module by unseating the fan module, physically verifying that the fan blades in each fan are rotating, and then reseat the fan module.

If	Do
all fans appear to be operational	step 19
one or more fans is faulty	step 13

13 Replace the faulty fan module(s), and then continue this procedure at step 16.

At the C28B cabinet containing the SDM

14 Remove or eliminate the heat source that caused the thermal shutdown..

15 Allow the SDM to cool to ensure it has returned below its thermal shutdown warning threshold (60 degrees C or 140 degrees F).

At the MSP

16 Cycle power to the SDM by turning both MSP breakers, located at the front of the MSP, off and on. The MSP breakers supply power to the SDM. Proceed according to the chassis in your system.

If your system contains	Do
a main chassis only	turn top two breakers off and on
contains a main and I/O expansion chassis	turn all four breakers off and on

Clearing MAP alarms triggered by the SDM Ext FSP major (end)

At the SDM

17 When power is restored, the SDM automatically reboots and returns to service. Monitor the system's progress as follows:

- When the SDM has booted successfully, the System in Service LED turns on solid (green), and the Component Out of Service LED is on (red).
- Immediately following the reboot, all module in service LEDs are off, and out of service LEDs are on (red). As each module returns to service, its in service LED turns on (green) and the out of service LED turns off.
- When the CPU controller modules have returned to service, they begin to reintegrate. During this time (approximately 3 min), the System in Service LED flashes.
- When the I/O controller modules have returned to service, they begin to reintegrate and reestablish disk mirroring. During this time (10 to 30 min, depending on the amount of data stored on the disks), the System in Service LED flashes.

At the MAP display

18 When disk reintegration is complete, check the APPL alarm banner for SDM-related alarms. Use the alarm clearing procedures in this document to clear any faults.

Go to step 20.

19 Contact the personnel responsible for the next level of support.

20 You have completed this procedure.

Cleaning the SDM DAT drive

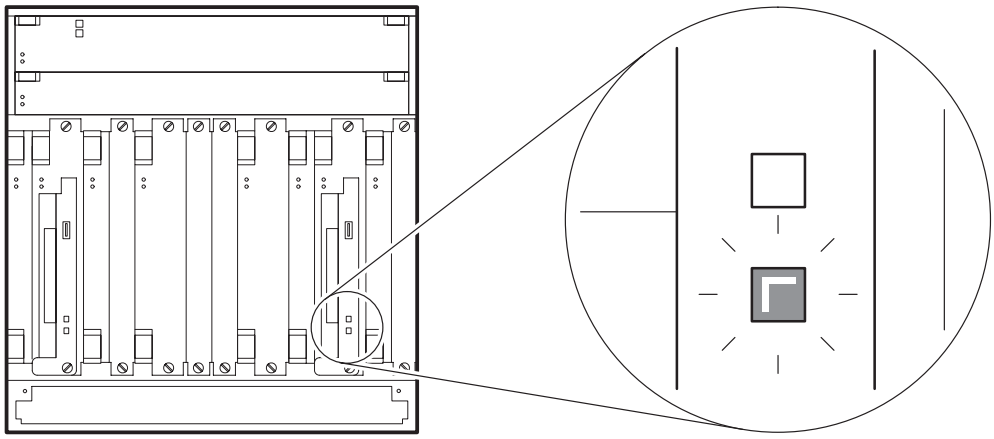
Application

Use this procedure to clean the digital audio tape (DAT) drive in an NTRX50FQ I/O controller module.

To clean the DAT drive, use an appropriate DAT drive cleaning cartridge. Nortel recommends the Maxell cleaning cartridge (part number HS–4/SL or equivalent). Refer to the documentation that accompanies the cleaning cartridge for additional information about its use, and the life expectancy of the cleaning tape.

Nortel recommends that you clean the tape drive heads after the first 4 hours of tape movement of a new cartridge, and then after each 25 hours of use.

A slowly flashing green LED may indicate that the tape is damaged or needs replacing. If the LED continues to flash after you have cleaned the DAT drive, then on replace the cleaning cartridge.



A solid green LED indicates that a tape is inserted with no errors. Slowly flashing green and amber LEDs indicates that a prerecorded audio cartridge is inserted and is being played automatically. A rapidly flashing green LED indicates that the drive cannot write to the tape correctly. Clean the DAT drive.

A solid amber LED indicates that the drive is reading or writing the tape. If the amber light flashes rapidly, a hardware fault has occurred.

Note: A flashing LED does not affect operations, and does not indicate that data has been lost.

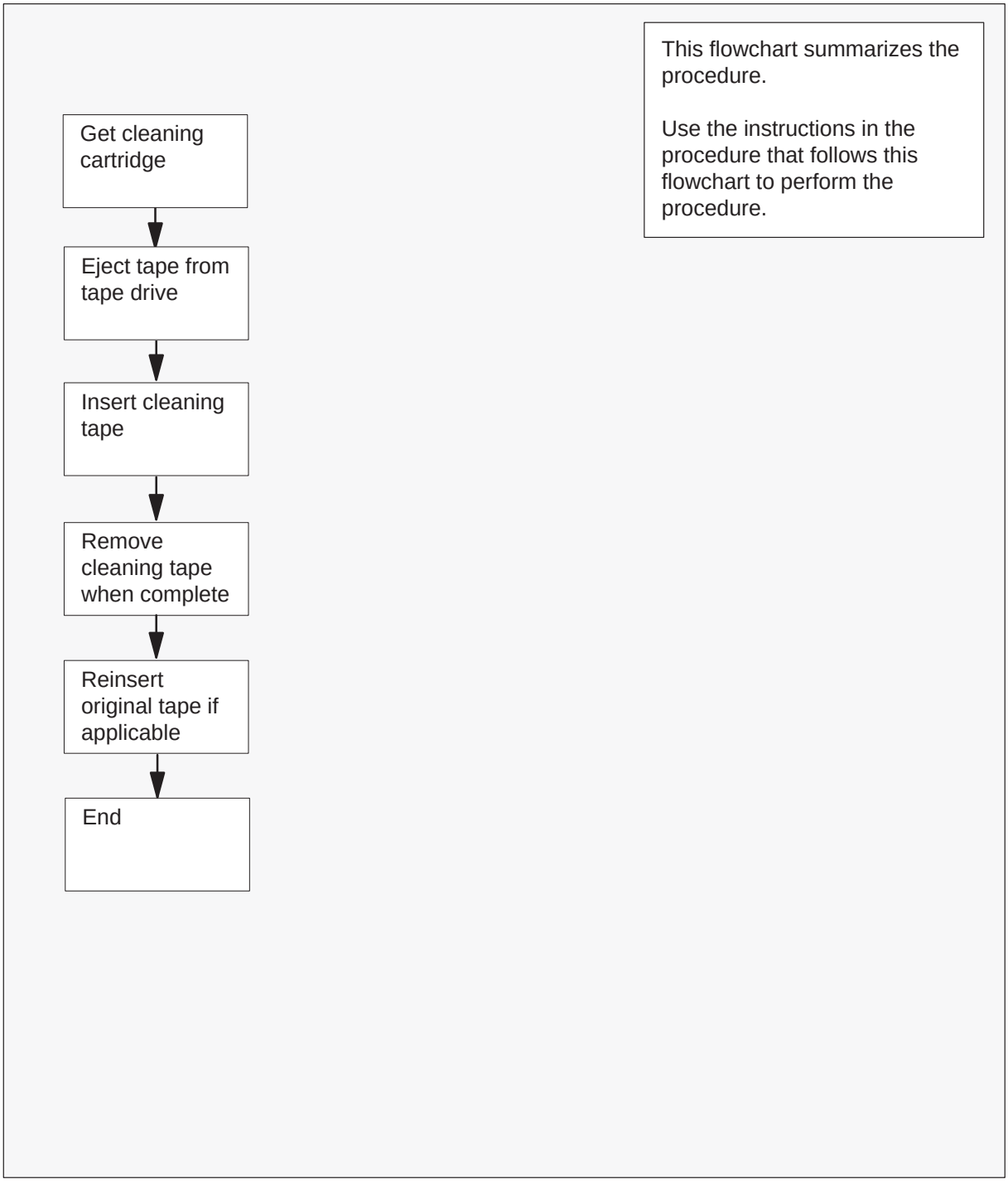
Cleaning the SDM DAT drive (continued)

Action

This procedure contains a summary flowchart as an overview of the procedure. Follow the specific steps to perform this procedure.

Cleaning the SDM DAT drive (continued)

Summary of Cleaning the SDM DAT drive



Cleaning the SDM DAT drive (end)

Cleaning the SDM DAT drive

At the front of the SDM

1 Obtain a cleaning cartridge (Maxell part number HS–4/CL or equivalent).

2 Press the eject button on the DAT drive and remove the tape cartridge, if applicable.

3 Insert the cleaning cartridge into the DAT drive.

Note: Cleaning begins automatically. When cleaning is complete, the cartridge is automatically ejected.

4 Remove the cartridge from the DAT drive.

5 If applicable, re-insert the tape you removed in step 2.

6 You have completed this procedure.

Controlling SDM applications

Application

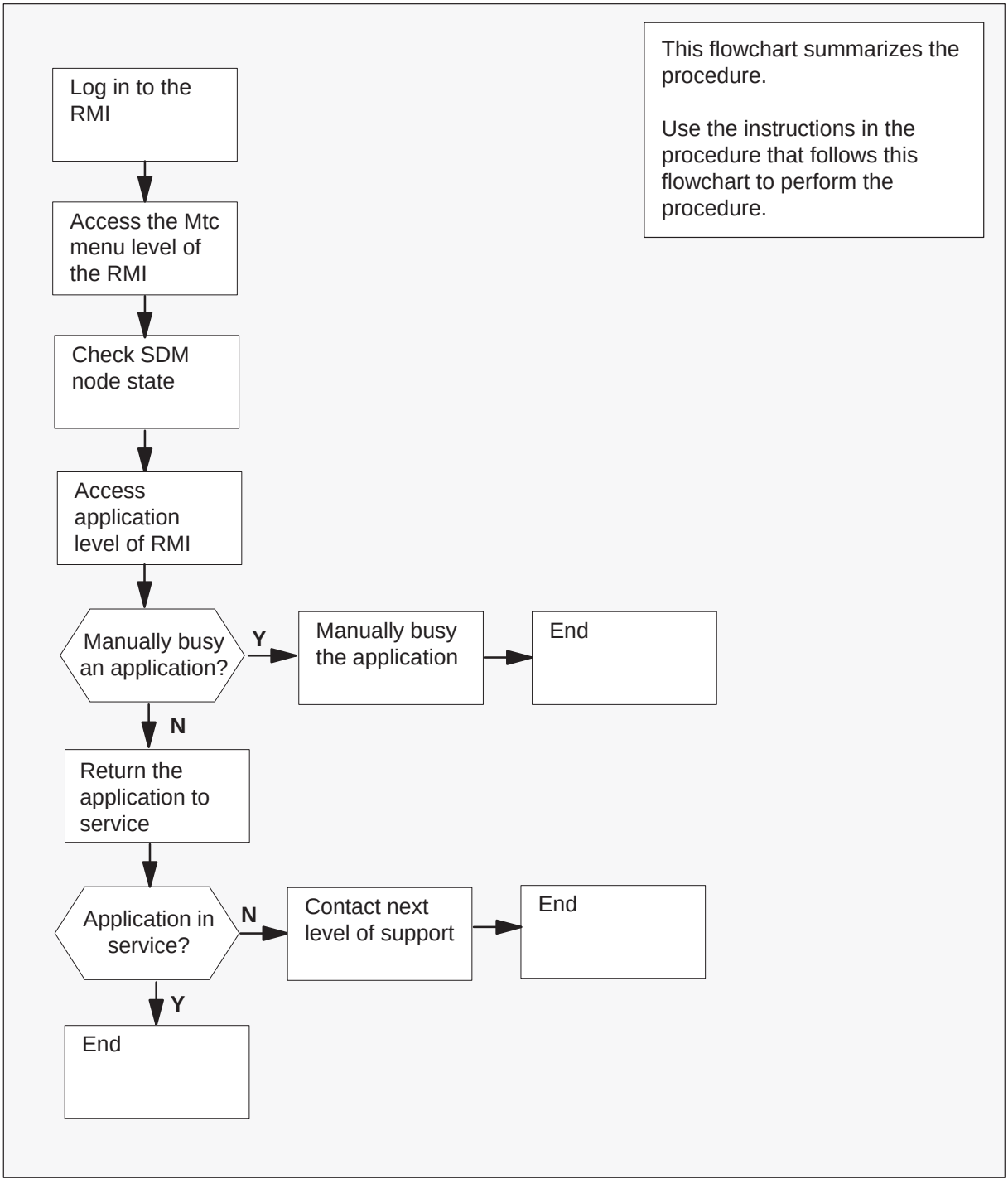
Use this procedure to shut down (manually busy) or restart (return to service) SDM application software packages. The SDM must be in in-service (InSv), in-service trouble (ISTb), or system busy (SysB) state to perform this procedure.

Action

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

Controlling SDM applications (continued)

Summary of Controlling SDM applications



Controlling SDM applications (continued)

Controlling SDM applications

At the local or remote VT100 terminal

1 Log in to the RMI as the root user or the maint user.

2 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

3 Access the maintenance (Mtc) menu level of the RMI by typing

>2
and pressing the Enter key.

4 Determine the SDM node state.

If the SDM node state is	Do
InSv, ISTb, or SysB	step 6
anything else	step 5

5 The SDM must be in InSv, ISTb, or SysB state to change the state of an SDM software package. Use the appropriate MAP alarm clearing procedure in this document to return the SDM to service.

Go to step 4.

6 Access the application (Appl) menu level of the RMI by typing

>4
and pressing the Enter key.

Example response:

```
SDM Node State:              ISTb
SDM Application State:       ISTb

 #  Package Description     Version    State
 1  Table Access Service    8.0.21.0   ISTb
 2  Operation Measurements  8.0.21.0   ISTb
 3  Log Delivery Service    8.0.21.0   InSv
```

Controlling SDM applications (continued)

7 Determine the application control activity you wish to perform.

If you want to	Do
shut down (manually busy) an SDM application software package	step 8
restart (return to service) an SDM application software package	step 11

8 Manually busy the application software by typing

>BSY n
and pressing the Enter key.

where

n is the number under "#" of the application you wish to shut down

Response:

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

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

9 Confirm the Busy command by typing

>Y
and pressing the Enter key.

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

Go to step 14.

Controlling SDM applications (end)

11 Return the application to service by typing

>RTS n

and pressing the Enter key.

where

n is the number of the application (from step 8)

Note: If the application is in the offline (OffL) state, it must be set to the manual-busy state as described in step 8 before entering the Bsy command.

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

12 Determine from the RMI display if the application returned to service successfully. This is indicated by the state InSv.

If the application state is	Do
InSv	step 14
anything else	step 13

13 Contact the personnel responsible for the next level of support.

14 You have completed this procedure.

Adding I/O controller modules

Application

Use this procedure to add the following hardware modules to the SDM:

- NTRX50FU – I/O controller module with two 2-Gbyte disk drives and Ethernet
- NTRX50GP – I/O controller module with two 4-Gbyte disk drives and Ethernet

To perform this procedure, you must know the following information:

- the chassis (SDMM for main chassis; SDME for I/O expansion chassis)
- the I/O controller module's slot number (from 1 to 16)
- the I/O controller module's product engineering code (PEC)

Note: I/O controller modules can be added to slots 4 and 5, and 15 and 16, of the SDM main chassis, and to unoccupied slots in the I/O expansion chassis.

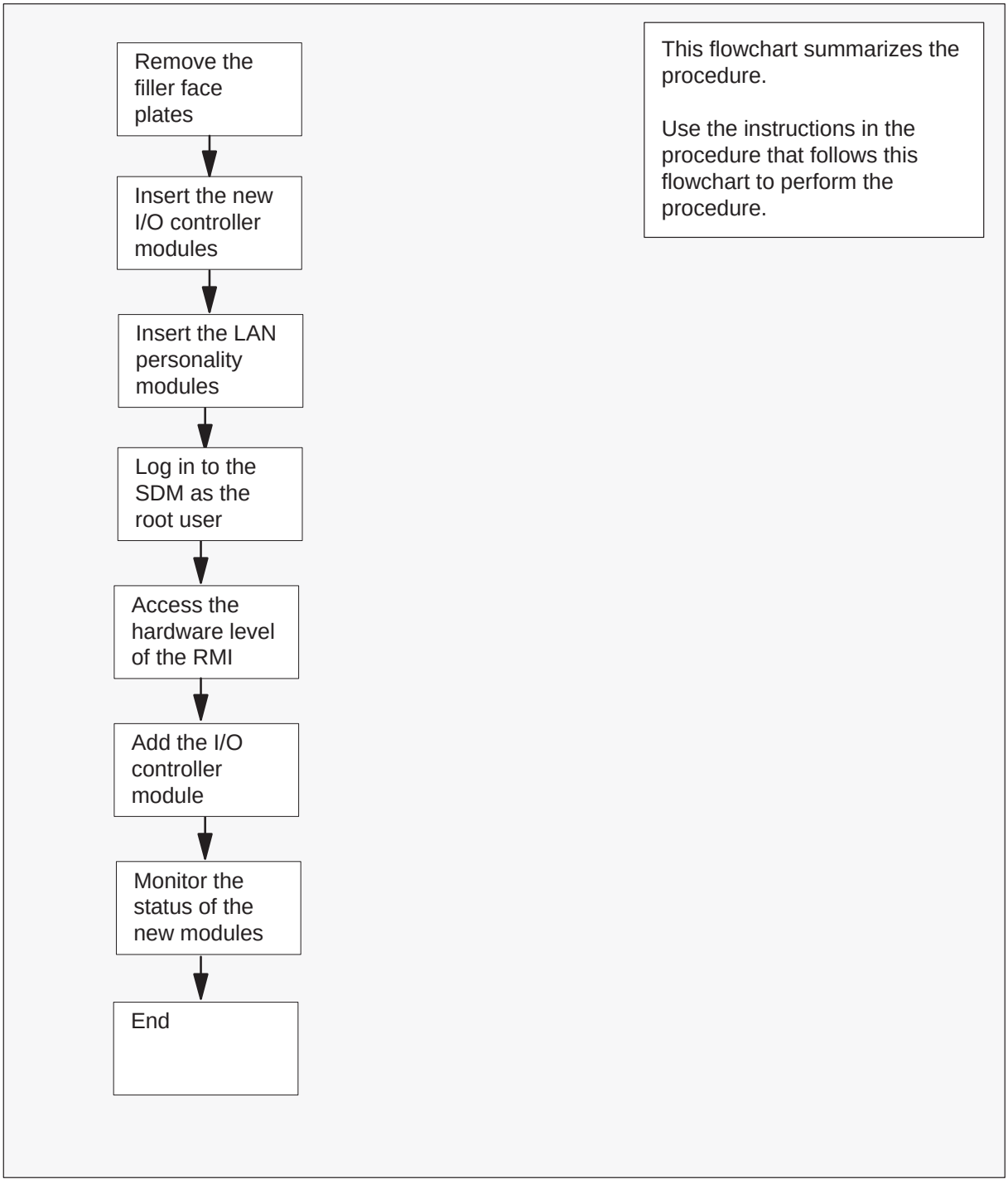
Note: Each I/O controller module must also have an associated LAN personality module (NTRX50FS) installed at the back of the SDM. Ethernet LAN connectivity, however, is only supported by the mandatory NTRX50FQ or NTRX50GN I/O controller modules located in slots 2 and 3, and 13 and 14, of the main chassis.

Action

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

Adding I/O controller modules (continued)

Summary of Adding I/O controller modules



Adding I/O controller modules (continued)

Adding I/O controller modules

At the front of the SDM

1

WARNING
Static electricity damage
Wear an ESD grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

2 Remove the filler plates covering the slots in which you will install the new modules.

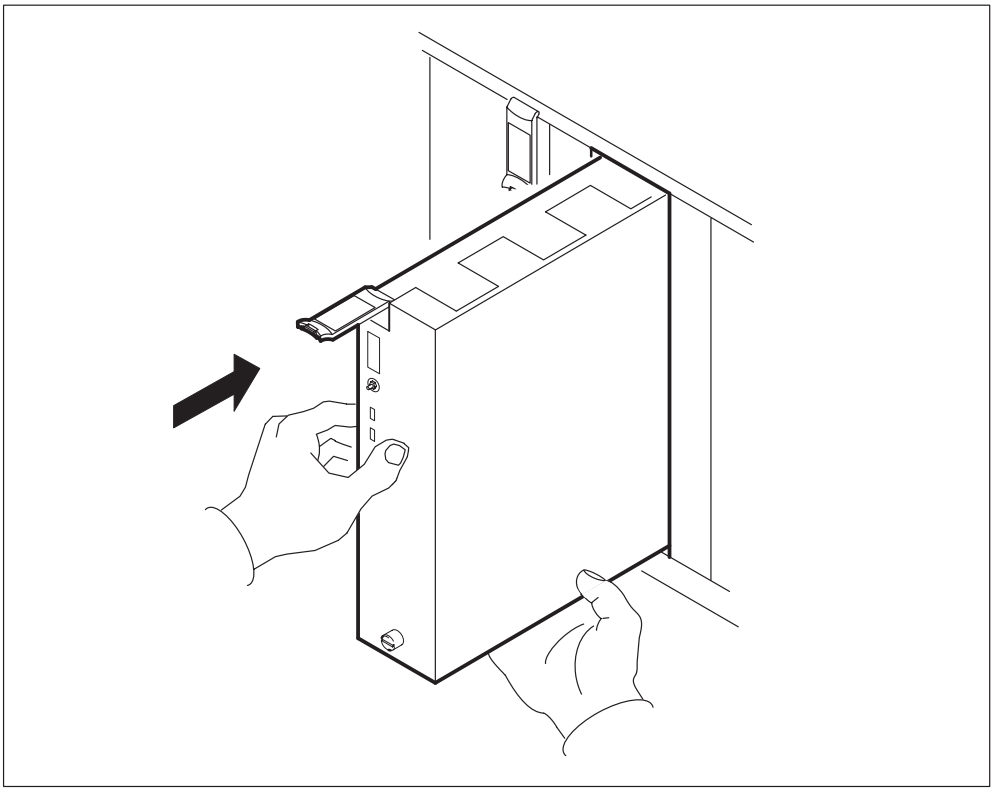
Note: I/O controller modules can be added to slots 4 and 5, and 15 and 16, of the SDM main chassis. All available slots can be used in the I/O expansion chassis to install two I/O controller modules as a logical pair, however, the left slot position of the left I/O controller module must be 8 slot positions apart from the left slot position of the right I/O controller module of the pair. For example, if the left I/O controller module of the pair occupies slots 1 and 2, the right I/O controller module must occupy slots 9 and 10. Both modules in a logical pair must have the same PEC.

Note: The rear LAN personality module (NTRX50FS) that is associated with each NTRX50FU and NTRX50GP I/O controller module must occupy the lower number of the two rear slots that are associated with the front module. For example, if the new I/O controller module occupies front slots 4 and 5, its associated NTRX50FS LAN personality module must be installed in rear slot 4. The unused rear slots remain covered by filler plates.

3 Insert the replacement module into the SDM shelf.

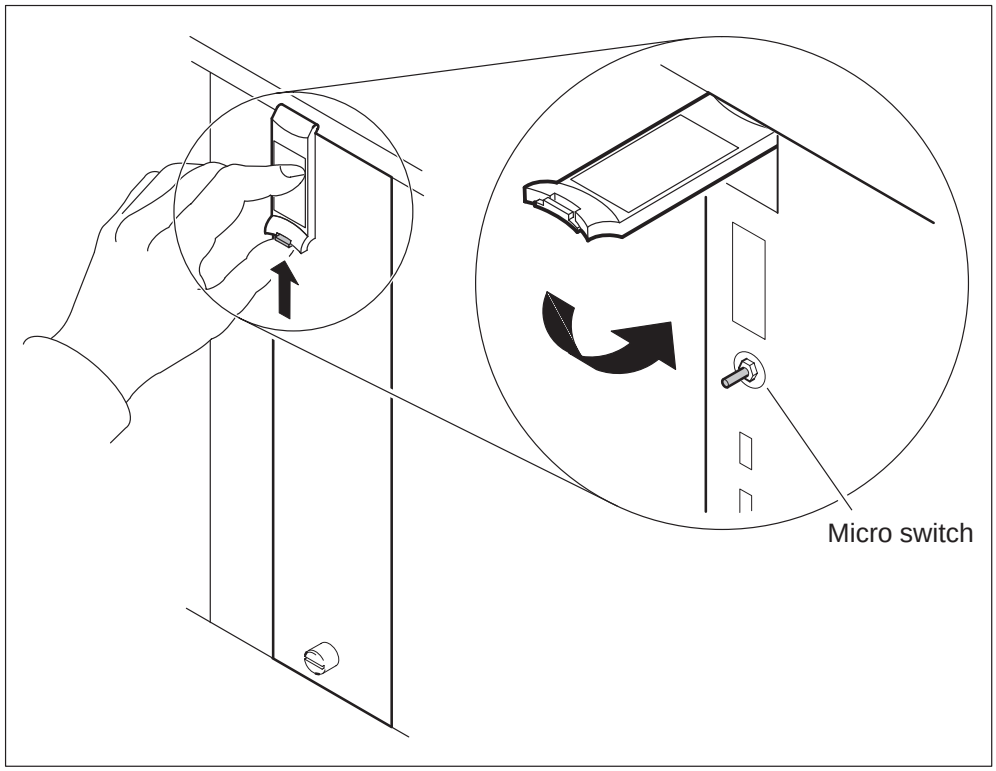
Adding I/O controller modules (continued)

4 Gently slide the module into the shelf until it is fully inserted.



Adding I/O controller modules (continued)

5 Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.



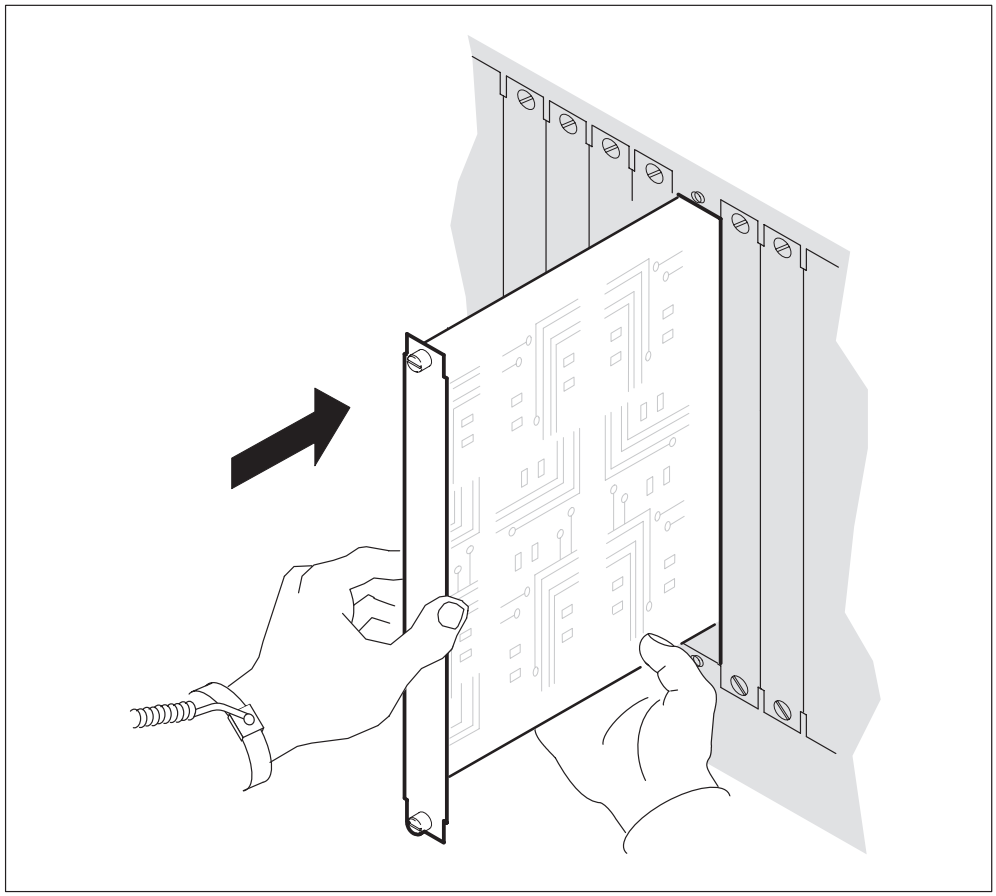
6 Tighten the thumbscrews on the module.

At the back of the SDM

7 Insert the new LAN personality module into the SDM shelf.

Adding I/O controller modules (continued)

8 Gently slide the LAN personality module into the shelf until it is fully inserted.



9 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

At the local or remote VT100 console

10 Log in to the SDM as the root user.

11 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

12 Access the hardware (Hw) menu level by typing

>HW
and pressing the Enter key.

Adding I/O controller modules (continued)

13 Add the logical pair of I/O controller modules by typing

>ADD chassis slot PEC
and pressing the Enter key.

where

chassis — is the chassis where the module will be located ("SDMM" for main chassis or "SDME" for I/O expansion chassis)
slot — is the lower of the two physical slot numbers the module occupies

Note: This command adds both modules in the logical pair simultaneously.

14 The ADD command may take several minutes to complete. When the command is finished, the following message is displayed:

Response:

```
Hardware Add Module – Command submitted.
```

15 Monitor the status of the new hardware at the hardware (Hw) menu level of the RMI. The screen does not initially show the new hardware that has been added.

Example response

```
          I F C E D 5
          C A P T S 1
          M N U H K 2

Domain 0  . . . . . .
Domain 1  . . . . . .
```

The system takes a few seconds to display the appropriate new hardware elements (DSKn for hard disks). Previously installed disks on the system are automatically renumbered, as required, to reflect the new hardware configuration. The status of the new hardware elements may initially appear on the RMI as "F" (failed).

Example response

```
          I F C E D D D D 5
          C A P T S S S A 1
          M N U H K K K T 2
                  1 2 3
Domain 0 . . . . . F F . .
Domain 1 . . . . . F F . .
```

Adding I/O controller modules (end)

After a few seconds, the modules are automatically put in service, at which time their status changes to in service (indicated by a dot).

Example response

```
          I F C E D D D D 5
          C A P T S S S A 1
          M N U H K K K T 2
                  1 2 3
Domain 0 . . . . . . . . .
Domain 1 . . . . . . . . .
```

Note: Devices have been renumbered. Use the Locate command to verify slot numbers.

16 You have completed this procedure.

Removing I/O controller modules

Application

Use this procedure to delete the following hardware modules from the SDM:

- NTRX50FU – I/O controller module with two 2-GByte disk drives and Ethernet
- NTRX50GP – I/O controller module with two 4-GByte disk drives and Ethernet

Note: This procedure can also be followed by the procedure ”Adding I/O controller modules” on page 4-64 to change or correct the physical location. The I/O controller modules (NTRX50FQ or NTRX50GN) in slots 2 and 3, and 13 and 14, of the main chassis are mandatory for system operation, and cannot be removed.

CAUTION

Re–using an I/O controller module

An I/O controller module must be manually busied and deleted before it can be re–used in a different slot.

To perform this procedure, you must know the following information:

- the chassis (SDMM for main chassis; SDME for I/O expansion chassis)
- the I/O controller module’s slot number (from 1 to 16)

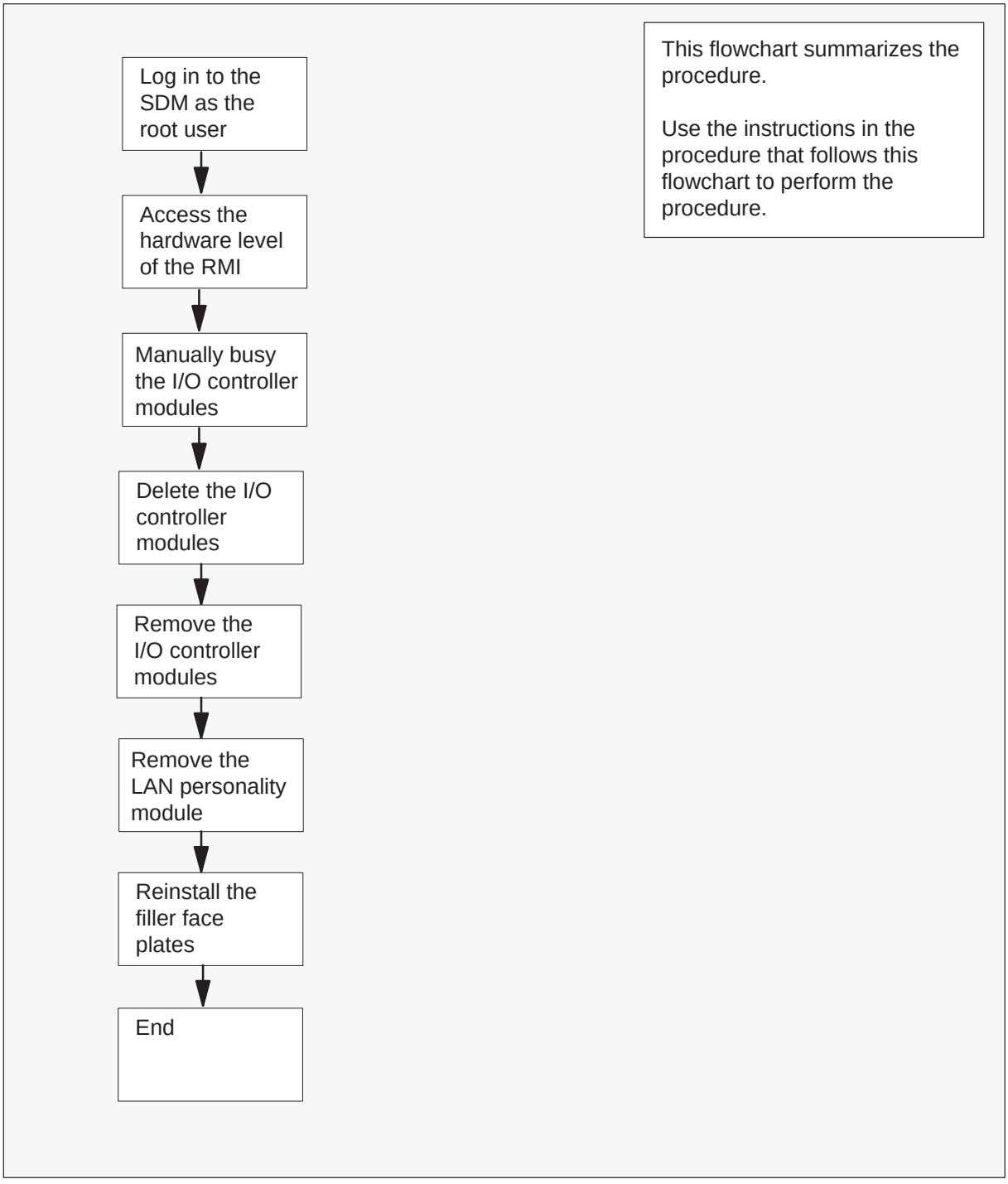
Note: Nortel recommends that you also remove I/O controller modules in pairs.

Action

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

Removing I/O controller modules (continued)

Summary of Removing I/O controller modules



Removing I/O controller modules (continued)

Removing I/O controller modules

At the local or remote VT100 console

1 Log in to the SDM as the root user.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the hardware (Hw) menu level by typing

>HW
and pressing the Enter key.

4 Determine the devices on the I/O controller module by using the Locate command. Use the Locate command by typing

>15
and pressing the Enter key.

5

CAUTION
Deleting an I/O controller module
Deleting an I/O controller module requires you to put the module in both domains in ManB state. These modules will not be in service.

Manually busy the module in each domain by typing

>BSY domain DSKn
and pressing the Enter key.

where

domain	is the domain (0 or 1) of the I/O controller module that you are replacing
n	is the disk number that you are replacing (Use the Locate command to determine the disk number of the module.)

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slots 4 and 5 of the main chassis,
- 1 if the module is located in slots 15 and 16 of the main chassis
- 0 if the module is located in any two slots from 1 to 8 in the I/O expansion chassis
- 1 if the module is located in any two slots from 9 to 16 of the I/O expansion chassis

Removing I/O controller modules (continued)

Example response:

```
Hardware Bsy – Domain 1 Device DSK2
Busying DSK2(1) will also busy DSK3(1).

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”):
```

6 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

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

Response:

```
Hardware Bsy – Command initiated.
Please wait...
```

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

Response:

```
Hardware Bsy – Command submitted.
```

If you have not yet manually busied the module in both domains, go to step 5. Otherwise, continue this procedure.

Note: After you see the response to the Bsy command, the I/O controller module’s state changes to “M” at the hardware menu level of the RMI.

8 Use the Locate command to determine the chassis and slot number of the module you wish to delete by typing

>15
and pressing the Enter key.

Example response:

```
Site  Flr  RPos Bay_id Shf Description    Slot EQPEC
HOST  00     00 CSDM  SDME DSK2(0),DSK3(0)   02 NTRX50FU FRNT
```

Note: The example shown only displays part of the information generated from the Locate command. Press the Enter key to scroll through the display.

9 Delete the module by typing

>DELchassis slot
and pressing the Enter key.

where

chassis — is the chassis where the module is located (SDMM for the main chassis or SDME for the I/O expansion chassis)
slot — is the slot number (from 1 to 16) where the module is located

Removing I/O controller modules (continued)

Note 1: The module in the corresponding slot of the other domain will also be deleted.

Note 2: In the example response shown in step 8, type DEL SDME 2.

Example response

```
Module in slot 4 of SDMM will be deleted.
DSK2(0), DSK3(0) will be deleted.
Module in slot 15 of SDMM will also be deleted.

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", "N"):
```

10 If you are sure this is the module you wish to delete, type

>Y
and press the Enter key.

11 The DEL command may take several minutes to complete. When the command is finished, the following message is displayed:

Response:

```
Hardware Del Module – Command submitted.
```

12 In a few seconds, the module disappears from the listing shown at the hardware menu level of the RMI.

Note: The device numbers change on the screen display.

At the front of the SDM

13

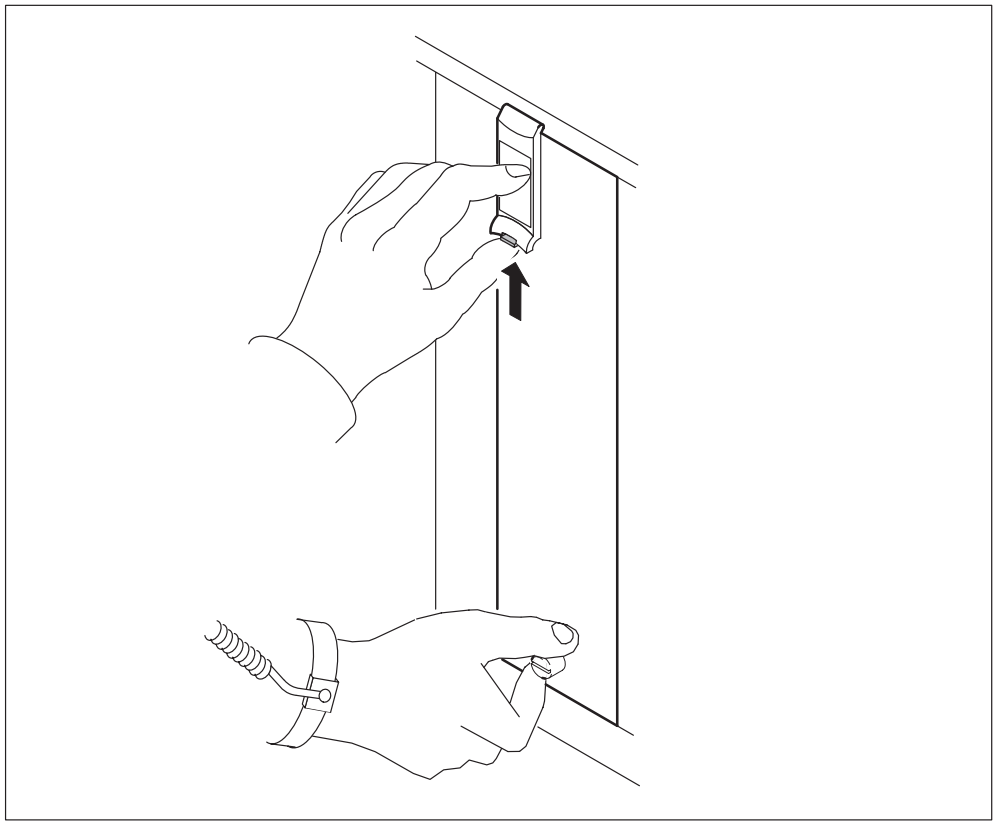
WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

14 Undo the thumbscrews located on the top and the bottom of the I/O controller module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

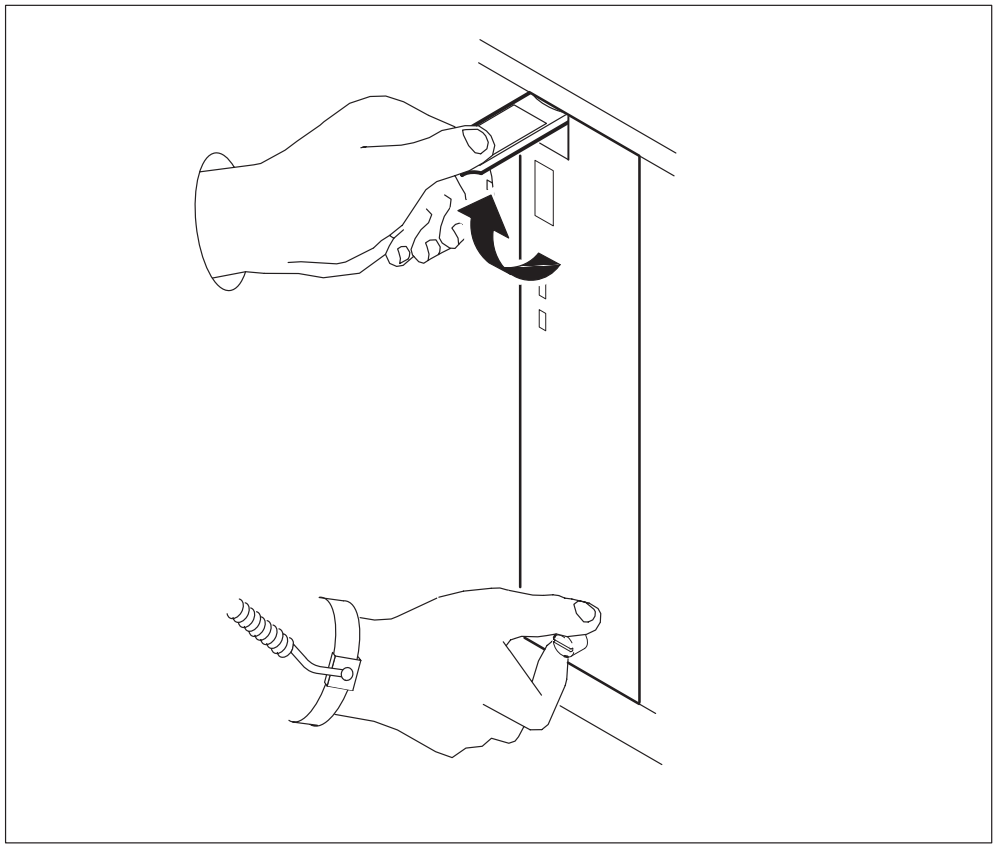
Removing I/O controller modules (continued)

15 Depress the tip of the locking lever on the face of the I/O controller module.



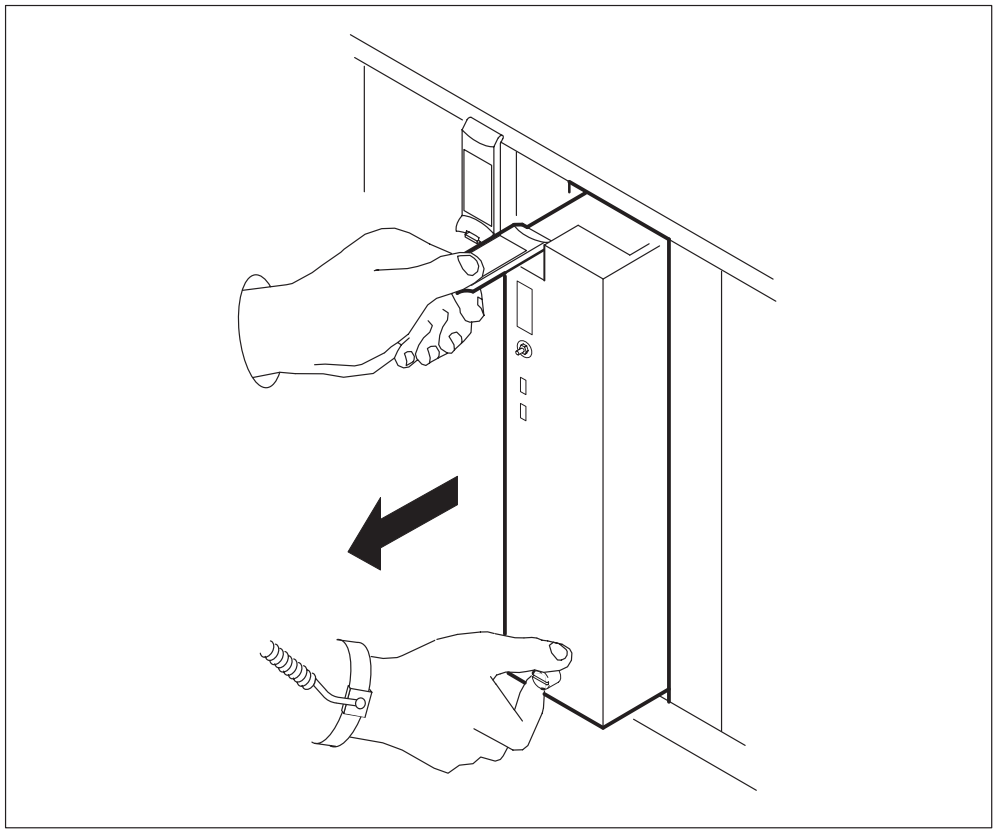
Removing I/O controller modules (continued)

16 Open the locking lever on the face of the module by moving the lever outwards.



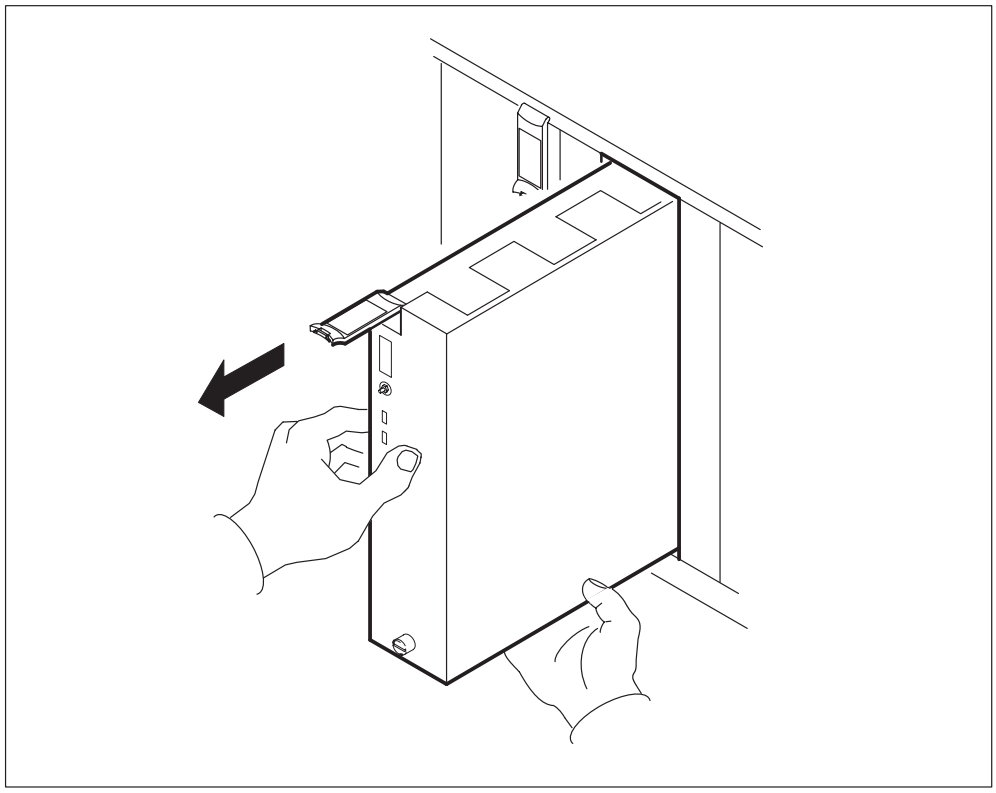
Removing I/O controller modules (continued)

17 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in (5.1 cm) from the SDM shelf.



Removing I/O controller modules (continued)

18 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



19 Place the module you have removed in an ESD protective container.

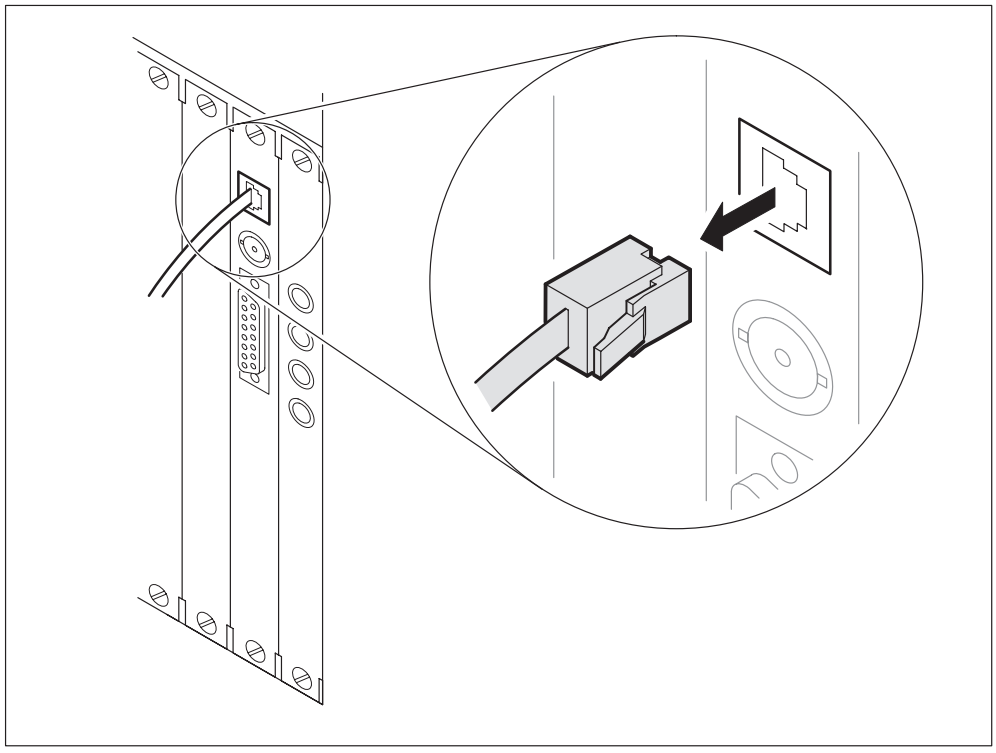
Removing I/O controller modules (continued)

At the back of the SDM

20 Determine what kind of hardware module your SDM has.

If you have	Do
NTRS50FQ or NTRX50GN	step 21
NTRX50FU or NTRX50GP	step 22

21 Disconnect the 10BASE-T cable from the corresponding LAN personality module, as shown in the following diagram.

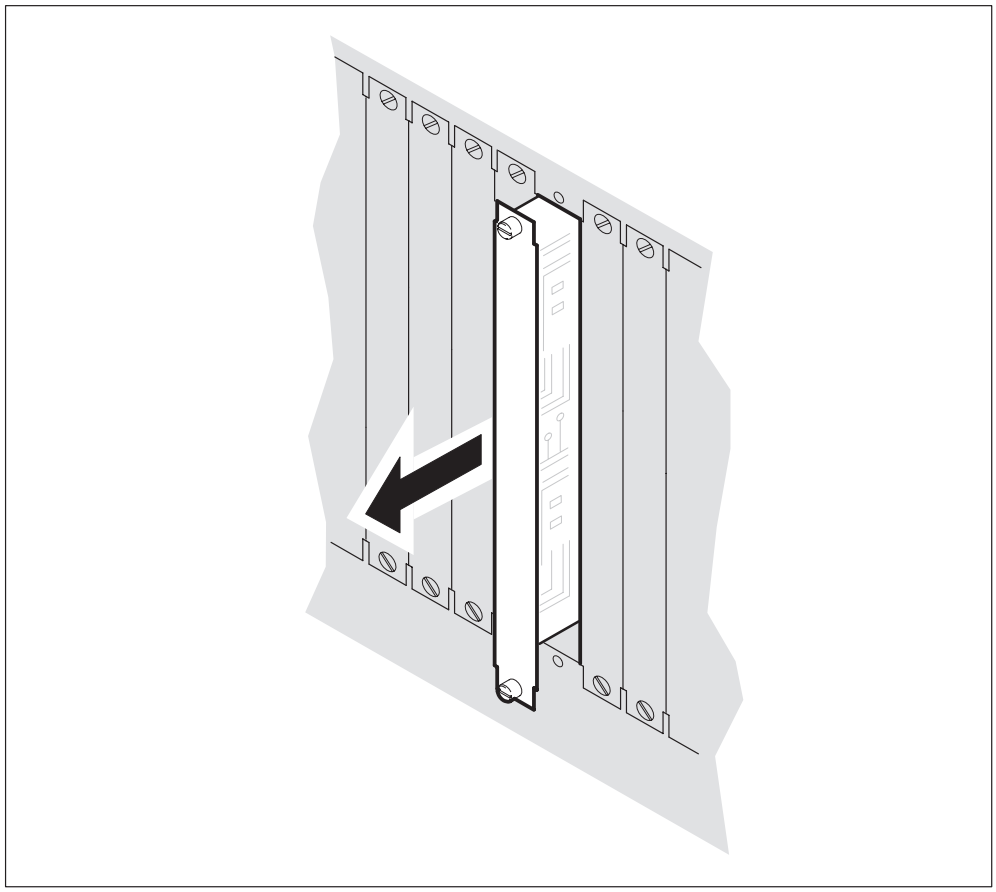


22 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

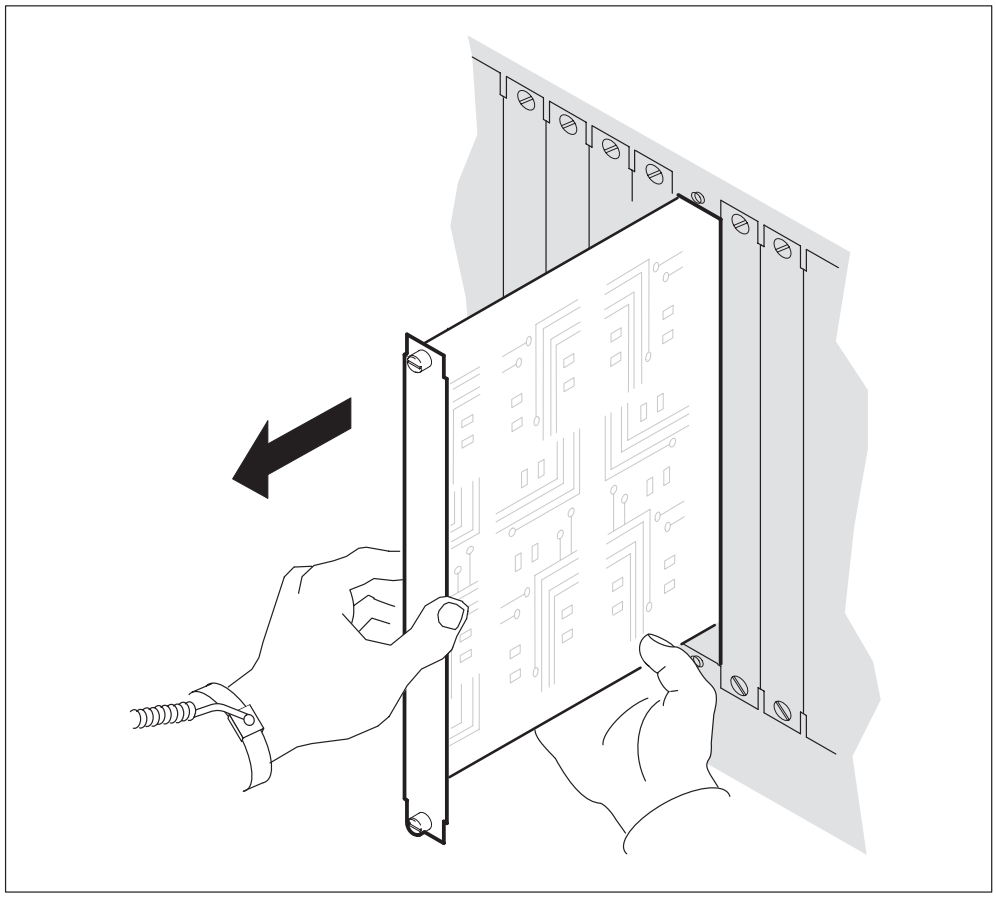
Removing I/O controller modules (continued)

23 While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in (5.1 cm) from the SDM shelf.



Removing I/O controller modules (end)

24 Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.



25 Place the LAN personality module you have removed in an ESD protective container.

26 Reinstall the filler plates covering the slots in which you removed the modules.

27 You have completed this procedure.

Establishing a modem connection

Application

Nortel recommends that you use the General DataComm (GDC) maintenance modem provided with the SDM equipment whenever a console dial-up modem connection to the SDM from a remote location is required. The GDC maintenance modem is installed and configured as part of the installation of the SDM.

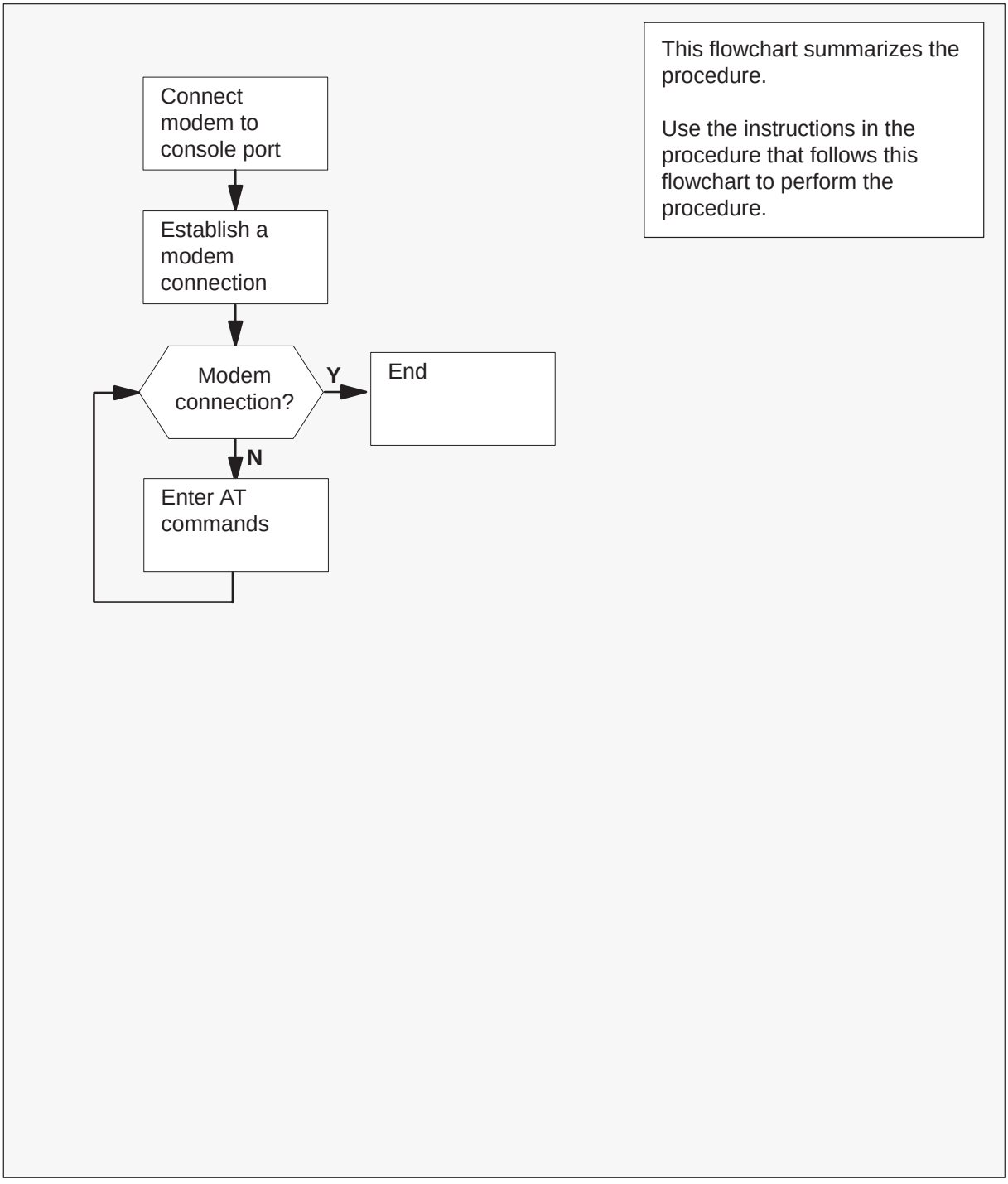
Use the following procedure to establish a dial-up modem connection to the SDM from a remote location.

Action

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

Establishing a modem connection (continued)

Summary of Establishing a modem connection



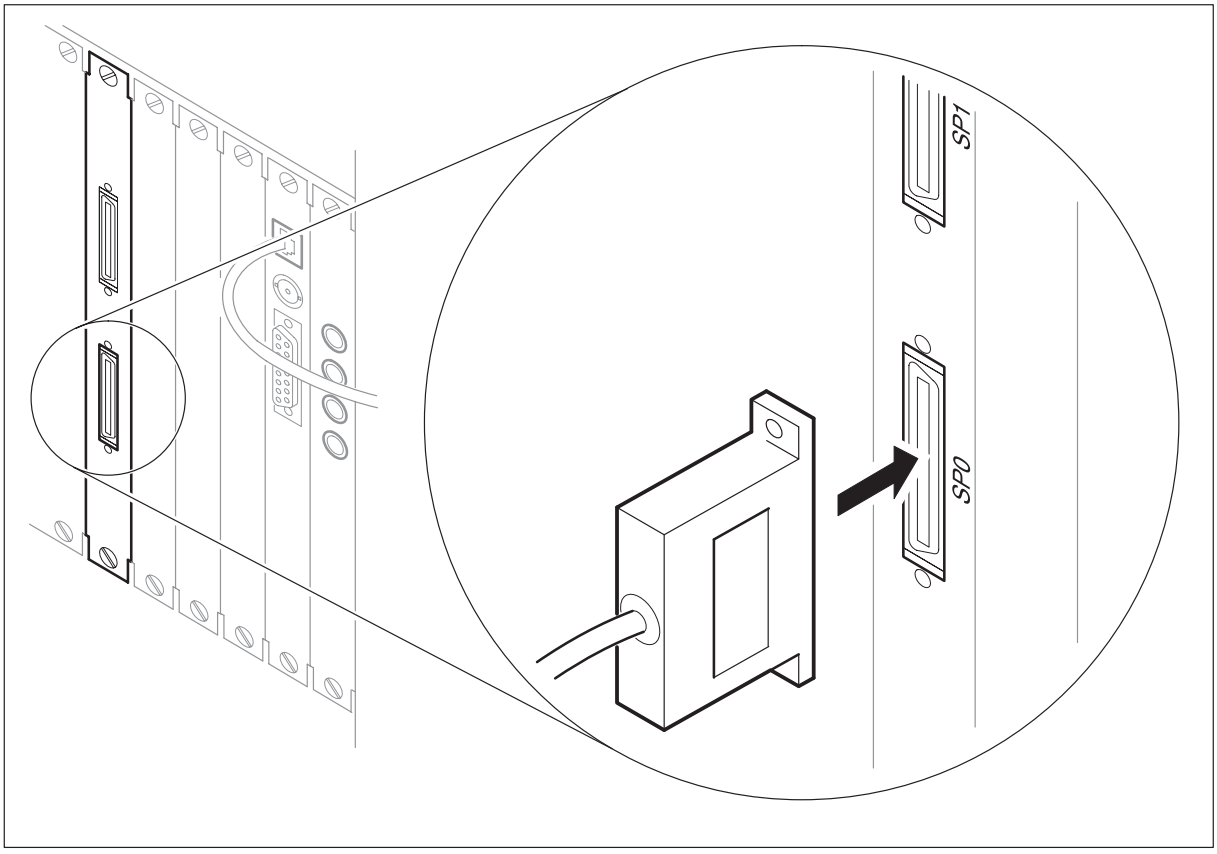
Establishing a modem connection (continued)

Establishing a modem connection

At the SDM

1 If necessary, connect the GDC maintenance modem to the SDM by first ensuring no other terminal device cables are connected to console port SP0 on the CPU personality module. Connect the NTRX5093 cable connected to the GDC maintenance modem to port SP0, and ensure a phone line is connected to the GDC maintenance modem.

Note: The modem is located in the appropriate MIS frame.



Establishing a modem connection (continued)

At a remote VT100 console

2 Use a terminal connected to a V.34 Hayes-compatible modem or other appropriate communications equipment connected to a V.34 modem, to establish remote connection to the SDM console port. Establish a modem connection to the SDM by typing

>atdt dial_in_number
and pressing the Enter key.

where

dial_in_number — is the telephone number for the modem attached to serial port 1

Note: For information on establishing a modem-to-modem connection, refer to the instructions for establishing a dial-up connection provided with the communications equipment you are using.

3 Determine if the connection has been established.

If you	Do
get a login prompt	step 4
do not get a login prompt	step 5

4 Log in at the prompt using your userID and password.

Go to step 15.

5 Execute the following steps to reconfigure your modem, starting at step 6. If you have already executed these commands, and are still having problems, contact the personnel responsible for your next level of support.

6 Reconfigure the GDC maintenance modem by connecting a VT100 console set to communicate at 9600 baud directly to the DTE connector on the GDC maintenance modem. Then enter the AT commands by first typing

>AT&F0
and pressing the Enter key.

Note: The command may or may not be echoed on the screen, depending on the previous configuration.

Note: If you make a mistake when entering the AT commands, restart the procedure at this point.

7 When the modem responds “OK”, type

>AT\T7
and press the Enter key.

Establishing a modem connection (end)

8 When the modem responds “OK”, type

>AT&R2
and press the Enter key.

9 When the modem responds “OK”, type

>AT&C1
and press the Enter key.

10 When the modem responds “OK”, type

>ATE0
and press the Enter key.

11 When the modem responds “OK”, type

>AT%K1
and press the Enter key.

Note: This command is not echoed on the screen.

12 When the modem responds “OK”, type

>ATQ1
and press the Enter key.

Note: The modem does not respond after you enter ATQ1. The command is not echoed on the screen.

13 Type

>AT&W0
and press the Enter key.

Note: The modem does not respond after you enter AT&W0. The command is not echoed on the screen.

14 Type

>AT&Y0
and press the Enter key.

Note: The modem does not respond after you enter AT&Y0. The command is not echoed on the screen.

Go to step 2.

15 You have completed this procedure.

Commissioning SDM-LAN connectivity

Application

Use this procedure to commission SDM to local area network (LAN) connectivity.

Note: This procedure does not include Distributed Computing Environment (DCE) commissioning. You must perform this procedure ("Commissioning SDM-LAN connectivity") before commissioning DCE. For information on commissioning DCE, refer to the procedure "Configuring an SDM in a DCE cell" on page 6-97 in the "SDM system administration procedures" chapter in this document.

To commission LAN nodes, see the procedure "Commissioning LAN nodes" on page 4-95.

To commission LAN connectivity, you must know the following:

- SDM hostname
- SDM LAN Internet protocol (IP) address
- SDM LAN netmask
- SDM LAN type (this is required at initial commissioning only and cannot be changed at the remote maintenance interface (RMI)
- SDM LAN gateway IP address (if a gateway is required)

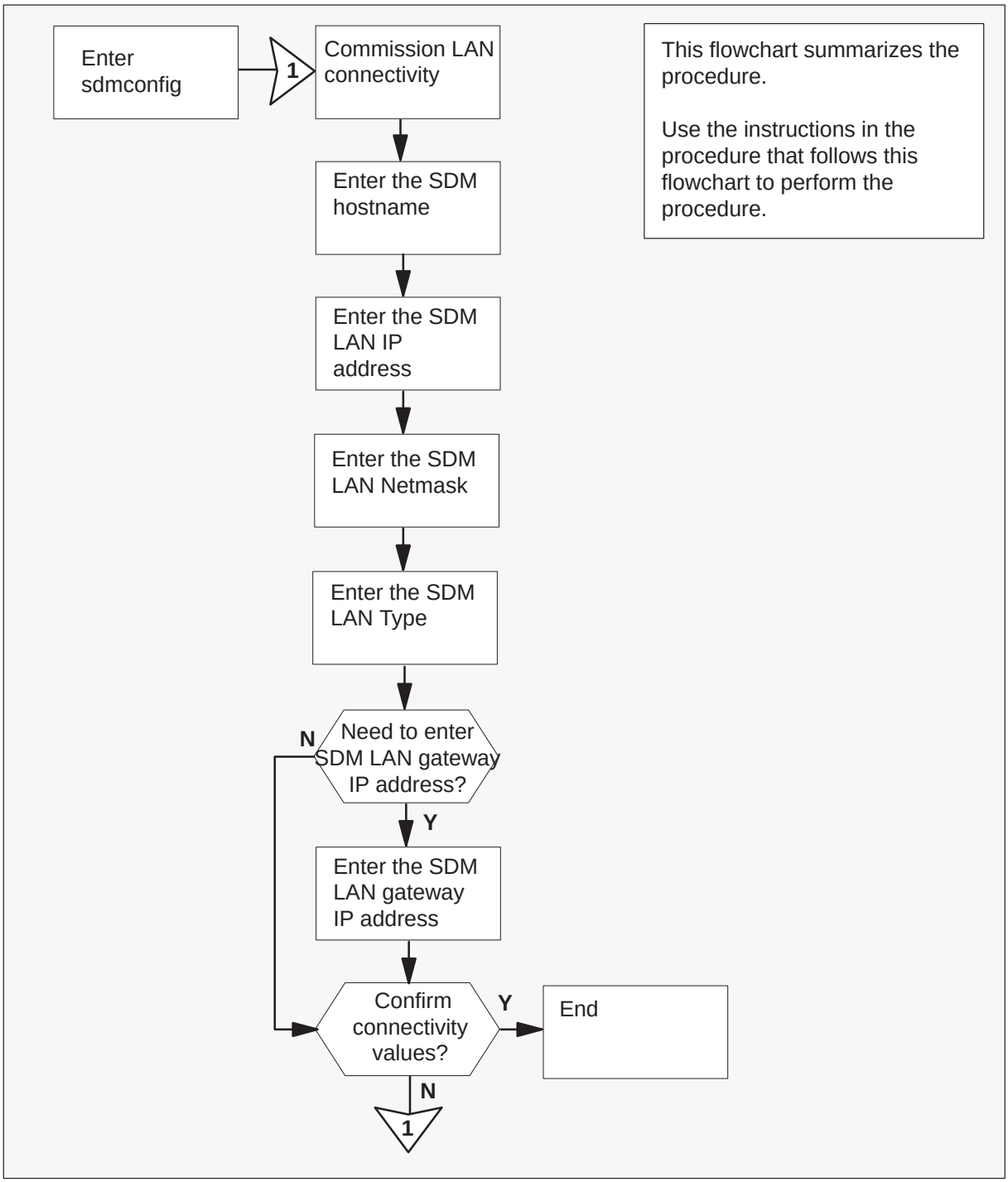
Note: After initial commissioning, the values for SDM hostname, LAN IP address, LAN netmask, and gateway IP address can be changed at the RMI. SDM LAN type cannot be changed at the RMI.

Action

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

Commissioning SDM-LAN connectivity (continued)

Summary of Commissioning SDM-LAN connectivity



Commissioning SDM-LAN connectivity (continued)

Commissioning LAN connectivity

At the local VT100 console

1 Begin SDM-LAN commissioning by typing

 # sdmconfig
and pressing the Enter key. The screen displays the information that you need to commission the LAN, if LAN commissioning has not been completed.

Response:

```
                              SDM COMMISSIONING

LAN CONNECTIVITY

You will be prompted for the following information:

– SDM Hostname
– SDM LAN IP Address
– SDM LAN Netmask
– SDM LAN Type
– SDM LAN Gateway (OPTIONAL)

Do you wish to proceed with LAN connectivity
commissioning? [YES]
```

2 Proceed with LAN connectivity commissioning by pressing the Enter key.

Response:

```
Please enter the SDM hostname:
```

3 Enter the SDM hostname by typing

>hostname
and pressing the Enter key.

where

hostname	is the SDM hostname to which you are commissioning LAN connectivity

Response:

```
Please enter the SDM IP Address:
```

Commissioning SDM-LAN connectivity (continued)

4 Enter the SDM LAN IP address by typing

>LAN IP address
and pressing the Enter key.

where

LAN IP address — is the IP address of the LAN that you are commissioning

Response:

```
Please enter the SDM LAN Netmask:
```

5 Enter the SDM LAN netmask by typing

>LAN netmask
and pressing the Enter key.

where

LAN netmask — is the LAN netmask of the LAN that you are commissioning

Response:

```
Please enter the SDM LAN Gateway IP: [No Gateway]
```

6 Enter the SDM LAN type by typing

>LAN type
and pressing the Enter key.

where

LAN type — is the LAN type of the LAN that you are commissioning

Response:

```
Please select the LAN Type, either (S)tandard or (I)EEE 802.3:[Standard]
```

Note: Standard is the default SDM to LAN connection. Once you choose an SDM to LAN connection, you cannot change it without re-installing the operating system. All information will be lost and the SDM will need to be commissioned from the beginning. Any applications installed on the SDM will be lost and need to be reinstalled and configured.

7 Proceed according to whether you are entering the SDM LAN Gateway IP address.

If you are	Do
entering the SDM LAN gateway IP address	step 8
not entering the SDM LAN gateway IP address	step 9

Commissioning SDM-LAN connectivity (continued)

8 Enter the SDM LAN gateway IP address by typing

>gateway IP address
and pressing the Enter key.

where

gateway IP address	is the SDM LAN gateway IP address of the LAN you that you are commissioning

Go to step 10.

9 If you do not wish to enter a SDM LAN gateway IP address, press the Enter key.

10 Determine whether you want to confirm the LAN commissioning values you have entered.

Example response:

```
                                SDM COMMISSIONING

LAN CONNECTIVITY

The following values have been entered:

SDM Hostname:          bnode75
SDM LAN IP Address:    47.105.144.29
SDM LAN Netmask:       255.255.240.0
SDM LAN Type:          Standard
SDM LAN Gateway:       47.105.144.1
Are these values correct? [YES]
```

If you are	Do
confirming the LAN commissioning values	step 11
not confirming the LAN commissioning values	step 12

11 If the LAN connectivity values are correct, press the Enter key.

Response:

```
Commissioning LAN Connection – PASSED

HIT ENTER TO CONTINUE
```

Note: If you get the response that commissioning of the LAN nodes failed, go to step 15.

Go to step 16.

Commissioning SDM-LAN connectivity (end)

12 If the values are incorrect, reject the LAN commissioning values you have entered by typing

>NO

and pressing the Enter key.

Response:

```
LAN CONNECTIVITY
– SDM Hostname
– SDM LAN IP Address
– SDM LAN Netmask
– SDM LAN Type
– SDM LAN Gateway (OPTIONAL)

Do you wish to proceed with LAN connectivity commissioning? [YES]
```

13 Decide if you want to proceed with LAN connectivity commissioning.

If you	Do
want to proceed with LAN connectivity commissioning	step 14
do not want to proceed with LAN connectivity commissioning	step 16

14 Return to step 2 and reenter the LAN commissioning values.

15 Contact your next level of support.

16 You have completed this procedure.

Commissioning LAN nodes

Application

Use this procedure to commission local area network (LAN) nodes. A maximum of four LAN nodes can be commissioned.

To commission LAN nodes, you must know the following:

- the description of each LAN node
- the hostname of each LAN node
- the Internet protocol (IP) address of each LAN node

Note 1: This procedure does not include commissioning SDM-LAN connectivity. You must perform the procedure "Commissioning SDM-LAN connectivity" on page 4-89 before you commission LAN nodes.

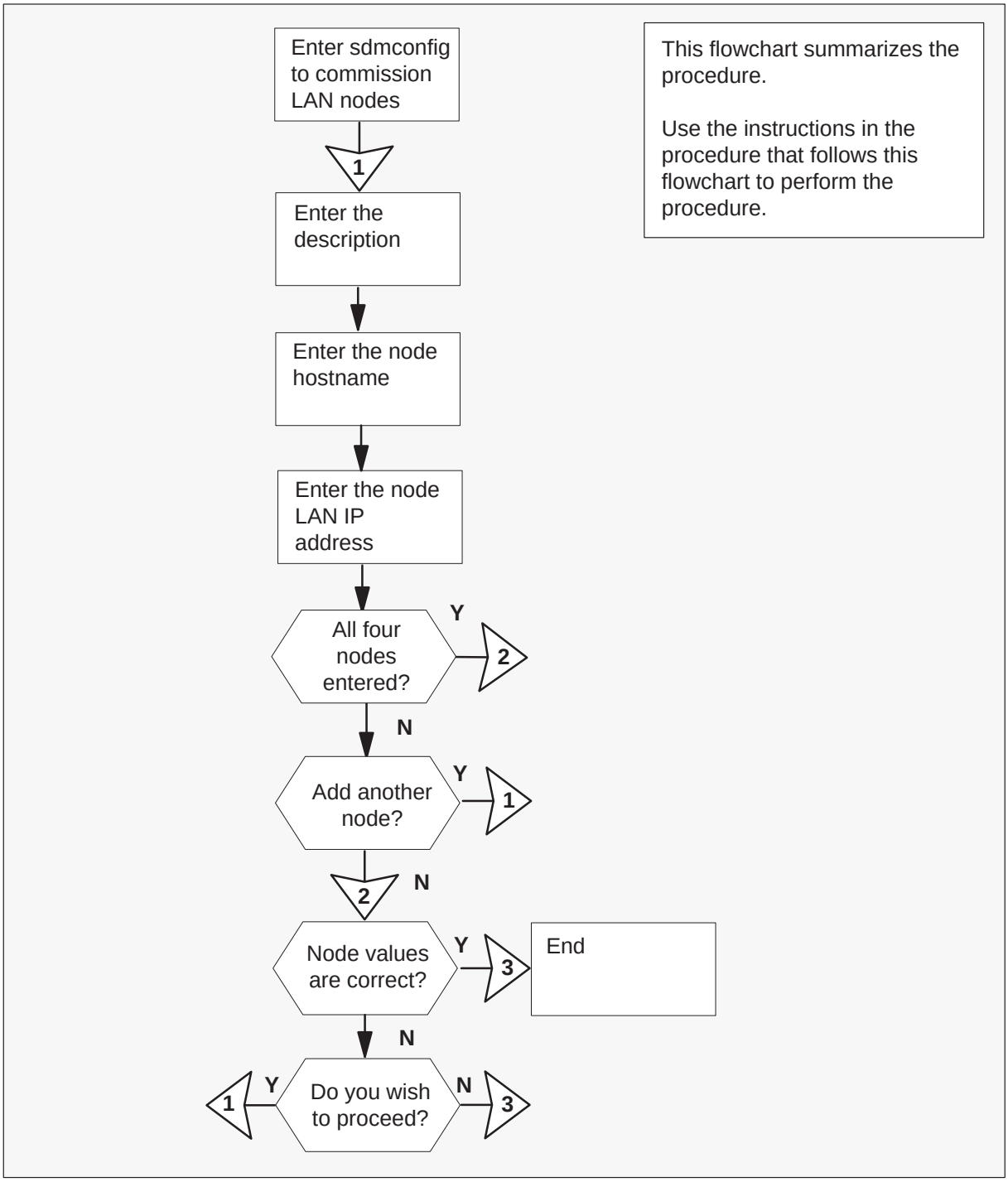
Note 2: LAN nodes can also be defined at the remote maintenance interface (RMI). See page 2-56 for more information.

Action

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

Commissioning LAN nodes (continued)

Summary of Commissioning LAN nodes



Commissioning LAN nodes (continued)

Commissioning LAN nodes

At the local VT100 console

1 Begin commissioning LAN nodes by typing

 # sdmconfig
and pressing the Enter key.

Note: If LAN commissioning has not been completed, the screen displays the information that you need to commission the LAN. Perform the procedure "Commissioning SDM-LAN connectivity" on page 4-89, before completing this procedure.

Response:

```
                                SDM COMMISSIONING

LAN NODES

You will be prompted for the following information:

– the Description for 1-4 LAN Nodes
– the Hostname for 1-4 LAN Nodes
– the IP Address for 1-4 LAN Nodes

Do you wish to proceed with LAN Node commissioning? [YES]
```

2 Press the Enter key to proceed with LAN node commissioning.

Example response:

```
Please enter the Description for LAN Node 1:
```

Note: In the preceding example response, the LAN node number is 1. This value can be 1 to 4 depending on what LAN node number you are commissioning. You can commission a maximum of four LAN nodes.

3 Enter the description for the LAN node by typing

>node
and pressing the Enter key.

where

node is the description for the LAN node.

Example response:

```
Please enter the Hostname for LAN Node 1:
```

Commissioning LAN nodes (continued)

4 Enter the hostname for the LAN node by typing

>hostname
and pressing the Enter key.

where

hostname is the hostname for the LAN node.

Example response:

```
Please enter the IP Address for LAN Node 1:
```

5 Enter the IP address for the LAN node by typing

>IP address
and pressing the Enter key.

where

IP address is the IP address for the LAN node. The format is xxx.xxx.xxx.xxx, where xxx is a number from 0 to 255.

Response:

```
Do you wish to add another LAN Node? [YES]
```

Note: If you have commissioned four LAN nodes, the response "Do you wish to add another LAN Node? [YES]" will not appear. In that case, go to step 9.

6 Proceed according to whether you wish to commission another LAN node.

If you	Do
wish to commission another LAN node	step 7
do not wish to commission another LAN node	step 8

7 To commission another LAN node, press the Enter key, then go to step 3.

Example response:

```
Please enter the Description for LAN Node 1:
```

8 To finish commissioning LAN nodes, type

>NO
and press the Enter key.

Commissioning LAN nodes (continued)

9 Determine whether the LAN node values are correct.

Example response:

```
                                SDM COMMISSIONING

LAN NODES

The following values have been entered:

LAN Node 1 Description: telco
LAN Node 1 Hostname:    bnode78
LAN Node 1 IP Address:  47.105.144.32

Are these values correct? [YES]
```

If the	Do
LAN node values are correct	step 10
LAN node values are not correct	step 11

10 If the LAN node values are correct, press the Enter key.

Response:

```
Commissioning LAN Nodes – PASSED

HIT ENTER TO CONTINUE
```

If you get a response that commissioning of the LAN nodes failed, go to step 13.

Go to step 14.

11 Indicate the values are incorrect by typing

>NO
and pressing the Enter key.

Response:

```
– the Description for 1-4 LAN Nodes
– the Hostname for 1-4 LAN Nodes
– the IP Address for 1-4 LAN Nodes

Do you wish to proceed with LAN Node commissioning? [YES]
```

Commissioning LAN nodes (end)

12 Decide if you want to proceed with LAN node commissioning.

If you	Do
want to proceed with LAN node commissioning	step 2
do not want to proceed with LAN node commissioning	step 14

13 Contact your next level of support.

14 You have completed this procedure.

Log Delivery device commissioning

Application

Use this procedure to commission the Log Delivery service and to view and modify Log Delivery parameters. The online SDM commissioning tool called Logroute controls Log Delivery operating parameters.

The Logroute Device List menu specifies the output devices that receive logs from Log Delivery, and the characteristics for each defined device. The Device List menu displays any defined Log Delivery output devices. At initial commissioning of the Log Delivery service, there are no output devices displayed because they are not defined. Define all required output devices at initial commissioning time. The Device List menu also allows adding, deleting, and modifying of already defined devices.

The Device List menu provides access to the following device-specific submenus:

- TCP Device—defines TCP/IP output links to OSSs. For each TCP device, define the IP address of the OSS host machine, the port number of the machine, the log format, and the logs that will be routed to the OSS.
- TCP-IN Device—defines TCP/IP incoming links. For each TCP-IN device, define the port number to be used on the SDM, the log format, the remote address of the connecting OSS, and the logs that will be routed to the OSS.
- File—defines SDM-resident UNIX output files. Define the filename and log format for each UNIX file, and the logs that will be routed to the file.

A maximum of ten output devices (UNIX files and TCP/IP links) can be commissioned. Any combination of UNIX files and TCP/IP links can make up the ten commissioned output devices.

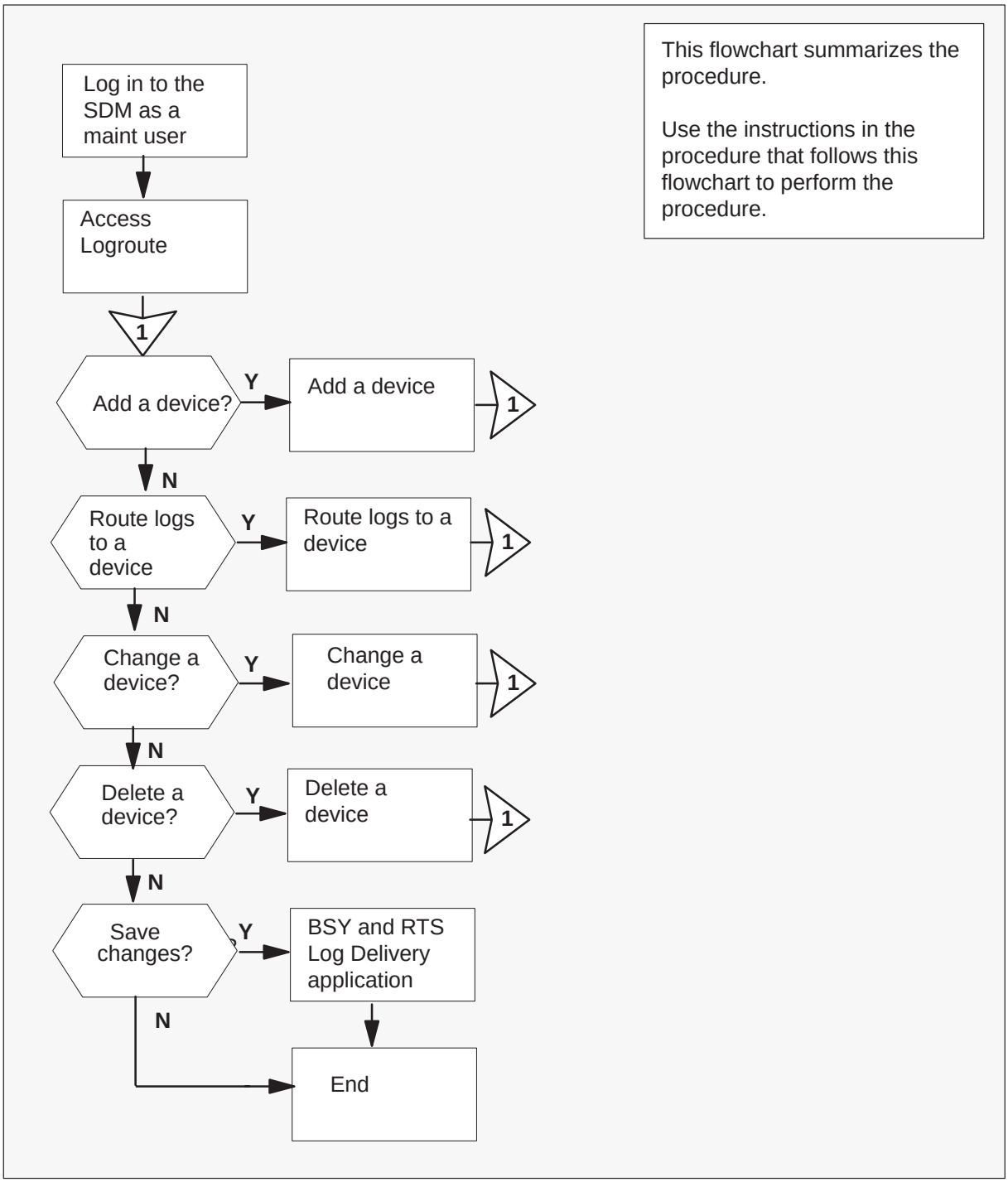
Note: To have commissioning changes take effect after you save the changes, busy and return the Log Delivery application to service. The Log Delivery application is not available for a short time during the busy and return-to-service process.

Action

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

Log Delivery device commissioning (continued)

Summary of Log Delivery device commissioning



Log Delivery device commissioning (continued)

Commissioning LAN connectivity

At the local or remote VT100 console

1 Log in to the RMI of the SDM as a maint user.

2 Access the Logroute commissioning tool by typing

>logroute
and pressing the Enter key.

Response:

```
                        Logroute Main Menu

              1 – Device List
              2 – Global Parameters
              3 – CM Configuration File



c:change menu,    q:quit,    h:help,   s:save changes

     Warning:  You must save, then BSY and RTS the Log Delivery
     =======   application for any changes to take effect.

Enter command ==>
```

Note: For help on Logroute commands, type h. To scroll down the help menu, type f. To scroll back through the help menu, type b. To quit the help menu, type p. To quit out of the Logroute tool, type q at the Logroute Main Menu.

3 Select change by typing

>c
and pressing the Enter key.

Response:

```
Enter number of main menu option:
```

Log Delivery device commissioning (continued)

4 Enter the option number for Device List by typing

>1
and pressing the Enter key.

Note: The following response shows an example where one output device (TCP/IP 47.208.7.54) has already been commissioned.

Response:

```
                          Device List

Devices:                                              Type:
1 – HOST:  47.208.7.54            PORT:  1200    TCP



c:change device,  a:add device,  d:delete device,  q:quit, h:help, m:main

Enter command ==>
```

5 Proceed according to whether you are adding a device, routing logs to a device, deleting a device or changing a device.

If you are	Do
adding a device	step 6
routing logs to a device (new or changed routing)	step 37
changing a device	step 54
deleting a device	step 51

Note: The changing a device option only allows you to change the device parameters (HOST IP, PORT, FILENAME, or FORMAT) and not the device's log routing.

6 Add a device by typing

>a
and pressing the Enter key.

Response:

```
Enter device type (t – TCP,  i – TCPIN, F – file)  ==>
```

Log Delivery device commissioning (continued)

7 Enter the device type by typing

>device type
and pressing the Enter key.

where

devicetype — is the device type. t defines TCP/IP output links to OSSs. i defines an in-bound TCP/IP connection. f defines SDM-resident UNIX output files.

Note: The following response shows an example for a TCP device type.

Response:

```
                              TCP Device

Device Parameters   1 – HOST IP    :
                    2 – PORT       :
                    3 – FORMAT     :STD

Log Routing



c:change parameter,  a:add log routing,  d:delete log routing
f: forward,  b:back, q:quit, h:help, p:previous menu, m:main

Enter command ==>
```

Log Delivery device commissioning (continued)

8 Proceed according to what kind of device you are adding.

If you are adding a	Do
TCP	step 9
TCP-IN device	step19
File device	step 30

9 Select the change option, by typing

>c
and pressing the Enter key.

Response:

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

10 Select the HOST IP option (to define the new device's IP address), by typing

>1
and pressing the Enter key.

Response:

```
Enter host IP address (###.###.###.###) ==>
```

11 Enter the HOST IP address by typing

>HOST IP
and pressing the Enter key.

where

HOST IP is the IP address of the OSS host machine.

12 Select the change option again by typing

>c
and pressing the Enter key.

Response:

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

13 Select the PORT option (to define the SDM port number the device will use), by typing

>2
and pressing the Enter key.

Response:

```
Enter port number (range – 5001 to 32767) ==>
```

14 Enter the port number by typing

>PORT NUMBER
and pressing the Enter key.

where

PORT NUMBER	is the port number of the OSS host machine. Enter a value between 5001 and 32 767.

Note: STD is the default value for the log format. If you do not want to change the default value for the log format, go to step 18.

15 Select the change option by typing

>c
and pressing the Enter key.

Response:

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

16 Select the FORMAT option (to define the format of logs sent to the new device), by typing

>3
and pressing the Enter key.

Response:

```
Enter format type (STD or SCC2) ==>
```

Log Delivery device commissioning (continued)

17 Enter the FORMAT by typing

>FORMAT
and pressing the Enter key.

where

FORMAT is the log format.

18 Proceed according to your requirements for further device work.

If you	Do
want to add log routing to this device	step 40
want to work on another device	step 5
do not want to do any more device work	step 61

19 Select the change option by typing

>c
and pressing the Enter key.

Response:

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

20 Select the PORT option to define the port on the SDM of the new device by typing

>1
and pressing the Enter key.

Response:

```
Enter port number (range - 8550 to 8559) ==>
```

Log Delivery device commissioning (continued)

21 Enter the PORT number by typing

>PORT NUMBER
and pressing the Enter key.

where:

PORT NUMBER — is the port on the SDM to which the remote OSS connects. Enter a value between 8550 and 8559.

Response:

```
                        TCP-IN DEVICE

Device Parameters
               1 – PORT            : 8558
               2 – FORMAT          : STD
               3 – REMOTE ADDRESS  : any
Log Routing

c:change change parameter, a:add log routing, d:delete log routing
f:forward, b:back, q:quit, h:help, p:previous menu, m:main menu

Enter command ==>
```

22 Select the change option by typing

>c
and pressing the Enter key.

Response:

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

23 Select the Format option to define the format of the logs sent to the new device by typing

>2
and pressing the Enter key.

Response:

```
Enter format type (STD or SCC2) ==>
```

Log Delivery device commissioning (continued)

24 Enter the FORMAT by typing

>FORMAT
and pressing the Enter key.

where

FORMAT is the log format.

Response:

```
                        TCP-IN DEVICE

Device Parameters
               1 – PORT            : 8558
               2 – FORMAT          : SCC2
               3 – REMOTE ADDRESS  : any
Log Routing

c:change change parameter, a:add log routing, d:delete log routing
f:forward, b:back, q:quit, h:help, p:previous menu, m:main menu

Enter command ==>
```

25 Proceed according to your requirements for your TCP-IN device.

If you	Do
want to specify a REMOTE ADDRESS	step 26
want to add log routing to this device	step 42
do not want to do any more device work	step 61
want to work on another device	step 5

26 Select the change option by typing

>c
and pressing the Enter key.

Response:

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

27 Select the REMOTE ADDRESS option to specify the IP address of the remote OSS by typing

>3
and pressing the Enter key.

Response:

```
Enter host IP address (###.###.###.###) or a for any ==>
```

28 Enter the REMOTE ADDRESS by typing

>REMOTE ADDRESS
and pressing the Enter key.

where

REMOTE ADDRESS — is the IP address of the OSS host machine or a for any host. If the REMOTE ADDRESS parameter is set to ”any”, the device accepts a connection from any IP address. Otherwise, the device only accepts a connection from a specified address.

Response:

```
                        TCP-IN DEVICE

Device Parameters
               1 – PORT            : 8558
               2 – FORMAT          : SCC2
               3 – REMOTE ADDRESS  : 47.208.12.237
Log Routing

c:change change parameter, a:add log routing, d:delete log routing
f:forward, b:back, q:quit, h:help, p:previous menu, m:main menu

Enter command ==>
```

If you	Do
want to add log routing to this device	step 42
do not want to do any more device work	step 61
want to work on another device	step 5

29 Select the change option again by typing

>c
and pressing the Enter key.

Response:

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

30 Access the change option to define the filename of the SDM-resident UNIX output files by typing

>c
and pressing the Enter key.

Response:

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

31

Log Delivery device commissioning (continued)

Select the option FILENAME (to define the file's UNIX name), by typing

>1
and pressing the Enter key.

Response:

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

32 Enter the file name by typing

>FILENAME
and pressing the Enter key.

where

FILENAME is the name of the UNIX file.

Response:

```
                                File

Device Parameters   1 – FILENAME   :/data/logs/logs
                    2 – FORMAT     :STD

Log Routing


c:change parameter,  a:add log routing,  d:delete log routing
f: forward,  b:back, q:quit, h:help, p:previous menu, m:main

Enter command ==>
```

Note: STD is the default value for the log format. If you do not want to change the default value for the log format, go to step 36.

33 Select the change option by typing

>c
and pressing the Enter key.

Response:

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

34 Select the option FORMAT (to define the log format), by typing

>2
and pressing the Enter key.

Response:

```
Enter format (STD or SCC2) ==>
```

35 Enter the format by typing

>FORMAT
and pressing the Enter key.

where

FORMAT is the log format. STD is the default value.

Response:

```
                              File

Device Parameters   1 – FILENAME   :/data/logs/LOGS
                    2 – FORMAT     :STD

Log Routing



c:change parameter,  a:add log routing,  d:delete log routing
f: forward,  b:back, q:quit, h:help, p:previous menu, m:main

Enter command ==>
```

36 Proceed according to your requirements for further device work.

If you	Do
want to add log routing to this device	step 40
want to work on another file device	step 5
do not want to do any more device work	step 61

Log Delivery device commissioning (continued)

37 Select the change option by typing

>c
and pressing the Enter key.

Response:

```
                              Device List

Devices:                                                    Type:
    1 – HOST: 99.99.99.99     PORT:     9999      TCP
    2 – HOST: 47.208.165.54   PORT      1002      TCP
    3 – /data/logs/logs




c:change device, a:add device, d:delete device, q:quit, h:help,  m:main

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

38 Enter the number of the device by typing

>n
and pressing the Enter key.

where

n is the number of the device you want to change.

Response:

```
c:change parameter, a:log routing, d:delete log routing, f:forward,
b:back, q:quit, h:help, p:previous menu, m:main

Enter command ==>
```

39 Proceed according to whether you are adding or deleting log routing.

If you	Do
want to add log routing	step 40
want to delete log routing	step 48

Log Delivery device commissioning (continued)

40 Select the add log routing option by typing

>a
and pressing the Enter key.

Response:

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

41 Decide if you want the new routing entry to add log(s) to the currently-defined stream (addrep) or delete log(s) from the currently-defined stream (delrep).

If you	Do
want to add log(s)	step 42
want to delete log(s)	step 45

42 Use the addrep command by typing

>a
and pressing the Enter key.

Response:

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

Log Delivery device commissioning (continued)

43 Enter the log identifier by typing

>log identifier
and pressing the Enter key.

where

log identifier — is the log type, or log type and log number.

Note: If both the log name and log number are entered, the log name and number must be separated by a space.

Response:

```
                              File

Device Parameters:                                          :
                    1 – FILENAME        :/data/logs/logs
                    2 – FORMAT          :SCC2


Log Routing         3 – ADDREP PM 100




c:change parameter, a:add log routing, d:delete log routing,
f: forward, b:back, q:quit, h:help,  p:previous menu, m:main

Enter command ==>
```

44 Proceed according to your requirements for further device work.

If you	Do
want to do more log routing on this device	step 39
want to work on another device	step 5
do not want to do any more device work	step 61

45 Use the delrep command by typing

>d
and pressing the Enter key.

Response:

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

46 Enter the log identifier by typing

>log identifier
and pressing the Enter key.

where

log identifier is the log type or log type number.

Note: If both the log name and log number are entered, the log name and number must be separated by a space.

Response:

```
                              File

Device Parameters:                                          :
                    1 – FILENAME        :/data/logs/logs
                    2 – FORMAT          :SCC2


Log Routing         3 – ADDREP PM 100
                    4 – DELREP PM 103



c:change parameter, a:add log routing, d:delete log routing,
f: forward, b:back, q:quit, h:help,  p:previous menu, m:main

Enter command ==>
```

47 Proceed according to your requirements for further device work.

If you	Do
want to do more log routing on this device	step 39
want to work on another device	step 5
do not want to do any more device work	step 61

48 Delete log routing by typing

>d
and pressing the Enter key.

Response:

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

Log Delivery device commissioning (continued)

49 Enter the number of the log routing from the File Menu by typing

>n
and pressing the Enter key.

where

n is the number of the log routing you want to delete.

50 Proceed according to your requirements for further device work.

If you	Do
want to do more log routing on this device	step 39
want to work on another device	step 5
do not want to do any more device work	step 61

51 Delete a device by typing

>d
and pressing the Enter key.

Response:

```
Enter device number to delete ==>
```

52 Enter the device number by typing

>device number
and pressing the Enter key.

where

device number is the menu number of the device you want to delete.

53 Proceed according to your requirements for further device work.

If you	Do
want to work on another device	step 5
do not want to do any more device work	step 61

54 Select the change device option by typing

>c
and pressing the Enter key.

Response:

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

55 Enter the menu number of the device you want to change by typing

>#
and pressing the Enter key.

where

is the menu number of the device you want to change.

Response:

```
                                TCP Device

Device Parameters   1 – HOST IP    :47.208.7.54
                    2 – PORT       :1212
                    3 – FORMAT     :STD

Log Routing




c:change parameter,  a:add log routing,  d:delete log routing
f: forward,  b:back, q:quit, h:help, p:previous menu, m:main

Enter command ==>
```

56 Select the change parameter option by typing

>c
and pressing the Enter key.

Response:

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

57 Enter the menu number of the parameter you want to change

>#
and pressing the Enter key.

where

is the menu number of the parameter you want to change.

Note: For a TCP or TCPIN device, the parameters are HOST IP, PORT, and FORMAT. For a File device, the parameters are FILE and FORMAT.

Log Delivery device commissioning (continued)

58 Enter the new value and press the Enter key.

59 Return to step 56 and repeat until you change every parameter you want to change.

60 Proceed according to your requirements for further device work.

If you	Do
want to work on another device	step 5
do not want to do any more device work	step 61

61 Return to the Logroute Main Menu by typing

>m
and pressing the Enter key.

62 Determine if you want to save any values you entered.

If you	Do
want to save the changes	step 63
do not want to save the changes	step 77

63 Save the values you entered by typing

>s
and pressing the Enter key.

Response:

```
                        Logroute Main Menu

              1 – Device List
              2 – Global Parameters
              3 – CM Configuration File



c:change menu,    q:quit,    h:help,   s:save changes

     Warning:  You must save, then BSY and RTS the Log Delivery
     =======   application for any changes to take effect.

    Save completed –– press return to continue
```

64 Press enter key and quit the Logroute tool by typing

>q
and pressing the Enter key.

Response:

```
NOTE:  Configuration data has changed
BSY and RTS the Log Delivery application
for changes to take effect.


maint:
```

65 Log out from the SDM by typing

>exit
and pressing the Enter key.

66 Determine if you want to activate the values you saved.

If you	Do
want to activate the values	step 67
do not want to activate the values	step 80

67 Log in to the SDM as the root user.

68 Access the top menu level of the RMI by typing

#sdmmtc
and pressing the Enter key.

69 Access the maintenance (MTC) menu level of the RMI by typing

>MTC
and pressing the Enter key.

70 Access the application (APPL) menu level of the RMI by typing

>APPL
and pressing the Enter key.

Example response:

```
# Package Description           Version     State
1  Table Access Service         9.0.21.0        InSv
2  OM Access Service            9.0.21.0        InSv
3  Log Delivery Service         9.0.21.0        InSv
4  Enhanced Terminal Access     8.0.21.0    InSv
5  Exception Reporting          8.0.21.0    InSv
```

Log Delivery device commissioning (continued)

71 Determine the number for the Log Delivery Service (shown under the header "#").

72 Manually busy the Log Delivery Service by typing

>BSY n
and pressing the Enter key.

where

n is the number under "#" of the Log Delivery Service from step 71.

Response:

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

Note: Busying the Log Delivery Service performs an orderly shutdown and can take up to 2 min.

73 Confirm the Busy command by typing

>Y
and pressing the Enter key.

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

75 Return the application to service by typing

>RTS n
and pressing the Enter key.

where

n is the number of the application (from step 71)

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

76 Quit the RMI by typing

>QUIT ALL
and pressing the Enter key.

Go to step 80.

77 Quit out of the Logroute tool without saving any of the values you have entered, by typing

>q
and pressing the Enter key.

Response:

```
Parameters have changed, do you want to save changes (y/n)?
```

Note: If you did not enter any changes, this message will not appear. Go to step 80.

78 Indicate that you do not want to save your changes by typing

>n
and pressing the Enter key.

79 Log out from the SDM by typing

>exit
and pressing the Enter key.

80 You have completed this procedure.

Log Delivery global parameters commissioning

Application

Use this procedure to commission the Log Delivery global parameters. 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.

The Logroute tool allows customization of the following global parameters:

- buffer size (number of logs)
- reconnect timeout value (secs)
- lost logs threshold (number of lost logs before the system generates a design log) Note: This parameter is for Nortel personnel only.
- ASCII line delimiter and log delimiter characters
- the number of days to keep log files

The global parameters are set to default values at initial installation and should not require modification. If the global parameters do require modification, the ranges and default for each numeric parameter are as follows:

- buffer size (number of logs): range is 50 to 300, default is 150
- reconnect timeout 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

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

Log Delivery global parameters commissioning (continued)

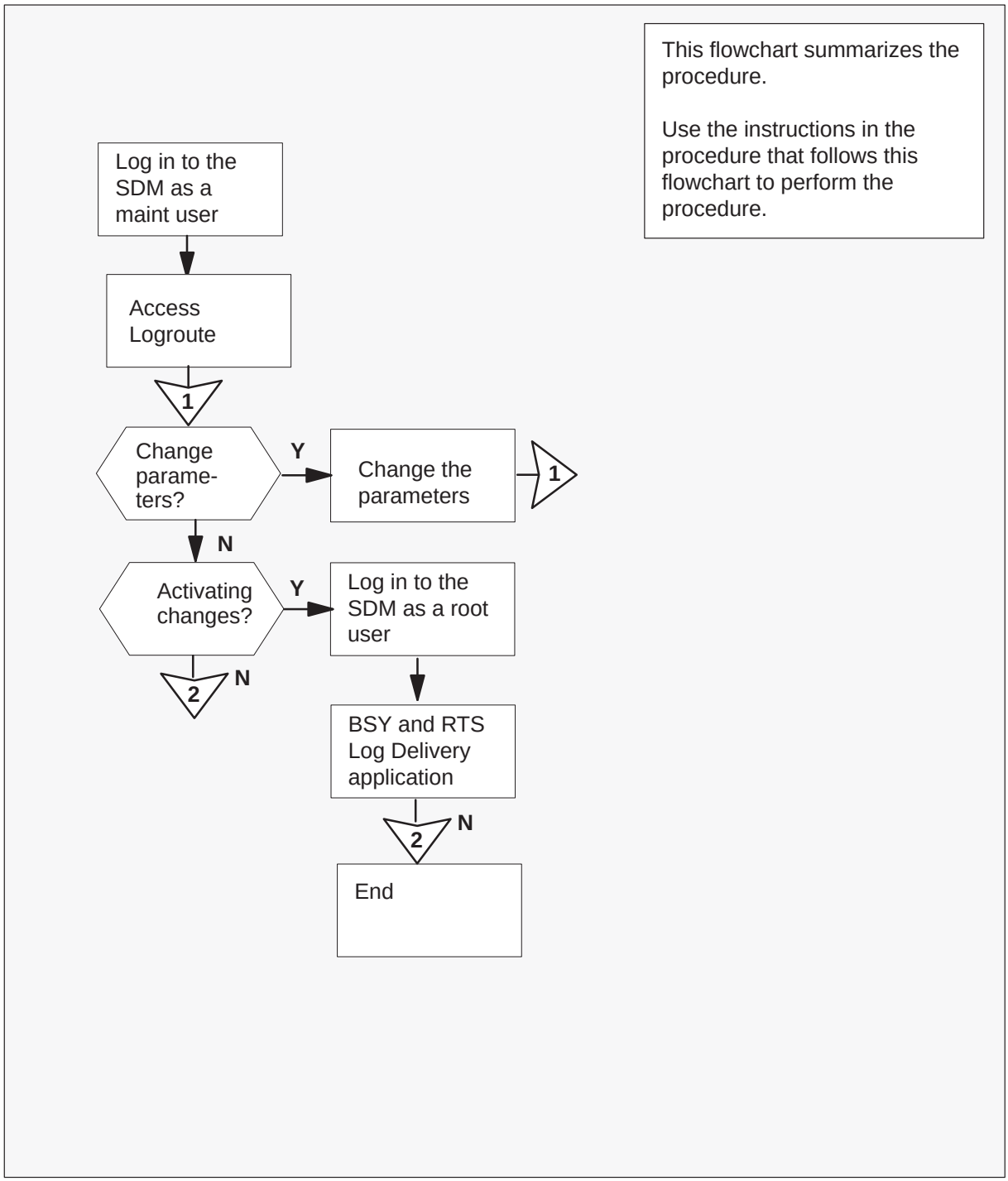
Note: To have any commissioning changes take effect after you save the changes, busy and return the Log Delivery application to service. The Log Delivery application is not available for a short time during the busy and return-to-service process.

Action

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

Log Delivery global parameters commissioning (continued)

Summary of Log Delivery global parameters commissioning



Log Delivery global parameters commissioning (continued)

Commissioning LAN connectivity

At the local or remote VT100 console

1 Log in to the RMI of the SDM as a maint user.

2 Access the Logroute commissioning tool by typing

#logroute
and pressing the Enter key.

Response:

```
                        Logroute Main Menu

              1 – Device List
              2 – Global Parameters
              3 – CM Configuration File



c:change menu,    q:quit,    h:help,   s:save changes

     Warning:  You must save, then BSY and RTS the Log Delivery
     =======   application for any changes to take effect.

Enter command ==>
```

Note: For help on Logroute commands, type h. To scroll down the help menu, type f. To scroll back through the help menu, type b. To quit the help menu, type p. To quit out of the Logroute tool, type q at the Logroute Main Menu.

3 Select change by typing

>c
and pressing the Enter key.

Response:

```
Enter number of main menu option:
```

4 Enter the option number for Global Parameters by typing

>2
and pressing the Enter key.

Log Delivery global parameters commissioning (continued)

Response:

```
                        Global Parameters


1 – Buffer size (number of logs)        : 150
2 – Reconnect timeout value (secs)      : 15
3 – Lost logs threshold (NT only)       : 100
4 – Incoming end of line character      : 10
5 – Outgoing end of line characters     : 10 13
6 – Start of log characters             : 10 13
7 – End of logs characters              : 10 13
8 – Number of days to keep log files    : 5



c:change item,  q:quit, h:help, m:main

Enter command ==>
```

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

5 Select the change item option by typing

>c
and pressing the Enter key.

Response:

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

6 Enter the menu number of the parameter you want to change by typing

>#
and pressing the Enter key.

where

is the menu number of the global parameter you want to change.

Note: The following display shows an example response for changing the buffer size parameter.

Log Delivery global parameters commissioning (continued)

Response:

```
                        Global Parameters


1 – Buffer size (number of logs)        : 150
2 – Reconnect timeout value (secs)      : 15
3 – Lost logs threshold (NT only)       : 100
4 – Incoming end of line character      : 10
5 – Outgoing end of line characters     : 10 13
6 – Start of log characters             : 10 13
7 – End of logs characters              : 10 13
8 – Number of days to keep log files    : 5


c:change item,  q:quit, h:help, m:main

Enter buffer size (range – 50 To 300) ==>
```

Note: 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. See the Help menu for details.

7 Enter a value. The changed value appears on the Global Parameter menu.

8 Determine if you want to change any other Global Parameters.

If you are	Do
changing another parameter	step 5
not changing another parameter	step 9

9 Return to the Logroute Main Menu by typing

>m

and pressing the Enter key.

10 Determine if you want to save your changes.

If you are	Do
saving your changes	step 11
not saving your changes	step 25

11 Save the values you entered by typing

>s

and pressing the Enter key.

Log Delivery global parameters commissioning (continued)

Response:

```
                        Logroute Main Menu

                1 – Device List
                2 – Global Parameters
                3 – CM Configuration File



c:change menu,    q:quit,    h:help,   s:save changes

     Warning:  You must save, then BSY and RTS the Log Delivery
     =======   application for any changes to take effect.

    Save completed –– press return to continue
```

12 Press the enter key and quit the Logroute tool by typing

>q
and pressing the Enter key.

Response:

```
NOTE:  Configuration data has changed
BSY and RTS the Log Delivery application
for changes to take effect.


maint:
```

13 Log out from the SDM by typing

>exit
and pressing the Enter key.

14 Determine if you want to activate the values you saved.

If you	Do
want to activate the values	step 15
do not want to activate the values	step 28

Note: Saved changes to the global parameters will not take effect unless you proceed to step 15.

15 Log in to the SDM as the root user.

16 Access the top menu level of the RMI by typing

#sdmmtc
and pressing the Enter key.

Log Delivery global parameters commissioning (continued)

17 Access the maintenance (MTC) menu level of the RMI by typing

>MTC
and pressing the Enter key.

18 Access the application (APPL) menu level of the RMI by typing

>APPL
and pressing the Enter key.

Example response:

```
# Package Description           Version     State
1  Table Access Service         9.0.21.0        InSv
2  OM Access Service            9.0.21.0        InSv
3  Log Delivery Service         9.0.21.0        InSv
4  Enhanced Terminal Access     8.0.21.0    InSv
5  Exception Reporting          8.0.21.0    InSv
```

19 Determine the number for the Log Delivery Service (shown under the header "#").

20 Manually busy the application software by typing

>BSY n
and pressing the Enter key.

where

n is the number under "#" of the Log Delivery Service

Response:

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

Note: Busying the Log Delivery Service performs an orderly shutdown and can take up to 2 min.

21 Confirm the Busy command by typing

>Y
and pressing the Enter key.

Log Delivery global parameters commissioning (continued)

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

23 Return the Log Delivery Service to service by typing

>RTS n
and pressing the Enter key.

where

n is the number of the Log Delivery Service (from step 18)

Response:

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

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”. Go to step 28.

Response:

```
Application RTS – Command submitted.
```

24 Press enter key and quit the RMI by typing

>QUIT ALL
and pressing the Enter key.

Go to step 27.

25 Quit out of the Logroute tool without saving any of the values you have entered, by typing

>q
and pressing the Enter key.

Response:

```
Parameters have changed, do you want to save changes (y/n)?
```

Note: If you did not enter any changes, the message above will not appear. Go to step 27.

Log Delivery global parameters commissioning (end)

26 Indicate that you do not want to save your changes by typing

>n
and pressing the Enter key.

27 Log out from the SDM by typing

>exit
and pressing the Enter key.

28 You have completed this procedure.

Log Delivery CM configuration file commissioning

Application

Use this procedure to commission the Log Delivery computing module (CM) configuration file parameters. When the Log Delivery service is first installed, it receives all logs in the CM log stream by default. The CM configuration file parameters do not require change unless you wish to modify the incoming global log stream. Use the CM configuration file menu in the Logroute commissioning tool to add or delete log reports to or from the incoming CM log stream.

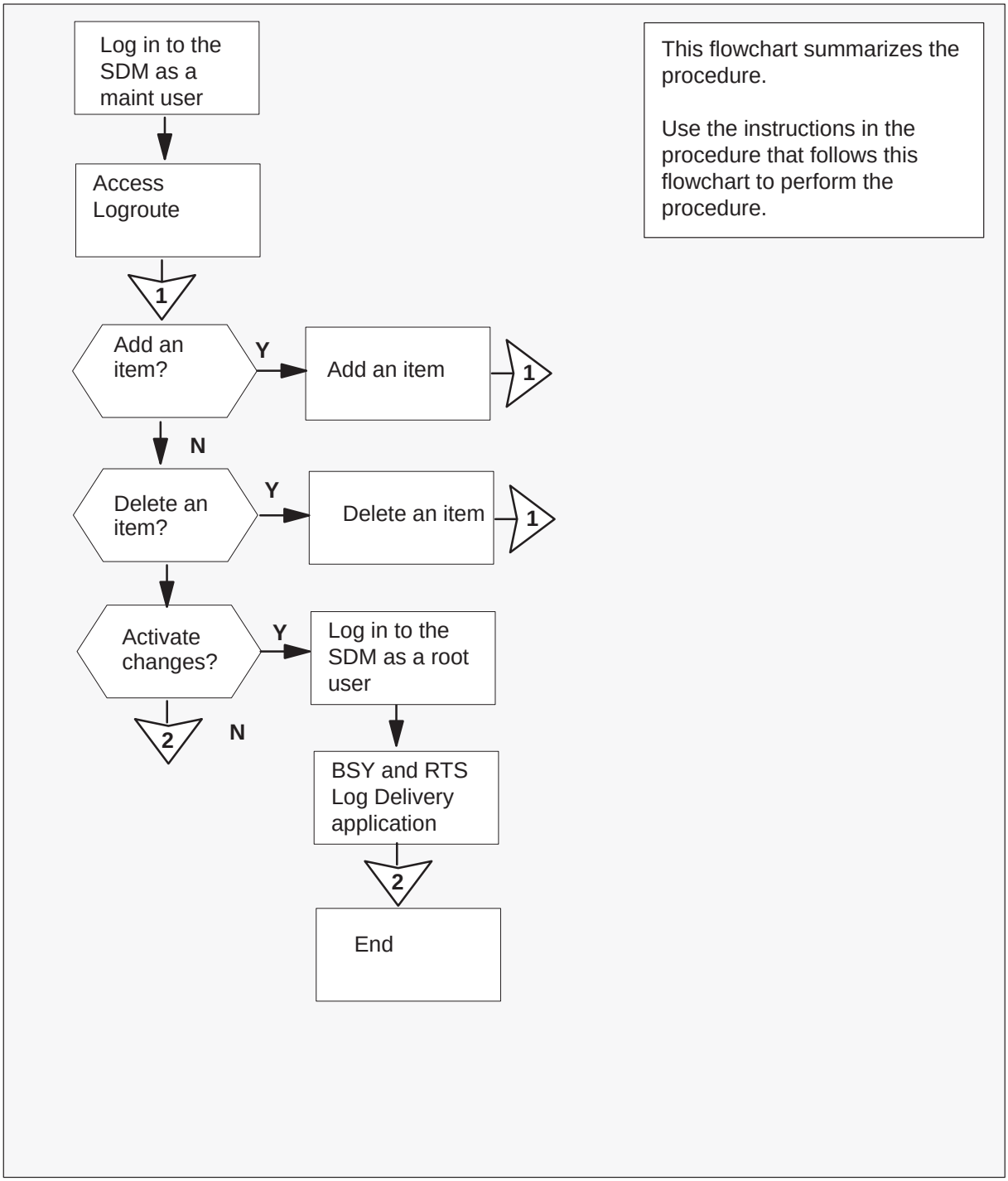
Note: To have any commissioning changes take effect after you save the changes, busy and return the Log Delivery application to service. The Log Delivery application is not available for a short time during the busy and return-to-service process.

Action

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

Log Delivery CM configuration file commissioning (continued)

Summary of Log Delivery CM configuration file commissioning



Log Delivery CM configuration file commissioning (continued)

Commissioning LAN connectivity

At the local or remote VT100 console

1 Log in to the RMI of the SDM as a maint user.

2 Access the logroute commissioning tool by typing

>logroute
and pressing the Enter key.

Response:

```
                        Logroute Main Menu

              1 – Device List
              2 – Global Parameters
              3 – CM Configuration File




c:change menu,    q:quit,    h:help,   s:save changes

     Warning:  You must save, then BSY and RTS the Log Delivery
     =======   application for any changes to take effect.

Enter command ==>
```

Note: For help on Logroute commands, type h. To scroll down the help menu, type f. To scroll back through the help menu, type b. To quit the help menu, type p. To quit out of the Logroute tool, type q at the Logroute Main Menu.

3 Select change by typing

>c
and pressing the Enter key.

Response:

```
Enter number of main menu option:
```

4 Enter the option number for CM Configuration File by typing

>3
and pressing the Enter key.

Note: The following display shows an example response where one log report (CM 100) has been deleted from the incoming CM log stream.

Log Delivery CM configuration file commissioning (continued)

Response:

```
                        CM Config File


1 – DEL CM 100



f:forward, b:back a:add item, d: delete item
     q:quit, h:help, m:main menu

Enter command ==>
```

5 Determine how you want to change the CM Config File.

If you want to	Do
add an item to the list	step 6
delete an item from the list	step 10
return to the main menu	step 13

6 Enter the menu option for adding an item by typing

>a
and pressing the Enter key.

Response:

```
Enter – a: addrep or d: delrep (or n for NOCMLOGS) ==>
```

7 Determine if you want the new list item to be a log addition or a log deletion by typing

>n
and pressing the Enter key.

where

n is the letter associated with the task you want to perform. Type a for a log addition (addrep). Type d for log deletion (delrep).

Response:

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

Log Delivery CM configuration file commissioning (continued)

8 Enter the log identifier by typing

>log identifier
and pressing the Enter key.

where

log identifier — is the log type, or log type and number to be added or deleted.

Note: If the log name and log number are both present, they must be separated by a space. In the following response, all PM logs were deleted by typing d pm.

Response:

```
                              CM Config File


                    1 – DEL CM 100
                    2 – DEL PM




f:forward, b:back a:add item, d:delete item
q:quit, h:help,  m:main menu

Enter – a: addrep or d: delrep (or n for NOCMLOGS) ==>
```

9 Determine if you want to make more changes to the CM log stream list.

If you	Do
want to make more changes	step 5
do not want to make more changes	step 14

10 Enter the menu option for deleting an item from the log stream list by typing

>d
and pressing the Enter key.

Response:

```
Enter item number to delete ==>
```

Log Delivery CM configuration file commissioning (continued)

11 Enter the number of the item you want to delete from the list by typing

>#

and pressing the Enter key.

where

is the number of the item from the list that you want to delete.

12 Determine if you want to make more changes to the CM log stream list.

If you	Do
want to make more changes	step 5
do not want to make more changes	step 14

13 Return to the Logroute Main Menu by typing

>m

and pressing the Enter key.

14 Determine if you want to save any values you entered.

If you	Do
want to save the changes	step 13
do not want to save the changes	step 29

15 Save the values you entered by typing

>s

and pressing the Enter key.

Note: After you save the changes you made to the CM log stream, the changes must be activated. Busy and return the log delivery application to service to have the changes take effect.

Log Delivery CM configuration file commissioning (continued)

Response:

```
                        Logroute Main Menu

                1 – Device List
                2 – Global Parameters
                3 – CM Configuration File



c:change menu,    q:quit,    h:help,   s:save changes

     Warning:  You must save, then BSY and RTS the Log Delivery
     =======   application for any changes to take effect.

    Save completed –– press return to continue
```

16 Press the enter key and quit the Logroute tool by typing

>q
and pressing the Enter key.

Response:

```
    NOTE:  Configuration data has changed
    BSY and RTS the Log Delivery application
    for changes to take effect.


maint:
```

17 Log out from the SDM by typing

>exit
and pressing the Enter key.

18 Determine if you want to activate the values you saved.

If you	Do
want to activate the values	step 19
do not want to activate the values	step 32

19 Log in to the SDM as the root user.

20 Access the top menu level of the RMI by typing

#sdmmtc
and pressing the Enter key.

Log Delivery CM configuration file commissioning (continued)

21 Access the maintenance (MTC) menu level of the RMI by typing

>MTC
and pressing the Enter key.

22 Access the application (APPL) menu level of the RMI by typing

>APPL
and pressing the Enter key.

Example response:

```
# Package Description           Version     State
1  Table Access Service         9.0.21.0        InSv
2  OM Access Service            9.0.21.0        InSv
3  Log Delivery Service         9.0.21.0        InSv
4  Enhanced Terminal Access     8.0.21.0    InSv
5  Exception Reporting          8.0.21.0    InSv
```

23 Note the number of the Log Delivery Service (shown under the header "#").

24 Manually busy the Log Delivery Service by typing

>BSY n
and pressing the Enter key.

where

n is the number of the Log Delivery Service (from step 23)

Response:

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

Note: Busying the Log Delivery Service performs an orderly shutdown and can take up to 2 min.

25 Confirm the Busy command by typing

>Y
and pressing the Enter key.

Log Delivery CM configuration file commissioning (continued)

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

27 Return the Log Delivery Service to service by typing

>RTS n
and pressing the Enter key.

where

n is the number of the Log Delivery Service (from step 22)

Response:

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

When the RTS command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”. Go to step 32.

Response:

```
Application RTS – Command submitted.
```

28 Quit the RMI by typing

>QUIT ALL
and pressing the Enter key.

Go to step 31.

29 Quit out of the CM Config File menu without saving any of the values you have entered, by typing

>q
and pressing the Enter key.

Response:

```
Parameters have changed, do you want to save changes (y/n)?
```

Note: If you did not enter any changes, the message above will not appear. Go to step 31.

Log Delivery CM configuration file commissioning (end)

30 Indicate that you do not want to save your changes by typing

>n
and pressing the Enter key.

31 Log out from the SDM by typing

>exit
and pressing the Enter key.

32 You have completed this procedure.

Migration from a rootvg system to a rootvg/datavg system

Application

ATTENTION

This procedure must be performed by a trained AIX system administrator who has root user privileges to access the SDM.

ATTENTION

Perform this procedure after your system has been installed with the required I/O controller modules installed, in pairs, in the appropriate slots in the main or I/O expansion chassis. If you have not installed the required modules, refer to the procedure ”Adding I/O controller modules” on page 4-64 in the “SDM maintenance procedures” chapter of this document.

Logical volume data can be stored in the root volume group (rootvg) or the data volume group (datavg). Nortel recommends that you create datavg for logical volumes with large amounts of data. If you do not create datavg, logical volume data is stored in rootvg.

ATTENTION

A maximum of 16-Gbyte storage capacity is supported for datavg in this release in SDM09.

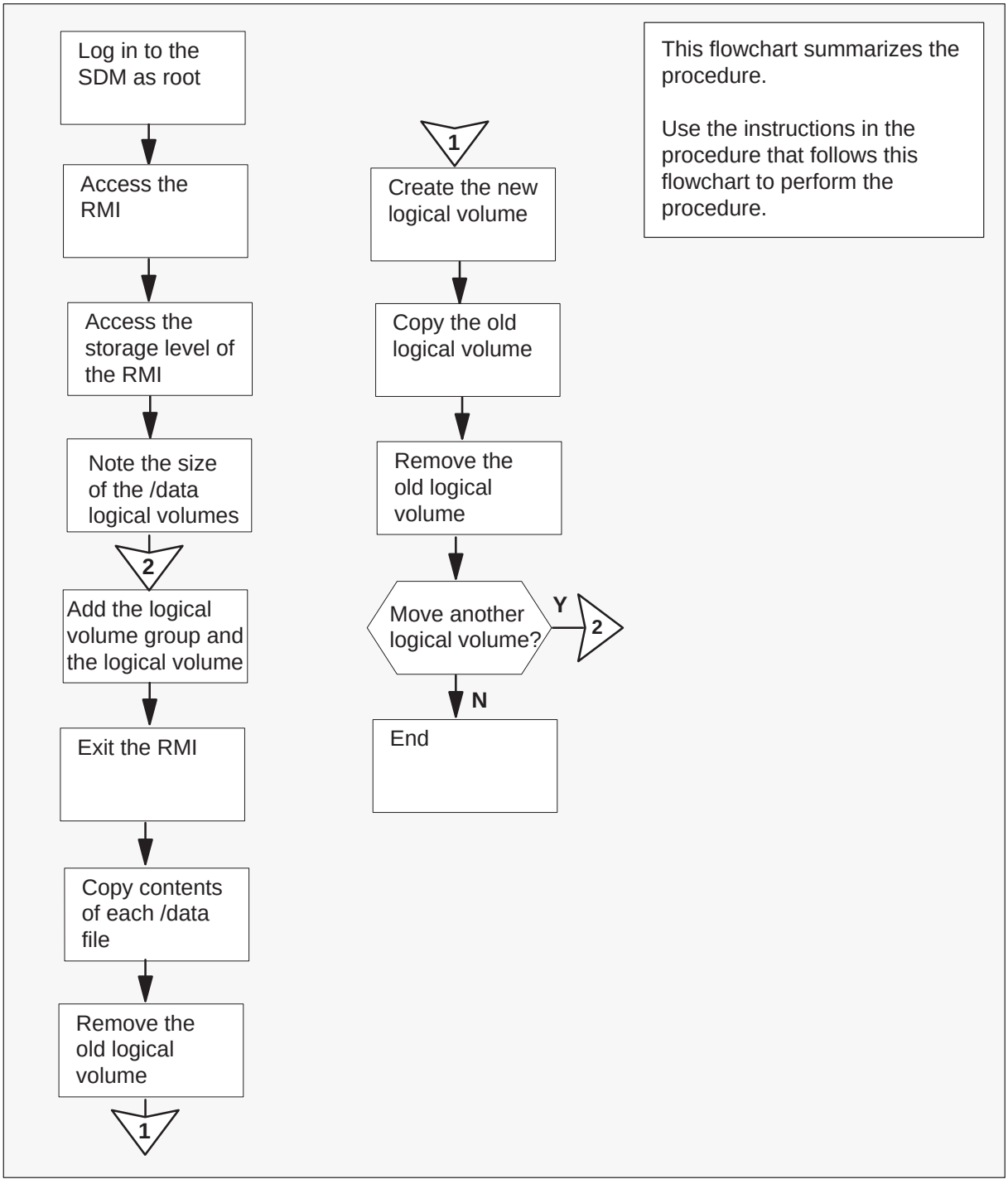
Use this procedure to move from a rootvg system to a system with both rootvg and datavg. This procedure creates datavg, and moves logical volumes from rootvg to datavg. Do not use this procedure if you have a new system that requires datavg. Refer to the procedure ”Creating a logical volume in the data volume group” on page 4-151 in the “SDM maintenance procedures” chapter in this document.

Action

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

Migration from a rootvg system to a rootvg/datavg system (continued)

Summary of Migration from a rootvg system to a rootvg/datavg system



Migration from a rootvg system to a rootvg/datavg system (continued)

Creating a data volume group

At the local VT100 console

1 Log in to the SDM as the root user.

2 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                    InSv
   Volume             Size (MB)        (% full/ threshold)
 1 /                     20                    25/ 80
 2 /usr                  192                   85/ 90
 3 /var                  40                    11/ 80
 4 /tmp                  24                     6/ 90
 5 /home                 300                    4/ 70
 6 /sdm                  300                   44/ 90
 7 /data/sba             112                   49/ 80
```

Note: The example response shows part of the information displayed at the storage menu level of the RMI. All data is stored in rootvg.

5 Note the size (in Mbyte) of each logical volume preceded by “/data”.

6 Add a new disk by typing

>ADD DSK
and pressing the Enter key.

Response:

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

Datavg is currently being created...
```

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

Response:

```
All disks were successfully added.

Command complete.
```

Migration from a rootvg system to a rootvg/datavg system (continued)

Note 1: This step automatically adds datavg.

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

7 Create the new logical volume in datavg by typing

>add lv xxx size
and pressing the Enter key.

where

xxx is the logical volume you are moving to datavg
size is the size of the logical volume in Mbyte

Note: Use the same size shown next to the /data/xxx_old logical volume in the system menu level screen.

Response:

```
Creating Volume tempfs
```

8 Press the Enter key to continue. A message is displayed after several minutes confirming that the volume has been successfully created.

Response:

```
Volume Successfully Created
```

9 Press the Enter key to continue.

Response:

```
Command complete.
```

Note: If any failure messages are displayed, contact the personnel responsible for the next level of support.

10 Press the Enter key after you see the “Command complete” response. The new tempfs logical volume is displayed under the datavg volume group listing.

Response:

```
Disk mirroring (rootvg):                    InSv
   Volume             Size (MB)        (% full/ threshold)
 1 /                     20                    25/ 80
 2 /usr                  192                   85/ 90
 3 /var                  40                    11/ 80
 4 /tmp                  24                     6/ 90
 5 /home                 300                    4/ 70
 6 /sdm                  300                   44/ 90
 7 /data/sba             112                   49/ 80

Disk mirroring (datavg):                     InSv
   Volume              Size (MB)       (% full/ threshold)
 8 /tempfs           112                    49/ 80
```

Migration from a rootvg system to a rootvg/datavg system (continued)

11 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

12 Copy the contents the original logical volume (/data/xxx) to the temporary logical volume (/data/tempfs) by typing

 # cp -R /data/xxx/* /data/tempfs
and pressing the Enter key.

where

xxx	is the logical volume you are moving to datavg

13 Remove the old logical volume that was moved by typing the following series of commands:

 # unmount /xxx
and press the Enter key.

 # rmfs /xxx
and press the Enter key.

 # rm -r /xxx
and press the Enter key.

where

xxx	is the logical volume you are moving to datavg

14 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

15 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

16 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

17 Create the new logical volume in datavg by typing

>add lv xxx size
and pressing the Enter key.

where

xxx	is the logical volume you are moving to datavg
size	is the size of the logical volume in Mbyte

Migration from a rootvg system to a rootvg/datavg system (continued)

Note: Use the same size which was shown next to the /xxx_old logical volume in the system menu level screen (noted in step 5).

Example response:

```
Creating Volume sba
```

18 Press the Enter key to continue. A message is displayed after several minutes confirming that the volume has been successfully created.

Response:

```
Volume Successfully Created
```

19 Press the Enter key to continue.

Response:

```
Command complete.
```

Note: If any failure messages are displayed, contact the personnel responsible for the next level of support.

20 Press the Enter key, after you see the “Command complete” response. The new logical volume is displayed under the datavg volume group listing.

Example response:

```
Disk mirroring (rootvg):                    InSv
   Volume             Size (MB)        (% full/ threshold)
 1 /                     20                    25/ 80
 2 /usr                  192                   85/ 90
 3 /var                  40                    11/ 80
 4 /tmp                  24                     6/ 90
 5 /home                 300                    4/ 70
 6 /sdm                  300                   44/ 90

Disk mirroring (datavg):                     InSv
   Volume               Size (MB)       (% full/ threshold)
 7 /tempfs          112                      49/ 80
 8 /data/sba             112                    49/ 80
```

21 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

22 Copy the contents of the temporary logical volume by typing

 # cp -R /data/tempfs/* /data/xxx/.
and pressing the Enter key.

where

xxx is the old logical volume in rootvg

Migration from a rootvg system to a rootvg/datavg system (end)

23 Remove the contents of the temporary logical volume by typing the following series of commands:

 # unmount /data/tempfs
and pressing the Enter key.

>rmfs /data/tempfs
and pressing the Enter key.

>rm -r /data/tempfs

24 Determine if you wish to move another logical volume to datavg.

If you	Do
wish to move another logical volume	step 25
do not wish to add another logical volume	step 28

25 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

26 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

27 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Go to step 7.

28 You have completed this procedure.

Creating a logical volume in the data volume group

Application

ATTENTION

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

ATTENTION

Perform this procedure after your system has been installed with the required I/O controller modules installed, in pairs, in the appropriate slots in the main or I/O expansion chassis. If you have not installed the required modules, refer to the procedure "Adding I/O controller modules" in this chapter.

Use this procedure if you have a new system that requires the data volume group (datavg) to store logical volume data. If you have a root volume group (rootvg) system, and wish to add datavg to your system, use the procedure "Migration from a rootvg system to a rootvg/datavg system" on page 4-144 in this chapter.

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

ATTENTION

The logical volume management feature does not prevent you from creating more than 16 logical volumes. The software only tracks the first 16 logical volumes and ignores the others.

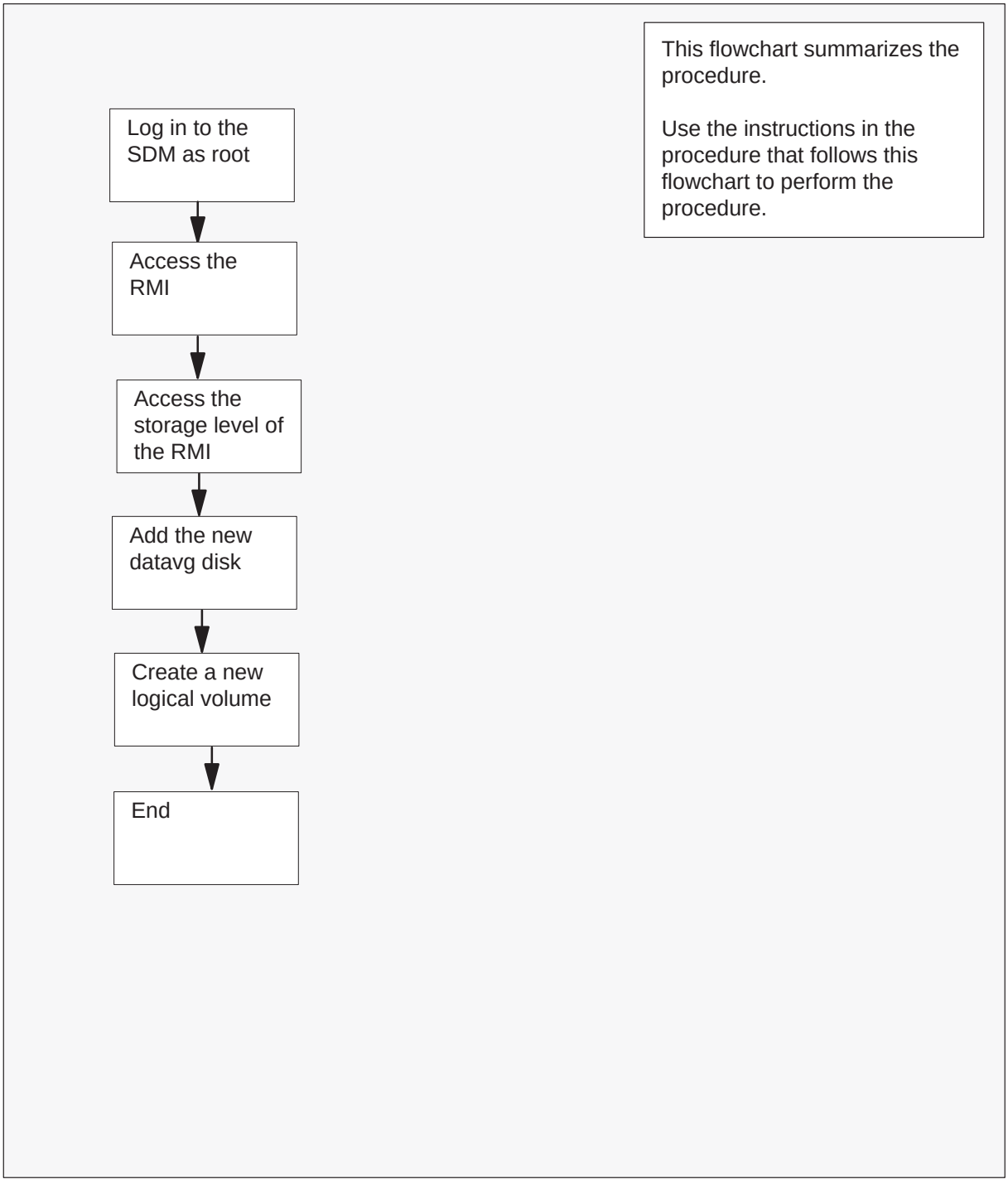
There is no impact on functionality and no increased risk of jeopardizing data. The amount of free space displayed in the unallocated field of the storage menu level screen always displays the correct data.

Action

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

Creating a logical volume in the data volume group (continued)

Summary of Creating a logical volume in the data volume group



Creating a logical volume in the data volume group (continued)

Creating a data volume group

At the local VT100 console

1 Log in to the SDM as the root user.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                        Mirrored
   Volume             Size (MB)        (% full/ threshold)
 1 /                     20                      25/ 80
 2 /usr                  192                     85/ 90
 3 /var                  40                      11/ 80
 4 /tmp                  24                       6/ 90
 5 /home                 300                      4/ 70
 6 /sdm                  300                     44/ 90
(unallocated)            608
```

Note: The example response shows part of the information displayed at the storage menu level of the RMI. There are no logical volumes in datavg.

Creating a logical volume in the data volume group (end)

5 Add a new disk by typing

>ADD DSK
and pressing the Enter key.

Example response:

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

Datavg is currently being created...
```

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

Example response:

```
All disks were successfully added.

Command complete.
```

Note 1: This step automatically adds datavg.

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

6 Create the new logical volume by typing

>add lv xxx Mbyte
and pressing the Enter key.

where

xxx	is the new logical volume name
Mbyte	is the size of the logical volume in Mbyte

Example response:

```
Creating volume sba.
```

Note: An error message appears if you enter a backslash as part of the logical volume name.

Example input:

>add lv abc/def 20

Example response:

```
ERROR: Slash '/' should not be part of filesystem name.
```

Note: If directory xxx already exists, and you try to create a new logical volume with the same name as directory xxx, an error message appears.

Example response:

```
ERROR: Mountpoint for the new filesystem /xxx
       already exists.
```

7 You have completed this procedure.

Increasing the size of a logical volume

Application

ATTENTION

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

Use this procedure to allocate more disk space to a logical volume.

WARNING

Increasing the size of a logical volume may limit future software upgrade capability.

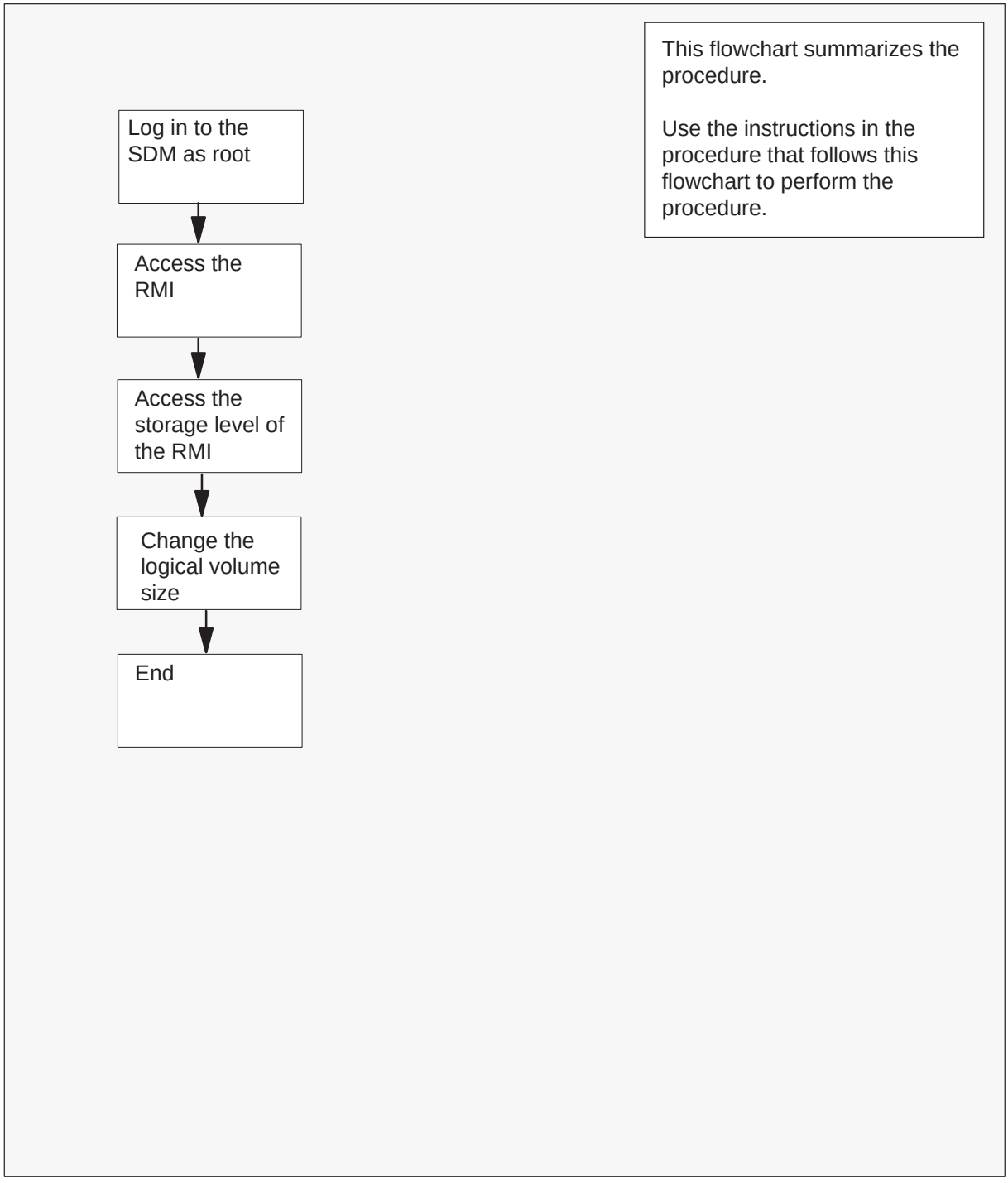
SDM logical volumes are pre-engineered to sizes that are adequate for Nortel customers. Do not increase the size of a logical volume unless absolutely necessary. If you need to change the size of a logical volume, do so only with the assistance of Nortel Technical Assistance and Support. Failure to follow this warning may jeopardize future software upgrade capability.

Action

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

Increasing the size of a logical volume (continued)

Summary of Increasing the size of a logical volume



Increasing the size of a logical volume (continued)

Increasing the size of a logical volume

At the local VT100 console

1 Log in to the SDM as the root user.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response:

```
SDM Node State:                 ISTb
SDM System State:               ISTb
SDM Storage State:              ISTb

Disk mirroring (rootvg):                          Mirrored
   Volume             Size (MB)        (% full/ threshold)
 1 /                     240                       52/ 80
 2 /usr                  204                       82/ 90
 3 /var                  40                        35/ 70
 4 /tmp                  24                        21/ 90
 5 /home                 304                       75/ 70*
 6 /sdm                  304                       47/ 90
 7 /home/sba             16                         7/ 80
(unallocated)            608
```

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

5 Determine if there is unallocated disk space that can be used to increase a logical volume.

If there is	Do
enough disk space	step 6
not enough disk space	step 8

6 Identify the logical volume whose size you want to increase. Note the volume name of the logical volume on the left of the System menu of the RMI.

Increasing the size of a logical volume (continued)

7

ATTENTION

A logical volume on the SDM must never reach 100% full. System behaviour cannot be predicted when a logical volume reaches 100% full. If the occupancy level of the specified logical volume has exceeded its alarm threshold, contact your system administrator to assess the current condition of the logical volume.

Change the size of the logical volume by typing

>CHANGE LV /xx Mbyte
and pressing the Enter key.

where

/xx	is the name of the logical volume
Mbyte	is the size in Mbytes to be added to the logical volume. The size must be less than the amount of unallocated disk space.

Example input:

>CHANGE LV /home 48

Example response:

```
Expanding Volume / home/sba


More...

SDM Node State                InSv
SDM System State              InSv
SDM Storage State             InSv

Disk mirroring (rootvg):                          Mirrored
   Volume             Size (MB)        (% full/ threshold)
 1 /                     240                      52/ 80
 2 /usr                  204                      82/ 90
 3 /var                  40                       35/ 70
 4 /tmp                  24                       21/ 90
 5 /home                 352                      65/ 70
 6 /sdm                  304                      47/ 90
 7 /home/sba             64                        7/ 80
(unallocated)            560
```

In the example response, the logical volme /home/sba was expanded by 48 Mbytes.

Increasing the size of a logical volume (end)

Note: The SDM may round the new size to the nearest 4-, 8-, or 16-Mbyte increment. For a 2-Gbyte disk, you can only add 4-Mbyte multiples. For a 4-Gbyte disk, add 8- or 16-Mbyte multiples. When the logical volume is created, the operating system determines the multiple that has to be used.

8 Contact your next level of support.

9 You have completed this procedure.

Adding an I/O expansion chassis (NTRX50EC)

Application

ATTENTION

Do not perform this procedure if there are any hardware faults on the SDM.

Use this procedure to add an I/O expansion chassis (NTRX50EC) to an existing system. You can perform this procedure when the hardware modules are available or not available. If the hardware modules are available when you are adding the I/O expansion chassis, do not plug the modules in.

Before you perform this procedure, mount the I/O expansion chassis in position 28 of the SDM cabinet.

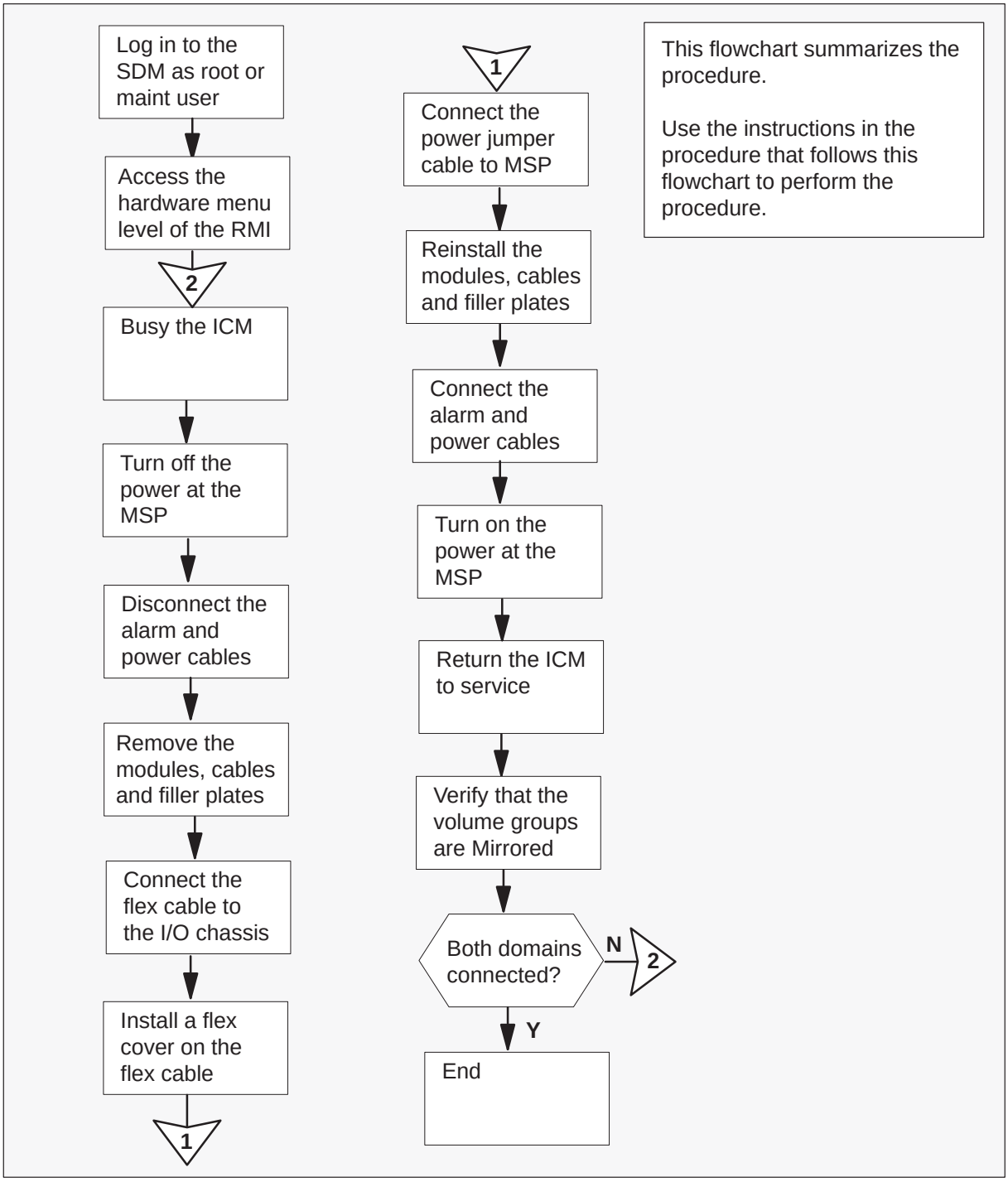
Before you perform this procedure, perform the procedure *Creating SDM backup tapes – System image backup (S-tape)* on page 6-26 of this book.

Action

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

Adding an I/O expansion chassis (NTRX50EC) (continued)

Summary of Adding an I/O expansion chassis (NTRX50EC)



Adding an I/O expansion chassis (NTRX50EC) (continued)

Adding an I/O expansion chassis (NTRX50EC)

At the local or remote VT100 console

1 Log in to the SDM as the root or maint user.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

Example response:

```
SDM Node State:            InSv
SDM Hardware State:        InSv

         I F C E D D 5
         C A P T S A 1
         M N U H K T 2

Domain 0 . . . . . .
Domain 1 . . . . . .
```

4 Check the status of hardware on the SDM. The component “Hw” in the alarm banner must show a dot (.), indicating that all hardware components are in service. In the example shown, there are no hardware faults on the SDM. If your system has any hardware faults, clear the faults before you continue this procedure.

5 Manually busy the interconnect module (ICM) in domain 0 by typing

>BSY 0 ICM
and pressing the Enter key.

Response:

```
Hardware Bsy – Domain 0 Device ICM
This action will affect all devices in I/O domain 0.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

6 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

Note: When you manually busy ICM 0, all subtending devices in domain 0 are also put in the ManB state.

Adding an I/O expansion chassis (NTRX50EC) (continued)

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

Response:

```
Hardware Bsy : Domain 0 Device ICM – Command initiated.
Please wait...
```

Several warnings are displayed. The “Please wait...” message, and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Response:

```
Hardware Bsy : Domain 0 Device ICM – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the interconnect module and all subtending devices changes to “C”. The out-of-service LED on the module is on (red).

Example response

```
SDM Node State:              ManB
SDM Hardware State:          ISTb

          I F C E D D 5
          C A P T S A 1
          M N U H K T 2

Domain 0 M C . C C C C
Domain 1 . . . . . . .
```

8 Access the system (Sys) menu level of the RMI by typing

>SYS

and pressing the Enter key.

Adding an I/O expansion chassis (NTRX50EC) (continued)

9 Access the storage menu level of the RMI by typing

>5

and pressing the Enter key.

Example response

```
Disk mirroring (rootvg):                    Not Mirrored
  Volume              Size(MB)       (% full/ threshold)
 1  /                    20                   79/ 80
 2  /usr                 192                  87/ 90
 3  /var                 40                   46/ 90
 4  /tmp                 20                   16/ 90
 5  /home                300                  81/ 90
(unallocated)            692

Disk mirroring (datavg):                    Not Mirrored
   Volume              Size(MB)       (% full/ threshold)
 7 /data/sba            1008                   66/ 80
(unallocated)           11168
```

10 Wait until the status of the root volume group (rootvg) and the data volume group (datavg), if applicable, is not mirrored.

At the front of the MSP

11 Turn off the power to SDM domain 0 by turning off both breakers in slot 10 of the modular supervisory panel (MSP).

At the back of the SDM

12

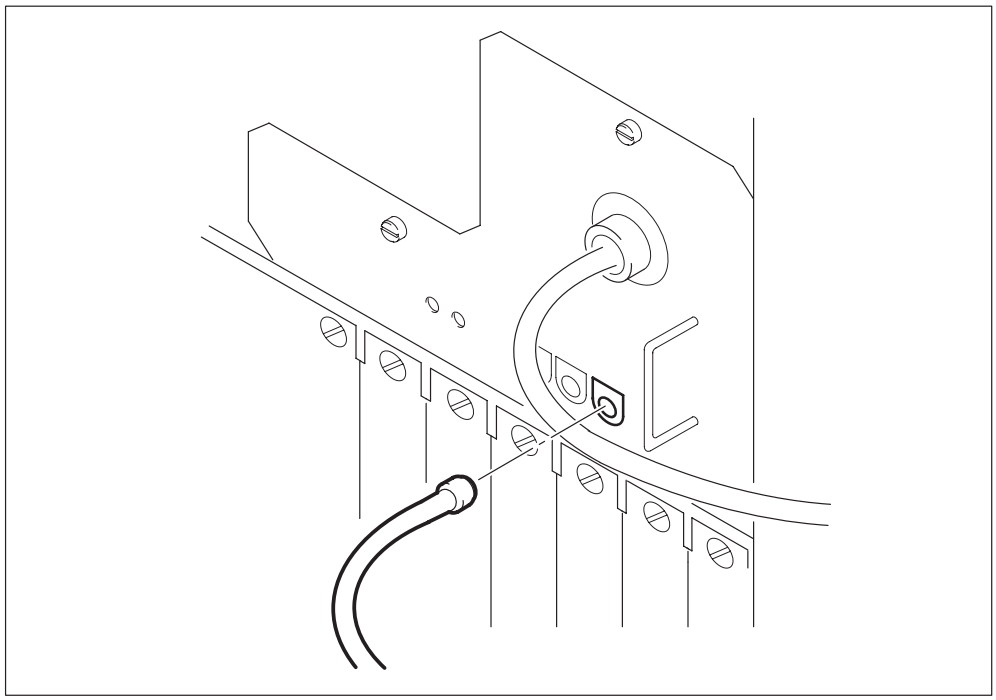
WARNING

Static electricity damage

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Adding an I/O expansion chassis (NTRX50EC) (continued)

13 Disconnect the alarm cable from ICM 0.

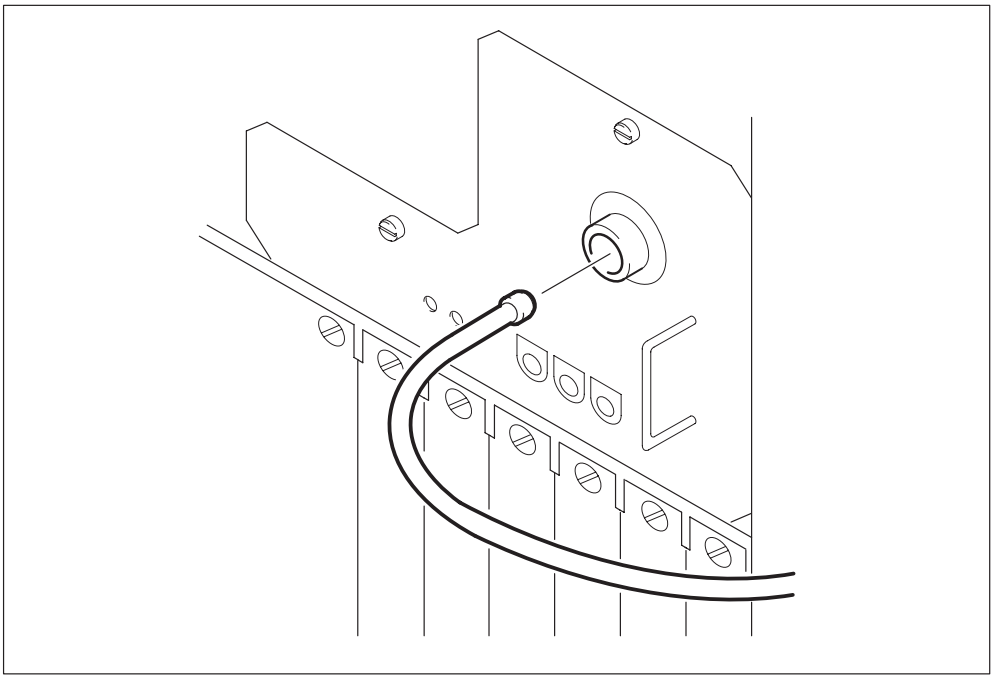


Note: The alarm cable is only present on systems with a main chassis only. This cable is not required when you add the I/O expansion chassis to your system.

Adding an I/O expansion chassis (NTRX50EC) (continued)

14 Disconnect the power cable from ICM 0.

CAUTION
Potential service interruption
Ensure that you disconnect the power cable from ICM 0. If you disconnect the power cable to the remaining in-service ICM (ICM 1), the entire SDM shuts down.



At the back of the SDM

15 Loosen the two thumbscrews located at the top and the bottom of the DS512 personality module (located in slot 1).

Note: The thumbscrews are the captive type, and cannot be removed from the module.

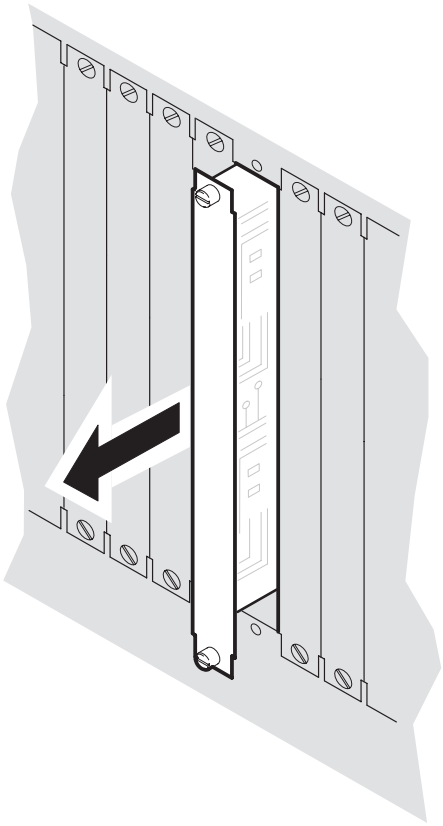
Adding an I/O expansion chassis (NTRX50EC) (continued)

16

CAUTION
Disconnecting transmit and receive cables
Do not mix the transmit and receive cables for each domain. If you have not already done so, label these cables to ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Disconnect the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the left.

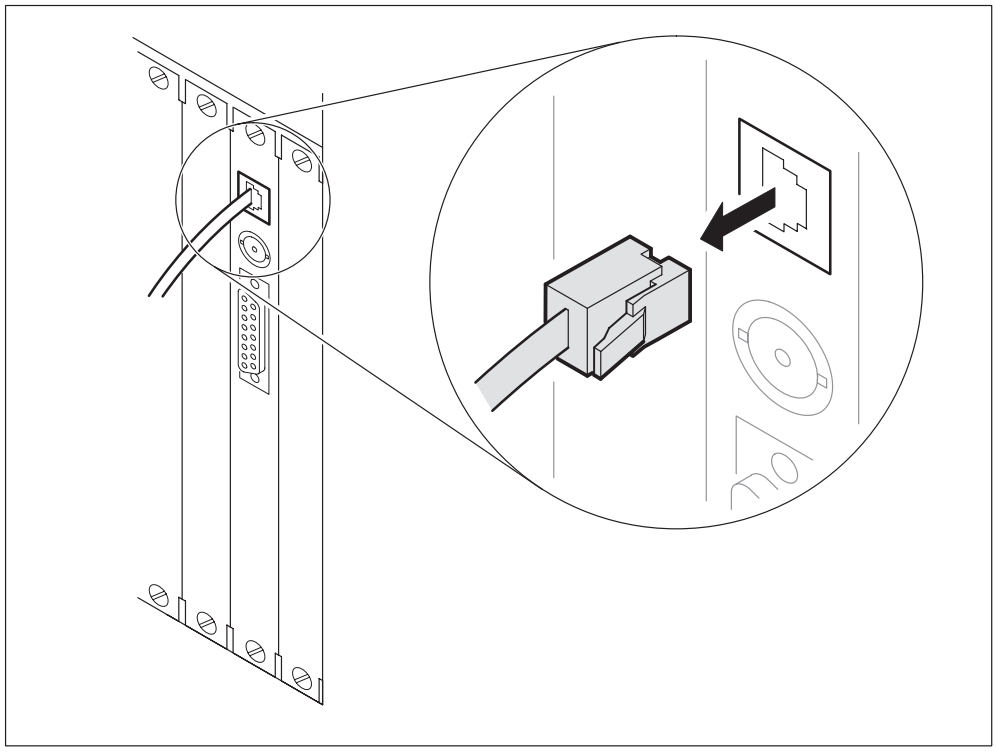
17 While grasping the thumbscrews, carefully pull the DS512 personality module toward you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



18 Place the DS512 personality module you have removed in an ESD protective container.

Adding an I/O expansion chassis (NTRX50EC) (continued)

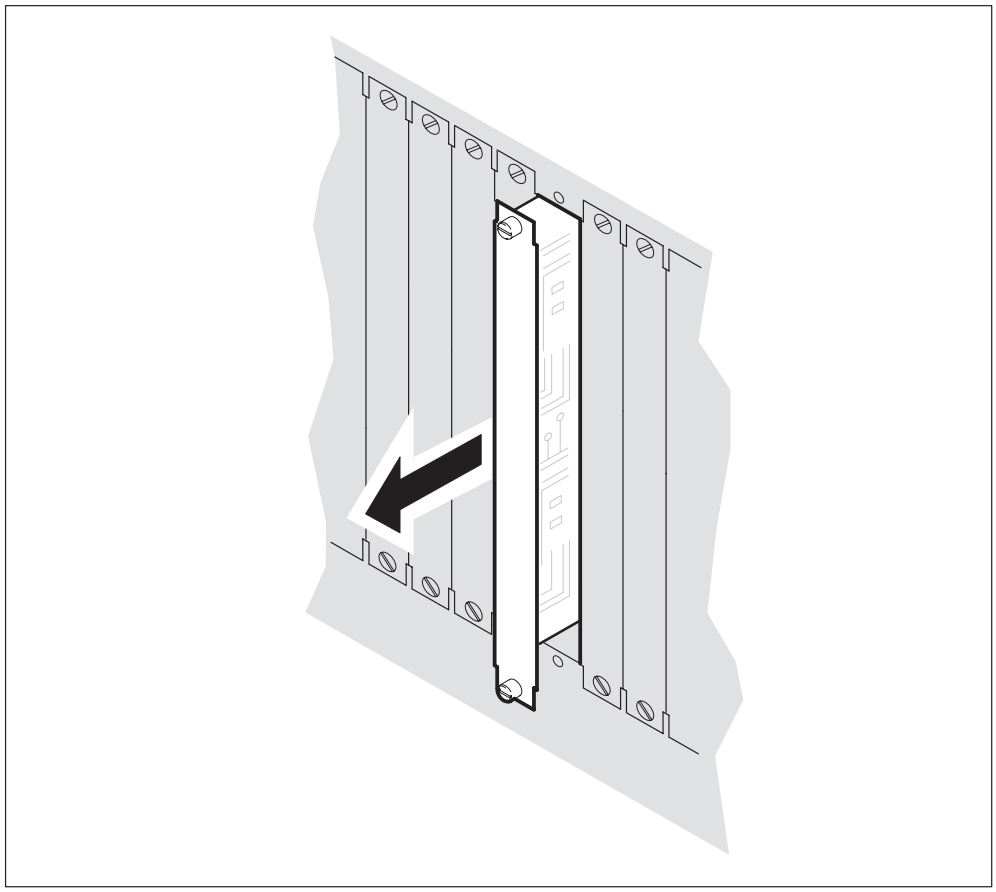
19 Disconnect the 10BASE-T cable from the LAN personality module (located in slot 2), as shown in the following diagram.



20 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module.

Adding an I/O expansion chassis (NTRX50EC) (continued)

21 While grasping the thumbscrews, carefully pull the LAN personality module toward you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



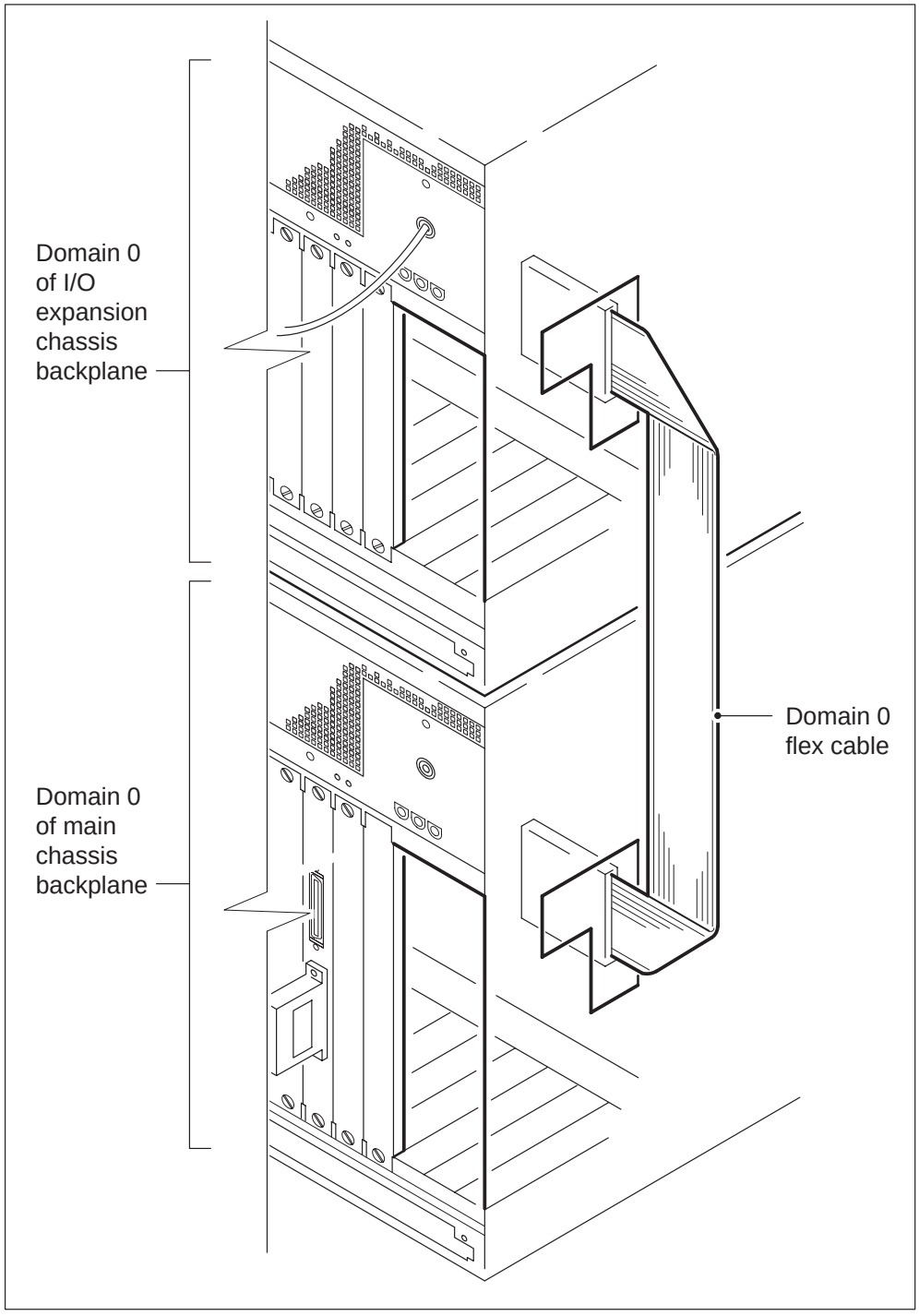
22 Place the LAN personality module you have removed in an ESD protective container.

23 Remove the filler plate in slot 3.

24 Remove the domain 0 flex cover that runs from the outside of the main and I/O expansion chassis.

25 Connect the domain 0 flex cable (NTRX5088) to the I/O expansion chassis back plane side 0. Route the cable correctly and plug it into the connector on the main chassis of the domain 0 backplane.

Adding an I/O expansion chassis (NTRX50EC) (continued)



26 Install flex cable covers on the flex cable to protect the cable from damage.

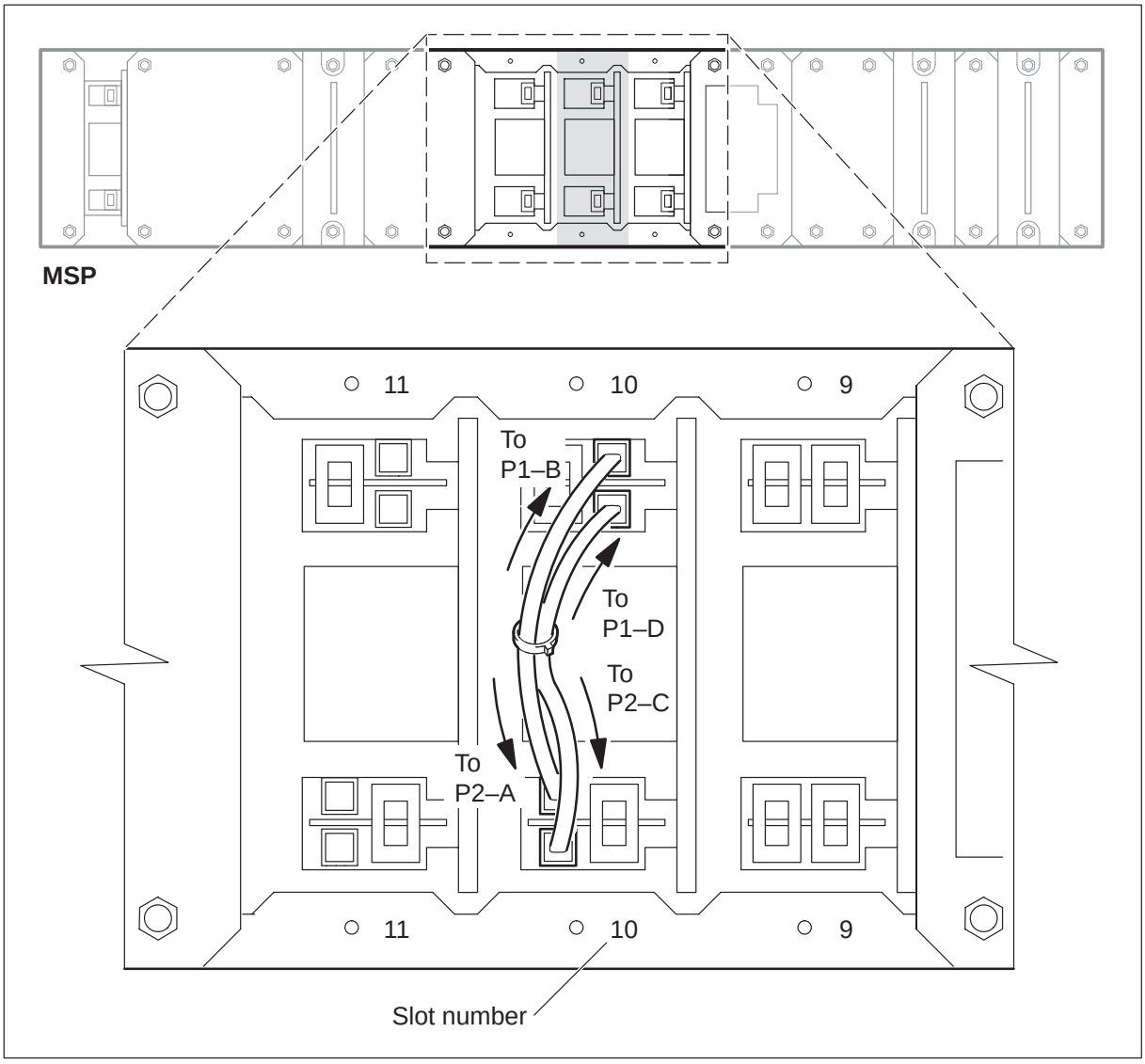
Adding an I/O expansion chassis (NTRX50EC) (continued)

At the back of the MSP

27 Connect the power jumper cable (NTRX5054) to slot 10 of the MSP in the following order:

- P1–D to P2–C
- P1–B to P2–A

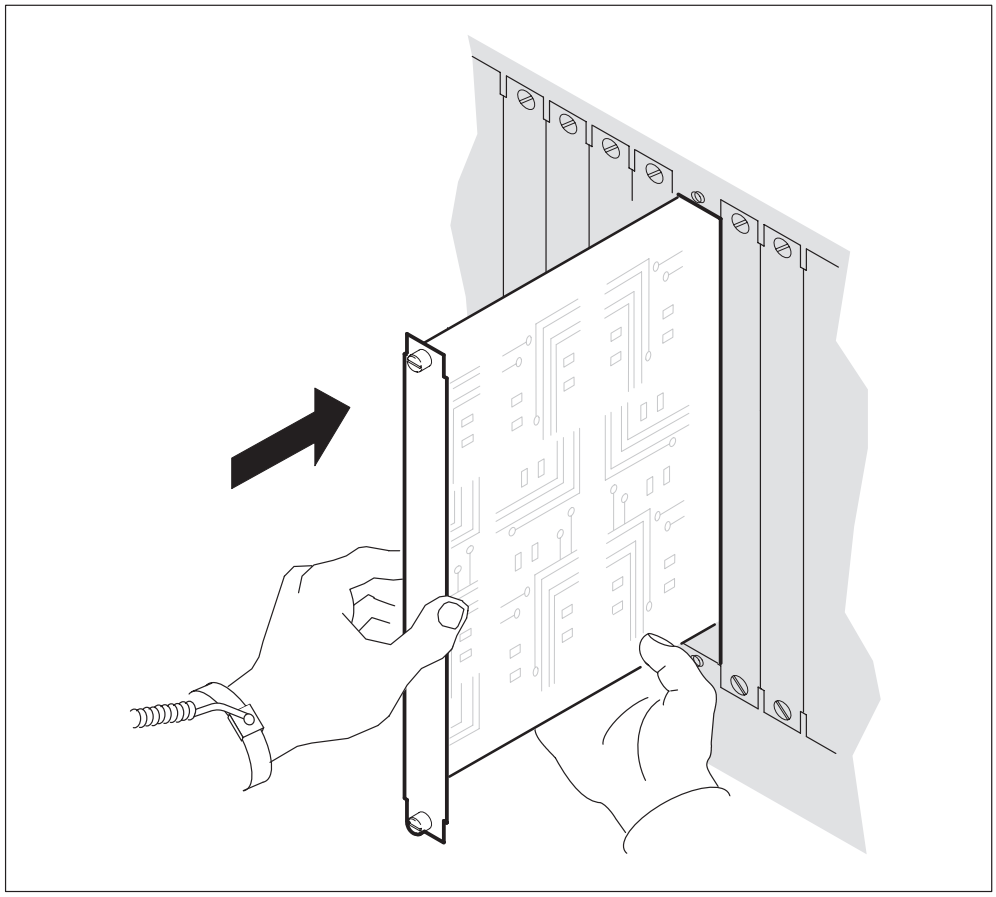
Note: The power jumper cable is already connected to P1 connector. The other end is tied.



Adding an I/O expansion chassis (NTRX50EC) (continued)

At the back of the SDM

28 Carefully slide the DS512 personality module into slot 1 of the shelf until it is fully inserted.



29 Tighten the thumbscrews at the top and the bottom of the DS512 personality module.

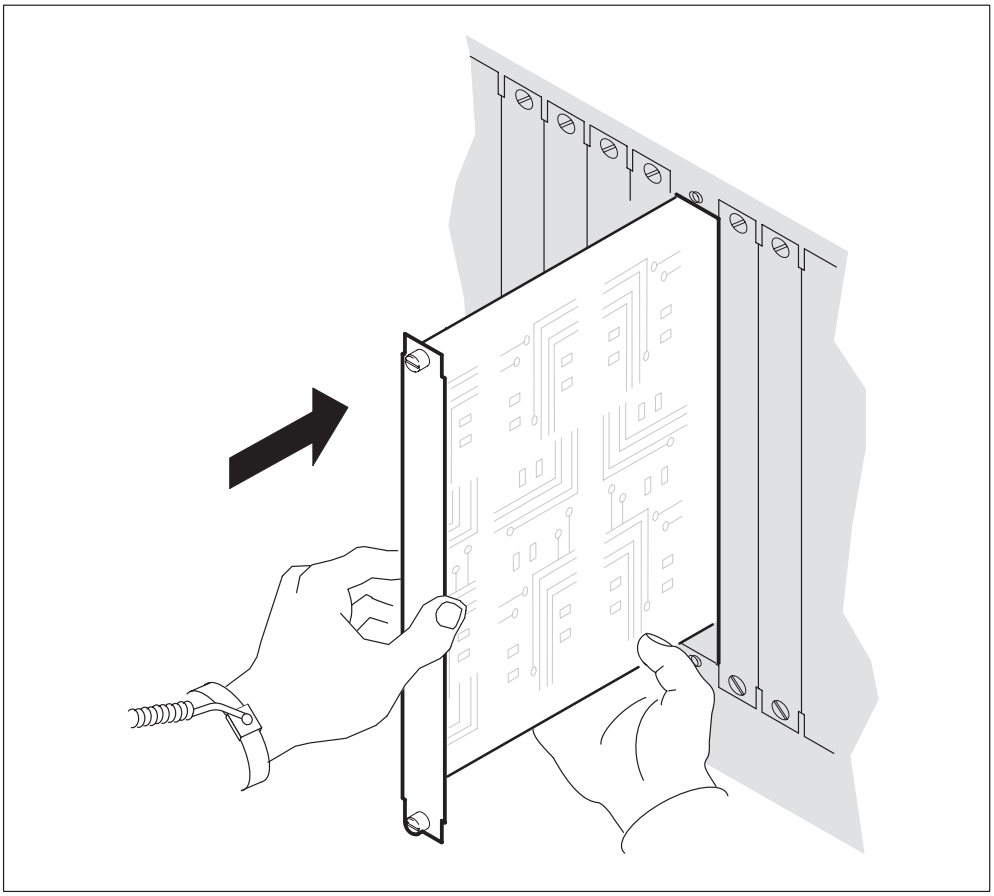
Adding an I/O expansion chassis (NTRX50EC) (continued)

30

CAUTION
Reconnecting transmit and receive cables
Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the right.

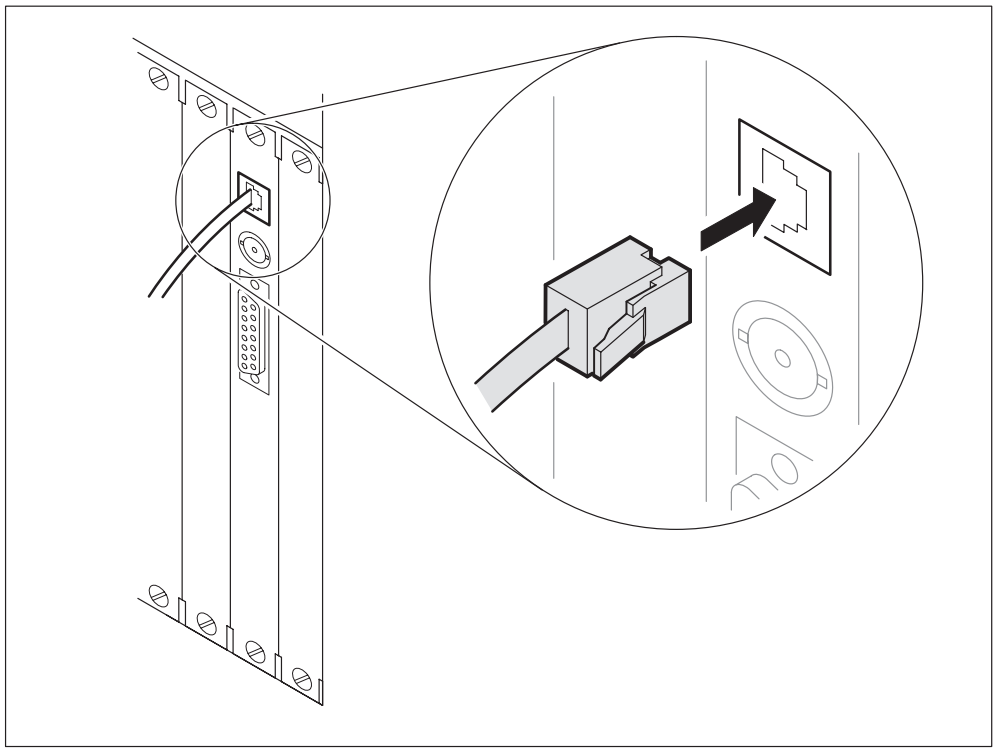
31 Carefully slide the LAN personality module into the slot 2 until it is fully inserted.



32 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

Adding an I/O expansion chassis (NTRX50EC) (continued)

33 Reconnect the 10BASE-T cable to the LAN personality module.



34 Reconnect the power cable to ICM 0 in the main chassis, and to ICM 0 in the I/O expansion chassis.

35 Reconnect the alarm cable to the main chassis.

At the front of the MSP

36 Turn on power to SDM domain 0 by turning on both breakers in slot 10 of the MSP.

Adding an I/O expansion chassis (NTRX50EC) (continued)

At the local or remote VT100 console

37 At the hardware menu level of the RMI, return the ICM 0 to service, by typing

>RTS 0 ICM

and pressing the Enter key

Response:

```
Hardware RTS : Domain 0 Device ICM – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device ICM – Command submitted.
```

38 Allow about 20 min for the interconnect modules to reintegrate. New columns are added at the RMI for the ICM and the fans in the I/O expansion chassis. The display at the RMI changes to a dot (.), indicating that the modules are in service.

Example response

```
SDM Node State:             InSv
SDM Hardware State:         InSv

          I I F C E D D 5
          C C A P T S A 1
          M M N U H K T 2
          1 2
Domain 0  . M . . . . . .
Domain 1  . - . . . . . .
```

Adding an I/O expansion chassis (NTRX50EC) (continued)

39 Return ICM 2 to service by typing

>RTS 0 ICM2
and pressing the Enter key.

Response:

```
Hardware RTS : Domain 0 Device ICM2 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device ICM2 – Command submitted.
```

40 Allow about 20 min for the interconnect modules to reintegrate. New columns are added at the RMI for the ICM and the fans in the I/O expansion chassis. The display at the RMI changes to a dot (.), indicating that the modules are in service.

Example response

```
SDM Node State:             InSv
SDM Hardware State:         InSv

          I I F F C E D D 5
          C C A A P T S A 1
          M M N N U H K T 2
          1 2 1 2
Domain 0 . M . M . . . . .
Domain 1 . - . - . . . . .
```

41 Return FAN 2 to service by typing

>RTS 0 FAN2
and pressing the Enter key.

Response:

```
Hardware RTS : Domain 0 Device FAN2 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device FAN2 – Command submitted.
```

Note: At the hardware menu level of the RMI, ICM 2 and FAN 2 change to in service, indicated by a dot (.).

Adding an I/O expansion chassis (NTRX50EC) (continued)

42 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

43 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response

```
Disk mirroring (rootvg):                  Integrating
  Volume              Size(MB)      (% full/ threshold)
 1  /                    20                   79/ 80
 2  /usr                 192                  87/ 90
 3  /var                 40                   46/ 90
 4  /tmp                 20                   16/ 90
 5  /home                300                  81/ 90
(unallocated)            692

Disk mirroring (datavg):                   Integrating
   Volume             Size(MB)       (% full/ threshold)
 7 /data/sba             1008                  66/ 80
(unallocated)            11168
```

44 Wait until rootvg and datavg, if applicable, are Mirrored. This may take up to 2 hours. If this problem persists, contact your next level of support.

45 Access the hardware menu level of the RMI by typing

>HW
and pressing the Enter key.

46 Manually busy the ICM in domain 1 by typing

>BSY 1 ICM1
and pressing the Enter key.

Response:

```
Hardware Bsy – Domain 1 Device ICM1
This action will affect all devices in I/O domain 1.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

47 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

Note: When you manually busy ICM 1, all subtending devices in domain 1 are also put in the C-side Bsy state.

Adding an I/O expansion chassis (NTRX50EC) (continued)

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

Response:

```
Hardware Bsy : Domain 1 Device ICM – Command initiated.
Please wait...
```

Several warnings are displayed. The “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Response:

```
Hardware Bsy : Domain 1 Device ICM – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the interconnect module changes and all subtending devices changes to “C”. The out-of-service LED on the module is on (red).

Example response

```
SDM Node State:              ManB
SDM Hardware State:          ManB

          I I F F C E D D 5
          C C A A P T S A 1
          M M N N U H K T 2
          1 2 1 2
Domain 0 . . . . . . . . . .
Domain 1 M - C - . C C C C
```

49 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

50 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Adding an I/O expansion chassis (NTRX50EC) (continued)

Example response

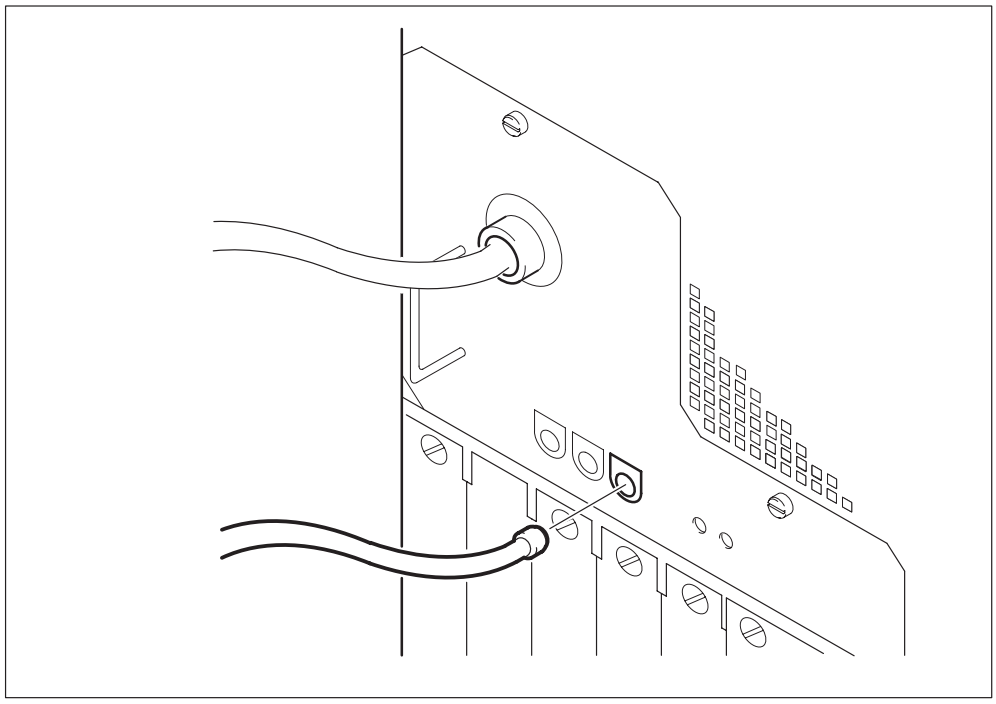
```
Disk mirroring (rootvg):                    Not Mirrored
  Volume              Size(MB)        (% full/ threshold)
 1  /                    20                   79/ 80
 2  /usr                 192                  87/ 90
 3  /var                 40                   46/ 90
 4  /tmp                 20                   16/ 90
 5  /home                300                  81/ 90
(unallocated)            692

Disk mirroring (datavg):                    Not Mirrored
   Volume              Size(MB)         (% full/ threshold)
 7 /data/sba            1008                   66/ 80
(unallocated)           11168
```

51 Wait until the status of rootvg and datavg, if applicable, is Not Mirrored.

At the front of the MSP

52 Turn off power to SDM domain 1 by turning off both breakers in slot 11 of the MSP.

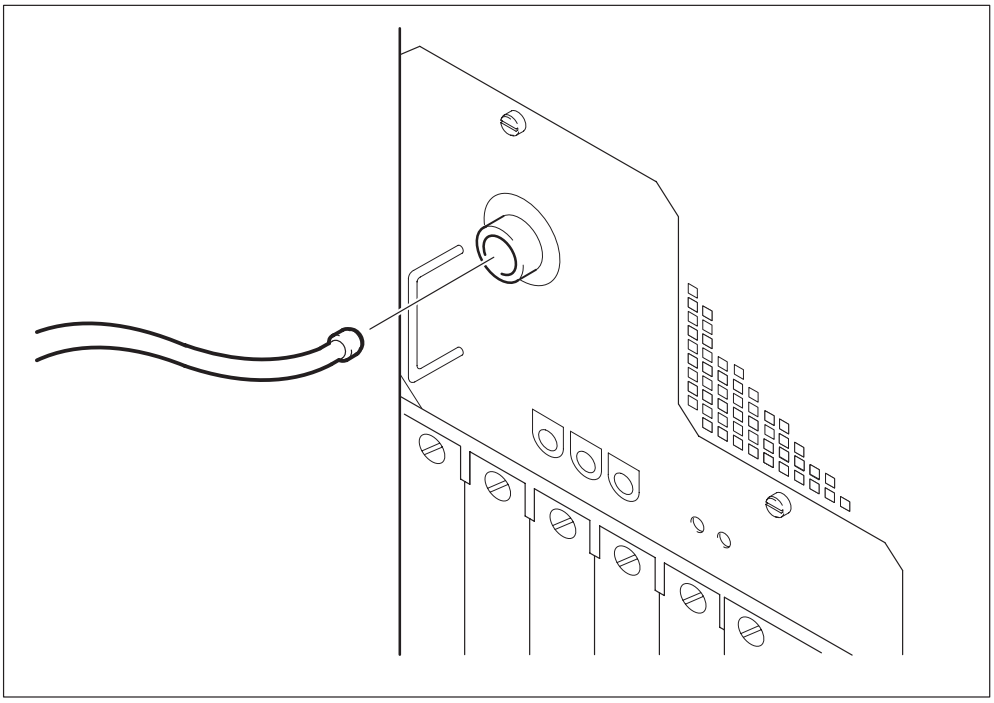
53 Disconnect the alarm cable from ICM 1.



Adding an I/O expansion chassis (NTRX50EC) (continued)

54 Disconnect the power cable from ICM 1.

CAUTION
Potential service interruption
Ensure that you disconnect the power cable from ICM 1. If you disconnect the power cable to the remaining in-service ICM (ICM 0), the entire SDM shuts down.



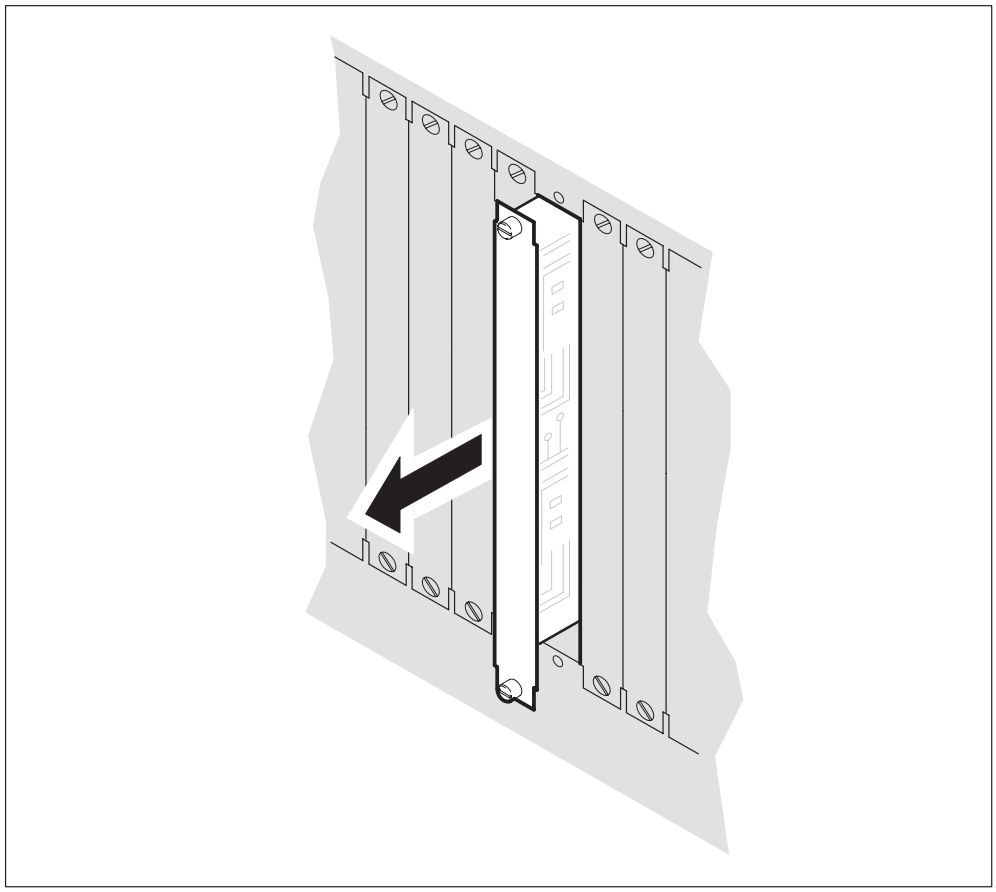
55 Proceed depending on whether your system has a LAN personality module mounted in slot 15 at the back of the main chassis.

If your system	Do
has a LAN personality module in slot 15	step 56
does not have a LAN personality module in slot 15	step 59

56 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module (located in slot 15).

Adding an I/O expansion chassis (NTRX50EC) (continued)

57 While grasping the thumbscrews, carefully pull the LAN personality module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



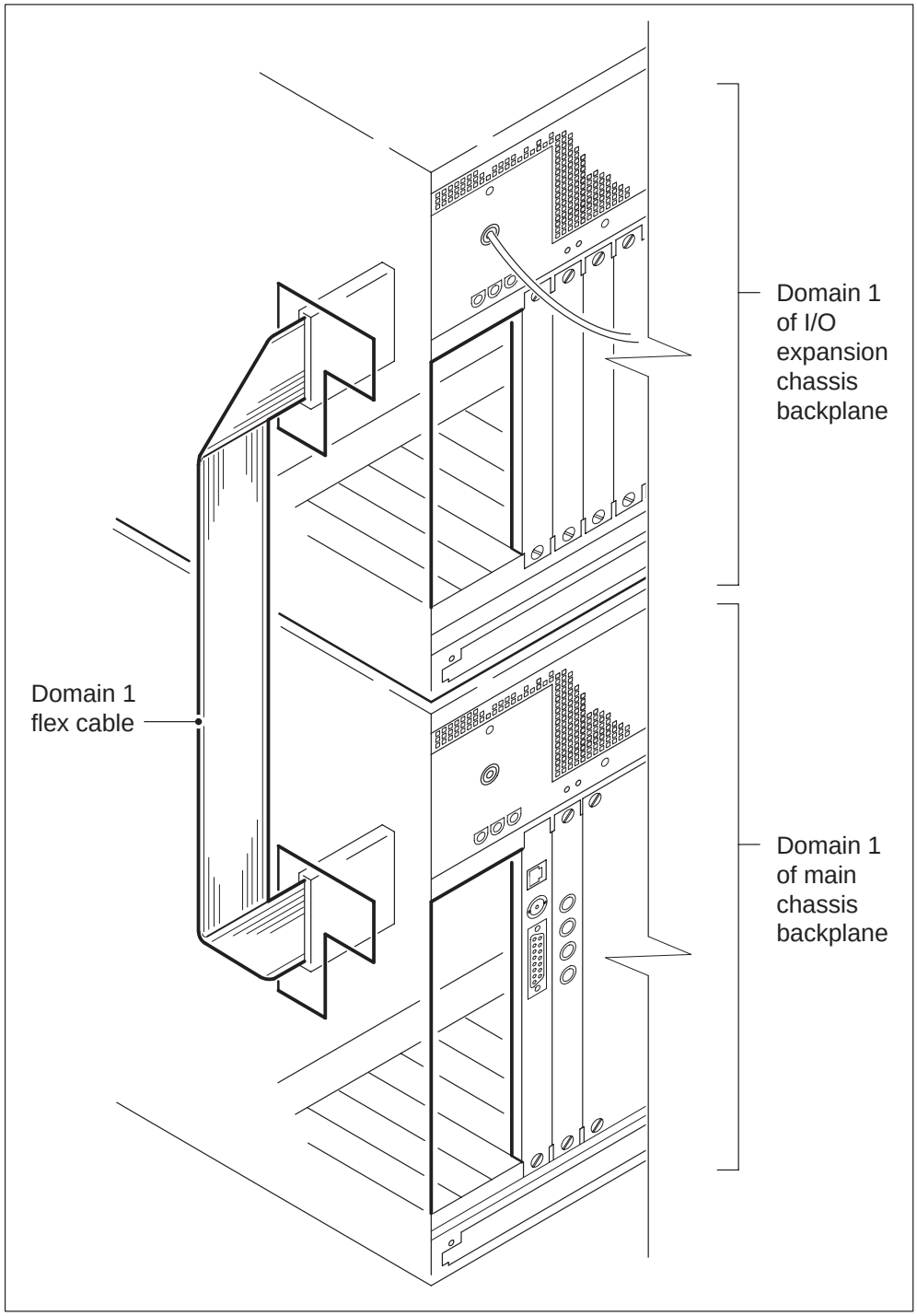
58 Place the LAN personality module you have removed in an ESD protective container.

59 Remove the filler plates in slots 14, 15 (if applicable) and 16.

60 Remove the domain 1 flex cover that runs from the outside of the main and I/O expansion chassis.

61 Connect the domain 1 flex cable (NTRX5089) to the I/O expansion chassis backplane side 1. Route the cable correctly and plug it into the connector on the main chassis of the domain 1 backplane.

Adding an I/O expansion chassis (NTRX50EC) (continued)



62 Install flex cable covers on the flex cable to protect the cable from damage.

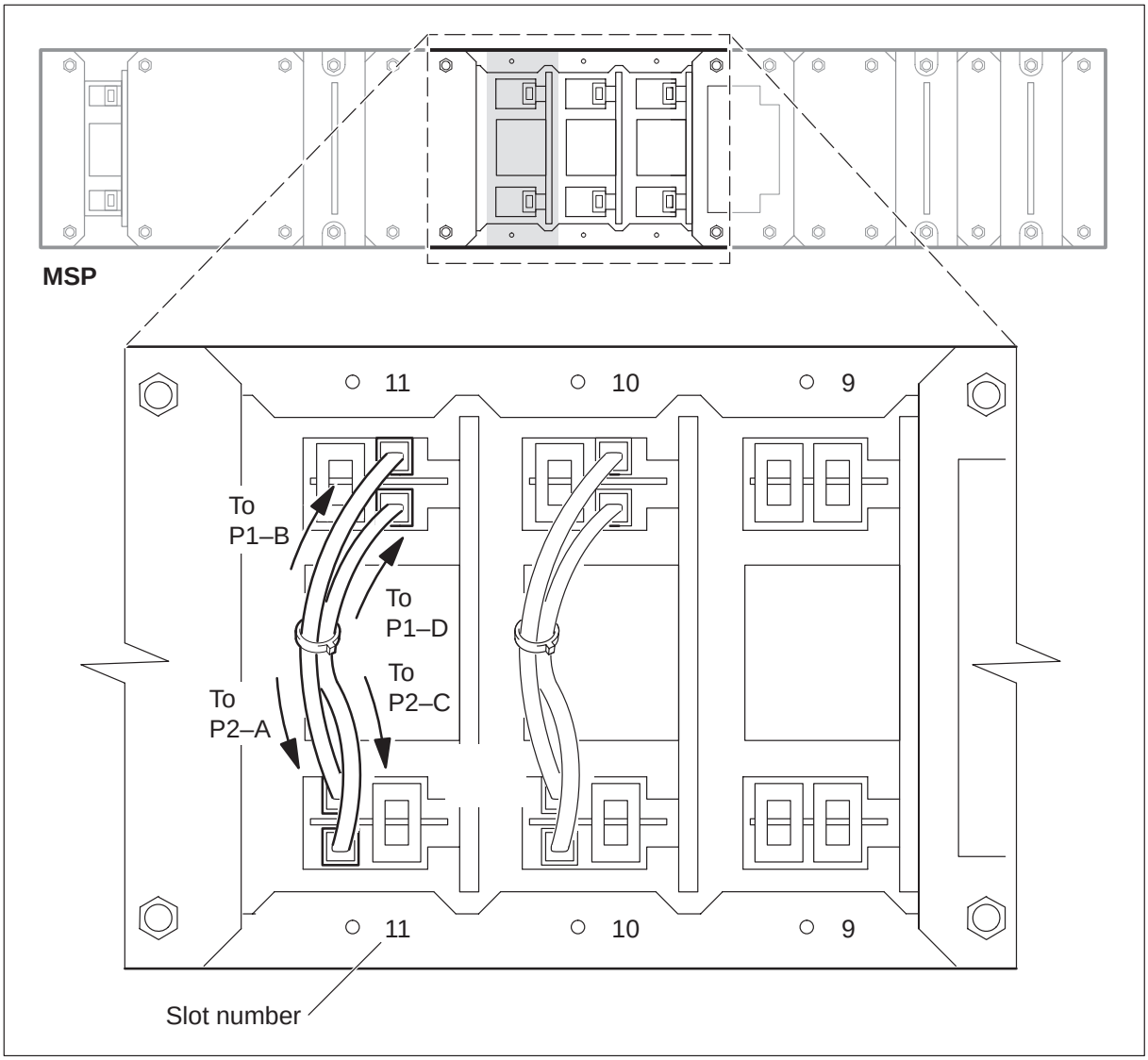
Adding an I/O expansion chassis (NTRX50EC) (continued)

At the back of the MSP

63 Connect the power jumper cable (NTRX5054) to slot 11 of the MSP in the following order:

- P1–D to P2–C
- P1–B to P2–A

Note: The power jumper cable is already connected to P1 connector. The other end is tied.



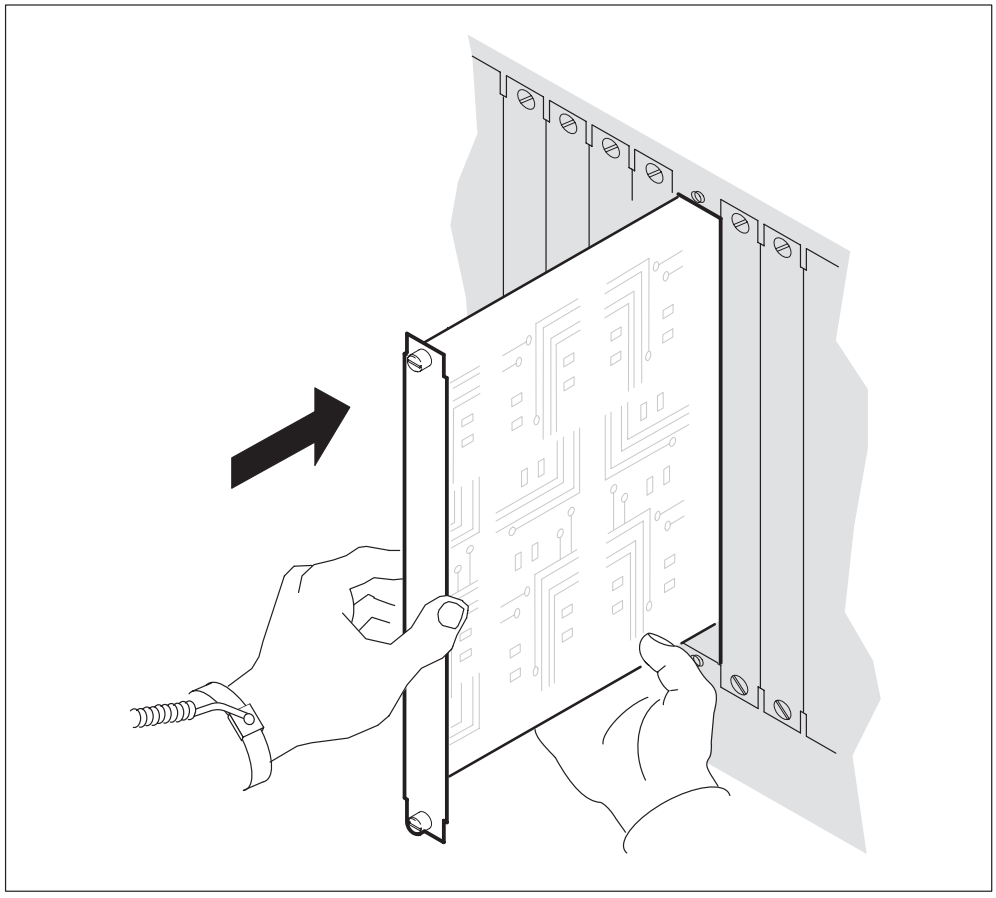
Adding an I/O expansion chassis (NTRX50EC) (continued)

64 Proceed depending on whether you removed a LAN personality module mounted from slot 15 at the back of the main chassis.

If you	Do
removed a LAN personality module from slot 15	step 65
did not remove a LAN personality module from slot 15	step 67

At the back of the SDM

65 Carefully slide the LAN personality module into the shelf until it is fully inserted.



66 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

67 Reinstall the filler plates in slots 14, 15 (if applicable) and 16.

Adding an I/O expansion chassis (NTRX50EC) (continued)

68 Reconnect the power cable to ICM 1 in the main chassis, and to ICM 1 in the I/O expansion chassis.

69 Reconnect the alarm cable to the main chassis.

At the front of the MSP

70 Turn on the power to SDM domain 1 by turning on both breakers in slot 11 of the MSP.

At the local or remote VT100 console

71 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

72 Return the ICM1 to service, by typing

>RTS 1 ICM1
and pressing the Enter key.

Response:

```
Hardware RTS : Domain 1 Device ICM1 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 1 Device ICM1 – Command submitted.
```

73 Allow about 20 min for the interconnect modules to reintegrate. New columns are added at the RMI for the ICM and the fans in the I/O expansion chassis. The display at the RMI changes to a dot (.), indicating that the modules are in service.

Example response

```
SDM Node State:             InSv
SDM Hardware State:         InSv

          I I F C E D D 5
          C C A P T S A 1
          M M N U H K T 2
          1 2
Domain 0 . . . . . . . .
Domain 1 . M . . . . . .
```

Adding an I/O expansion chassis (NTRX50EC) (continued)

74 Return ICM 2 to service by typing

>RTS 1 ICM2
and pressing the Enter key.

Response:

```
Hardware RTS : Domain 1 Device ICM2 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 1 Device ICM2 – Command submitted.
```

75 Allow about 20 min for the interconnect modules to reintegrate. New columns are added at the RMI for the ICM and the fans in the I/O expansion chassis. The display at the RMI changes to a dot (.), indicating that the modules are in service.

Example response

```
SDM Node State:             InSv
SDM Hardware State:         InSv

          I I F F C E D D 5
          C C A A P T S A 1
          M M N N U H K T 2
          1 2 1 2
Domain 0 . M . – . . . . .
Domain 1 . - . . . . . .
```

76 Return FAN 2 to service by typing

>RTS 1 FAN2
and pressing the Enter key.

Response:

```
Hardware RTS : Domain 1 Device FAN2 – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 1 Device FAN2 – Command submitted.
```

Note: At the hardware menu level of the RMI, ICM 2 and FAN 2 change to in service, indicated by a dot (.).

Adding an I/O expansion chassis (NTRX50EC) (end)

77 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

78 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response

```
Disk mirroring (rootvg):                    Not Mirrored
  Volume              Size(MB)      (% full/ threshold)
 1  /                    20                   79/ 80
 2  /usr                 192                  87/ 90
 3  /var                 40                   46/ 90
 4  /tmp                 20                   16/ 90
 5  /home                300                  81/ 90
(unallocated)            692

Disk mirroring (datavg):                    Not Mirrored
   Volume              Size(MB)       (% full/ threshold)
 7 /data/sba              1008                 66/ 80
(unallocated)            11168
```

79 Wait until rootvg and datavg, if applicable, are Mirrored. This may take up to 2 hours. If this problem persists, contact your next level of support.

80 You have completed this procedure.

Changing system thresholds

Application

Use this procedure to change SDM system thresholds. You can change the following SDM system thresholds at the system menu level of the Remote Maintenance Interface (RMI):

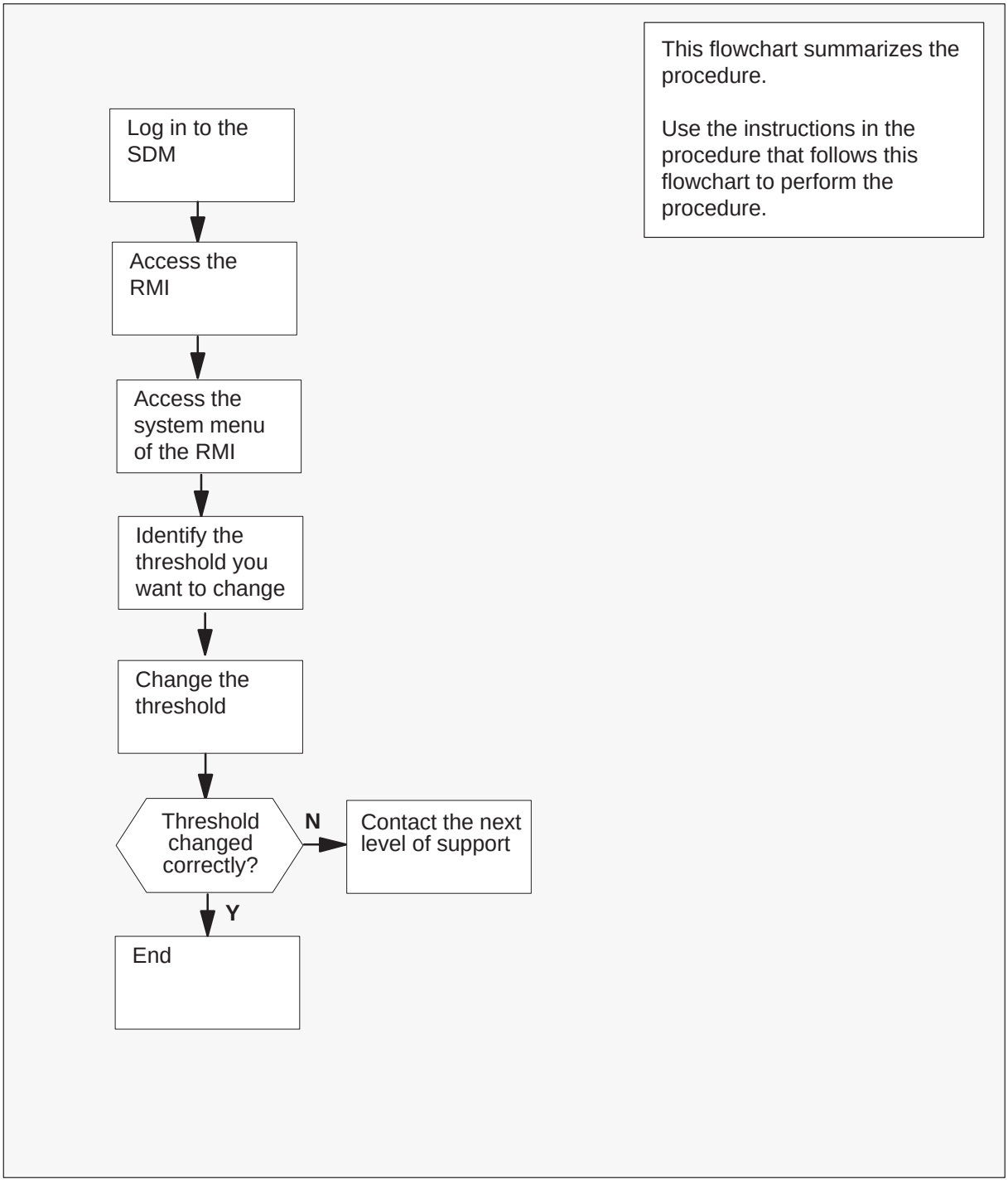
- CPU (run queue entries)
- Number of Processes
- Number of Zombies
- Swap Space (% full)
- Number of Swap Queue Entries

Action

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

Changing system thresholds (continued)

Summary of Changing system thresholds



Changing system thresholds (continued)

Changing system thresholds

At the local VT100 console

1 Log in to the SDM.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

Response:

```
SDM Node State:               ISTb
SDM System State:             ISTb
SDM Storage State:            InSv
Automated Incremental Backup:  Completed on 11/16/97

# Description                           Current/Threshold
1 CPU (run queue entries):                   1/  5
2 Number of Processes:                      63/250
3 Number of Zombies:                         0/  3
4 Swap Space (% full):                      72/ 70*
5 Number of Swap Queue Entries:              0/  2
```

4 Identify which system threshold you want to change. Note the entry number of the system threshold on the left of the RMI System menu. The number is shown under the header “#”.

In the example in step 3, the entry number for CPU threshold is 1. The entry number for the Number of Processes threshold is 2. The entry number for the Number of Zombies is 3. The entry number for the Swap Space threshold is 4 and the entry number for Number of Swap Queue Entries is 5.

The current threshold value is shown under the header “Current/Threshold”.

Changing system thresholds (end)

5 Change the system threshold by typing

>CHANGE n n1
and pressing the Enter key.

where

n is the entry number of the threshold you want to change

n1 is the new threshold value

Example input:

>CHANGE 4 80

Note: Here, the threshold for “Swap Space” changes from 70 to 80.

Example response:

```
SDM Node State:               InSv
SDM System State:             InSv
SDM Storage State:            InSv
Automated Incremental Backup:  Completed on 11/16/97

# Description                            Current/Threshold
1 CPU (run queue entries):                    1/  5
2 Number of Processes:                       63/250
3 Number of Zombies:                          0/  3
4 Swap Space (% full):                       72/ 80
5 Number of Swap Queue Entries:               0/  2

Command submitted.
```

6 Wait 5 min. Check to see that the system threshold changed to the value that you entered.

If the system threshold did not change correctly, contact the personnel responsible for the next level of support.

7 You have completed this procedure.

Changing logical volume thresholds

Application

Use this procedure to change SDM logical volume thresholds. You can change the following SDM logical volume thresholds at the storage level of the Remote Maintenance Interface (RMI):

- /
- /usr
- /var
- /tmp
- /home
- /sdm

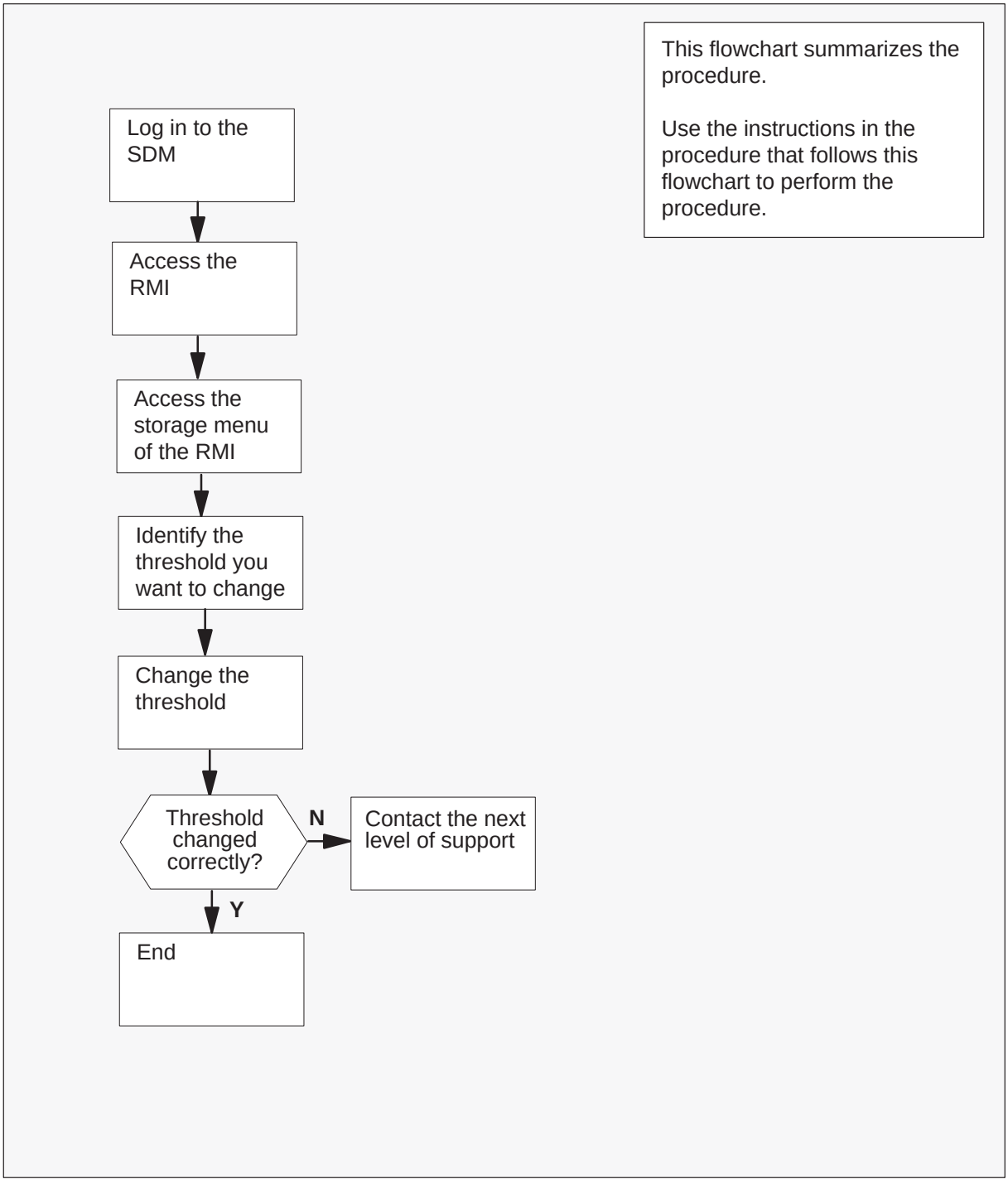
You can also change logical volume thresholds added by operating company personnel.

Action

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

Changing logical volume thresholds (continued)

Summary of Changing logical volume thresholds



Changing logical volume thresholds (continued)

Changing system thresholds

At the local VT100 console

1 Log in to the SDM.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level of the RMI by typing

>STORAGE
and pressing the Enter key.

Response:

```
SDM Node State:               ISTb
SDM System State:             ISTb
SDM Storage State:            ISTb

Disk mirroring (rootvg):                          Mirrored
   Volume             Size (MB)        (% full/ threshold)
 1 /                     240                      52/ 80
 2 /usr                  204                      82/ 90
 3 /var                  40                       35/ 70
 4 /tmp                  24                       21/ 90
 5 /home                 304                      75/ 70*
 6 /sdm                  304                      47/ 90
 7 /home/sba             16                        7/ 80
(unallocated)            608
```

4 Identify which logical volume threshold you want to change. Note the entry number of the logical volume threshold on the left of the RMI System menu. The number is shown under the header “#”.

The current threshold value is shown under the header “Current/Threshold” .

Changing logical volume thresholds (end)

5 Change the logical volume threshold by typing

>CHANGE n n1
and pressing the Enter key.

where

n is the entry number of the threshold you want to change

n1 is the new threshold value

Example input:

>CHANGE 5 80

Note: The threshold for "/home" has changed from 70 to 80.

Example response:

```
SDM Node State:               InSv
SDM System State:             InSv
SDM Storage State:            InSv

Disk mirroring (rootvg):                          Mirrored
   Volume             Size (MB)        (% full/ threshold)
 1 /                     240                      52/ 80
 2 /usr                  204                      82/ 90
 3 /var                  40                       35/ 70
 4 /tmp                  24                       21/ 90
 5 /home                 304                      75/ 80
 6 /sdm                  304                      47/ 90
 7 /home/sba             16                        7/ 80
(unallocated)            608
```

6 Wait 5 min. Check to see that the logical volume threshold changed to the value that you entered.

If the logical volume threshold did not change correctly, contact the personnel responsible for the next level of support.

7 You have completed this procedure.

Changing the time interval for performance log SDM620

Application

Use this procedure to change the time interval for performance log SDM620. Log report SDM620 reports the following examples of current SDM system performance data:

- CPU use
- number of processes
- system thresholds for swap space occupancy
- logical volume capacities

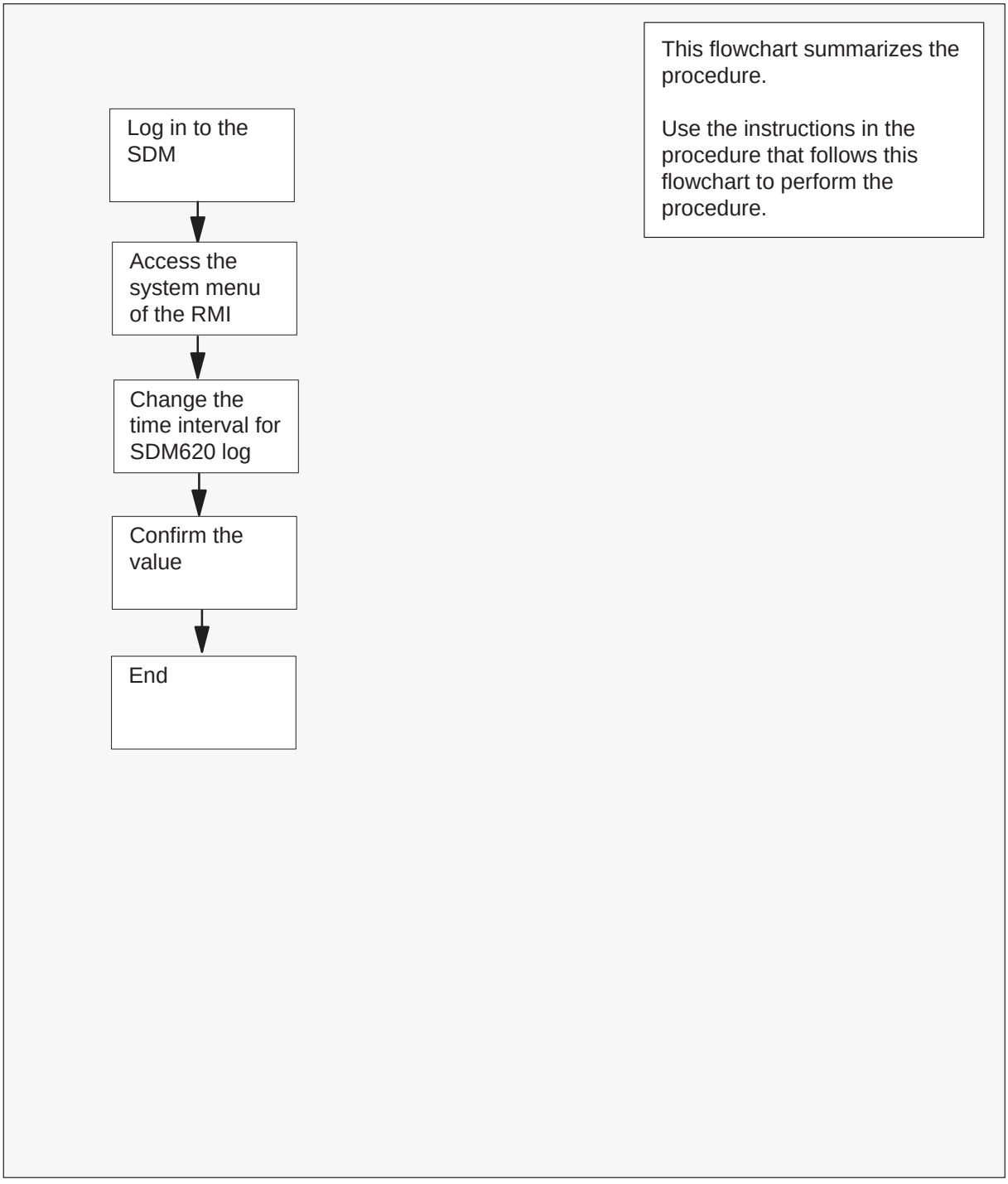
The time interval defines how frequently the SDM generates the SDM620 log report.

Action

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

Changing the time interval for performance log SDM620 (continued)

Summary of Changing the time interval for performance log SDM620



Changing the time interval for performance log SDM620 (continued)

Changing the time interval for performance log SDM620

At the local VT100 console

1 Log in to the SDM as the root user.

2 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

Response:

```
SDM Node State:            ISTb
SDM System State:             InSv
SDM Storage State:           InSV
Automated Incremental Backup:  Completed on 11/16/97

# Description                              Current/Threshold
1 CPU (run queue entries):                      1/ 5
2 Number of Processes:                         63/250
3 Number of Zombies:                             0/250
4 Swap Space (% full):                         16/ 70
5 Number of Swap Queue Entries:                 0/  2

Command submitted.
```

4 Check the performance log interval value by typing

>QUERYSDM
and pressing the Enter key 3 times.

Response:

```
System Indicator Thresholds       (threshold/default)
--------------------------------------------------
Number of events before log:         4
CPU (Run Queue Entries):             12
Number of Processes:                 250
Number of Zombies:                   3
Swap Space (% full):                 70
Number of Swap Queue Entries:        2

Performance Log Time Interval:        5
```

Note: In the preceding response, the performance log time interval is 5.

Changing the time interval for performance log SDM620 (continued)

5 Change the Performance Log Time Interval by typing

>CHANGE TI
and pressing the Enter key.

Response:

```
Time Interval:  5
```

Note: The system displays the current time interval value. In the preceding response, the time interval is the default value of 5.

6 Enter the Performance Log Time Interval value by typing

>n
and pressing the Enter key.

where

n is the value in minutes. The valid range for this field is 5 to 20 160 (14 days) min. The default value is 5 min. The system will not let you enter a value less than 5 min.

Response:

```
Values to be changed:
Performance Log Time Interval:  6 minutes
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

7 Decide if you want to confirm the value you entered.

If you want to	Do
confirm the value	step 8
reject the value	step 9
edit the value	step 10

8 Confirm the value by typing

>Y
and pressing the Enter key.

Response:

```
Change Time Interval – Command initiated.
Please wait...


Change Time Interval – Command initiated.
```

Go to step 12.

Changing the time interval for performance log SDM620 (end)

9 Reject the value by typing

>N
and pressing the Enter key.

Response:

```
Change Time Interval – Command cancelled.
```

Go to step 12.

10 Edit the value by typing

>E
and pressing the Enter key.

Response:

```
Time Interval: 6
```

Note: The system displays the current time interval value. In the preceding response, the time interval value is 6.

11 Enter the time interval value by typing

>n
and pressing the Enter key.

where

n is the time interval value. The time interval value must be entered in minutes. The valid range for this field is 5 to 20 160 (14 days) min. The default value is 5 min.

Response:

```
Values to be changed:
Performance Log Time Interval:  6 minutes
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

Return to step 7.

12 You have completed this procedure.

SDM hardware replacement procedures

Introduction to SDM hardware replacement procedures

WARNING
SDM hardware warranty
This chapter only describes how to replace SDM hardware. Do not attempt to open or disassemble any SDM hardware modules. This may damage SDM hardware, and violates the SDM product warranty.

CAUTION
System damage
Do not plug in any hardware modules that will not be used. Extra modules may confuse the system after a reboot or an installation from tape.

This chapter contains SDM hardware replacement procedures. Each procedure contains the following:

- explanatory and context-setting information
- summary flowchart
- step-action instructions

Explanatory and context-setting information

The first page of each procedure contains the following headings:

- Application (why you would perform the procedure)
- Action (how to use the flowchart and step-action instructions)

Summary flowchart

The flowchart is only a summary of the main actions, decision points, and possible paths you may take. Do not use the summary flowchart to perform the procedure. Instead, use it to preview what you will be doing and to

prepare for it. For example, if you see that these instructions involve another office, you will know to advise that office before you begin the step-action instructions.

Step-action instructions

The step-action instructions tell you how to perform the procedure. Normally you will perform the steps in order, but you may be directed to return to a previous step and repeat a sequence. The successful completion of a step may depend on previous steps; therefore, always perform the steps in the order specified.

While following the step-action instructions, you may be sent to other procedures of this book to perform a set of instructions, or to another NTP for a related procedure. If this happens, you will be told when to return to the original instructions, and to which point in those instructions you should go.

The step-action instructions provide the command syntax and system information you use or see while performing the procedure. For help on DMS and SDM commands or output, see the "About this document" chapter at the beginning of this document.

Return key and Enter key

The carriage return key is identified in different ways (such as Enter, Return or Carriage Return) on various types of terminals. It is always used to enter commands and parameters into the system.

The procedures contained in this book and in other NTPs instruct you to press the Enter key after each step. If your terminal has a Return key, press the Return key instead. Do not press the Enter key located beside the numeric key pad.

NTRX50FD
CPU personality module

Application

Use this procedure to replace the CPU personality module, located at the rear of the main chassis (slot 6) of a fault-tolerant SDM.

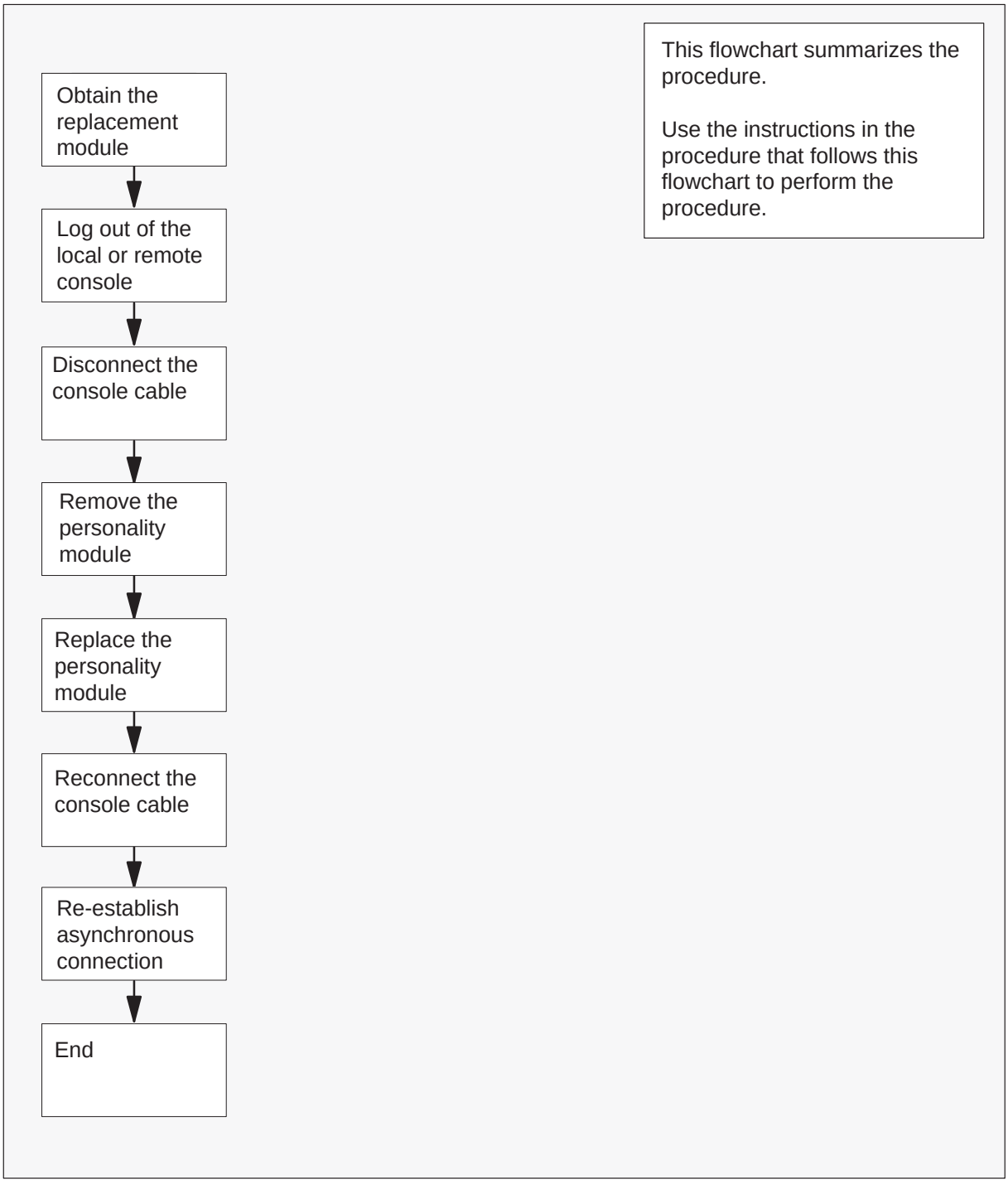
Nortel PEC	Name
NTRX50FD	CPU personality module

Action

The following flowchart is only a summary of the procedure. To replace the CPU personality card, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FD
CPU personality module (continued)

Summary of Replacing a CPU personality module



NTRX50FD
CPU personality module (continued)

Replacing a CPU personality module

1 Obtain a replacement CPU personality module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written at the top of the module.

At the local or remote VT100 console

2 If you are logged in to the local or remote console, log out by typing

>logout
and pressing the Enter key.

3

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

At the back of the SDM

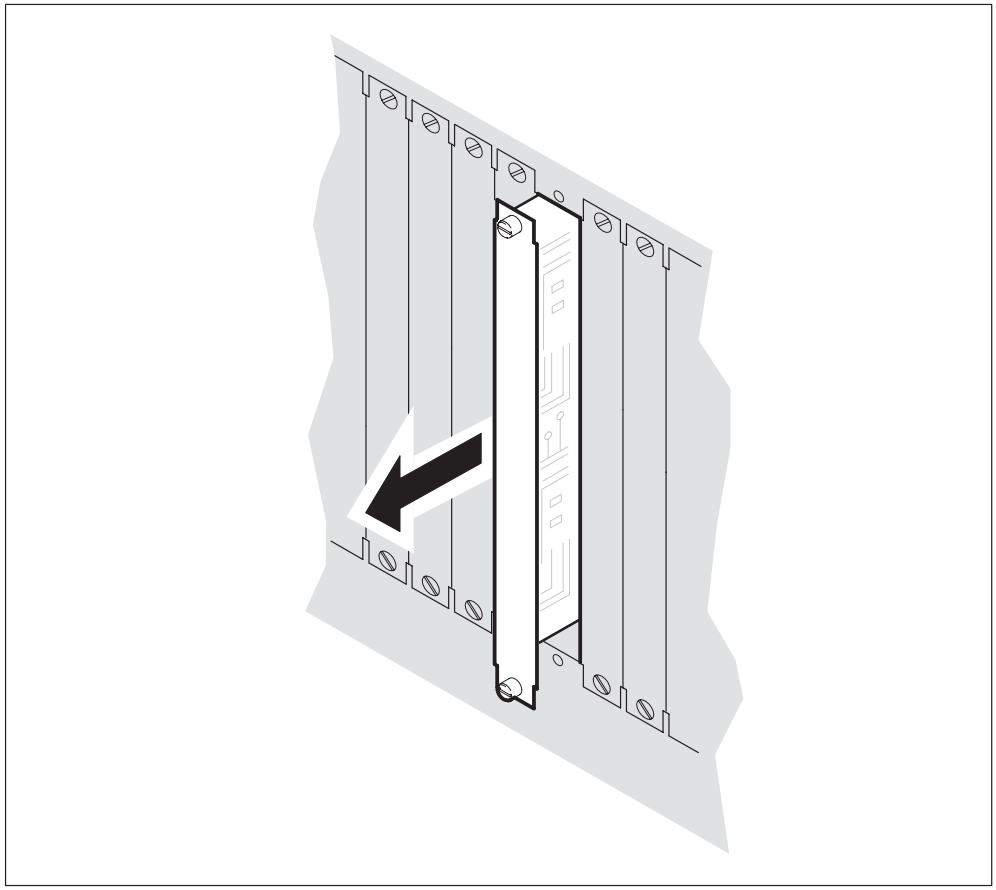
4 Disconnect the console cable (labelled SP0) connected to the CPU personality module.

5 Loosen the two thumbscrews located at the top and bottom of the CPU personality module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

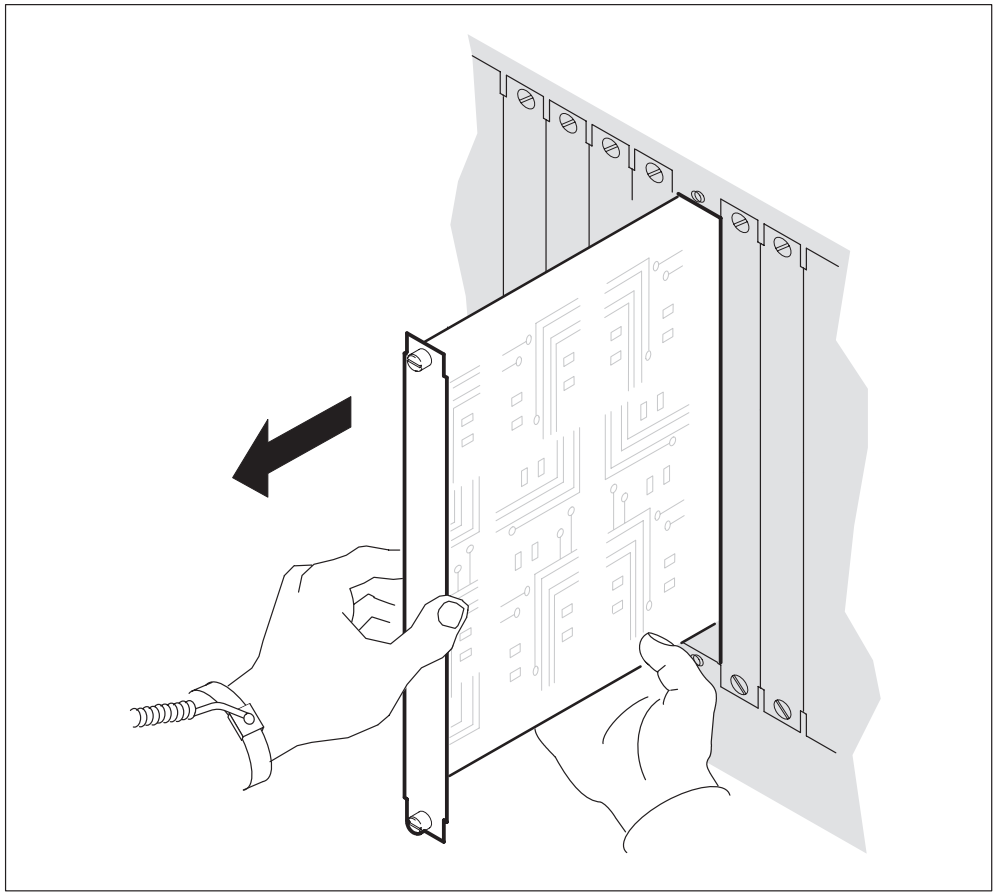
NTRX50FD
CPU personality module (continued)

6 While grasping the thumbscrews, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



NTRX50FD
CPU personality module (continued)

7 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.

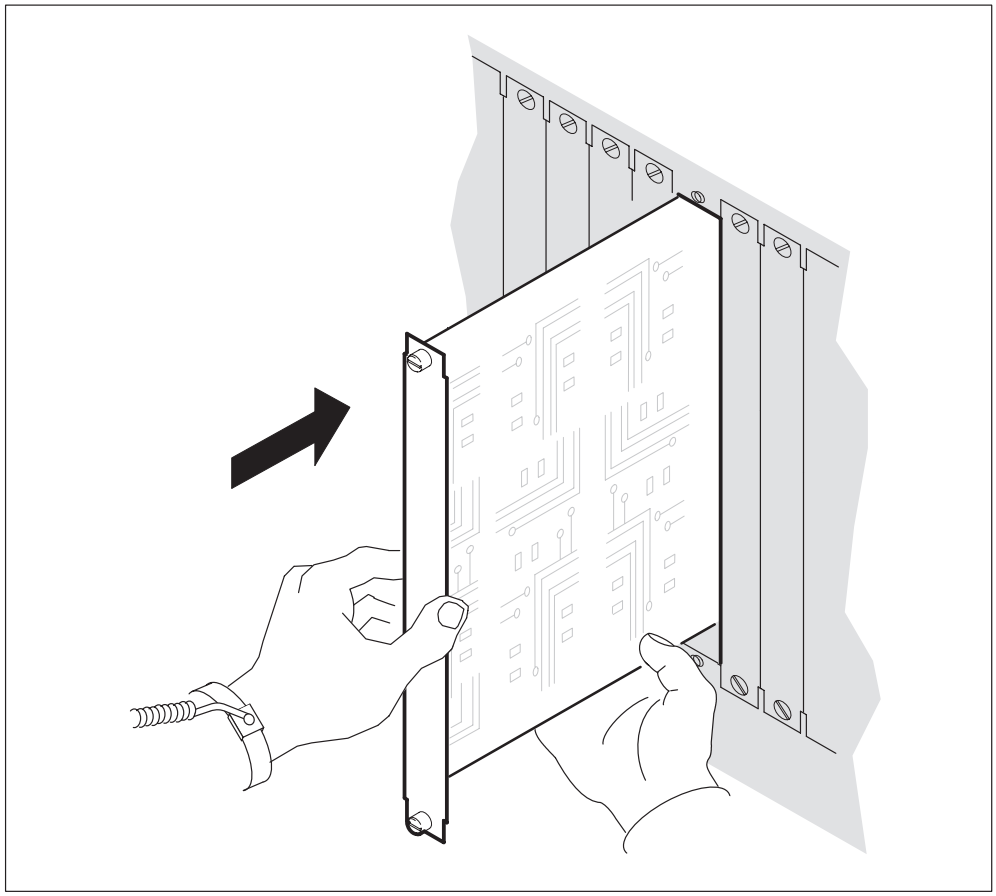


8 Place the module you have removed in an ESD protective container.

9 Insert the replacement module into the SDM shelf.

NTRX50FD
CPU personality module (continued)

10 Gently slide the CPU personality module into the shelf until it is fully inserted.



11 Tighten the thumbscrews at the top and the bottom of the CPU personality module.

12 Reconnect the console cable to the CPU personality module.

At the local or remote VT100 console

13 If you are using the local VT100 console, the asynchronous connection is re-established automatically. Go to step 16.

If you are using a remote VT100 console, re-establish the asynchronous connection to the SDM, continue this procedure.

14 Log in to the SDM.

15 Press the Enter key when you see the prompt, “TERM=(vt100)”. The console prompt is then displayed.

NTRX50FD
CPU personality module (end)

16 You have completed this procedure.

NTRX50FE, NTRX50KD
Fan tray 0

Application

Use this procedure to replace the upper fan trays (fan tray 0), located at the front of the main and I/O expansion chassis of a fault-tolerant SDM.

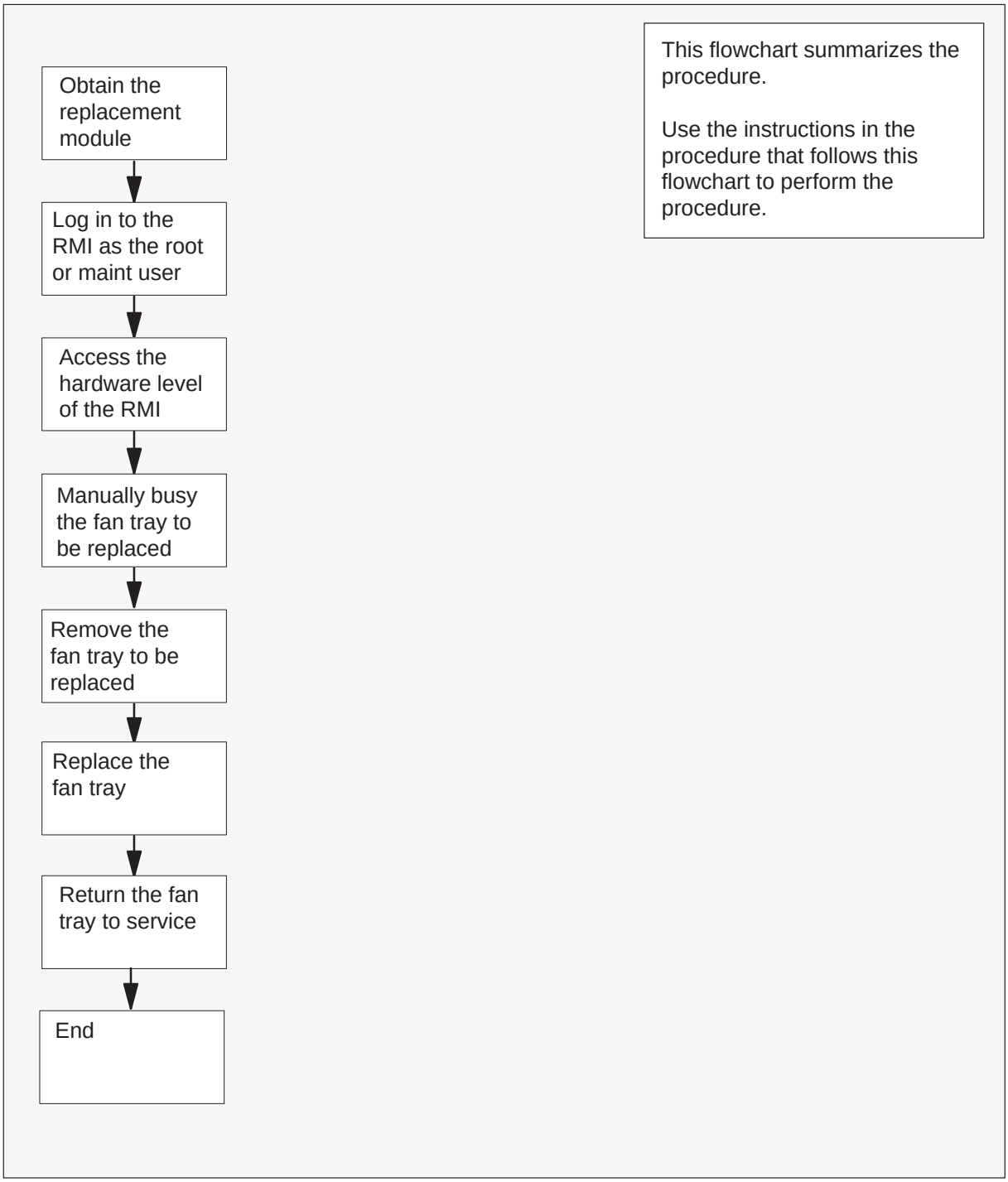
Nortel PEC	Name
NTRX50FE	Fan tray 0 in main chassis
NTRX50KD	Fan tray 0 in I/O expansion chassis

Action

The following flowchart is only a summary of the procedure. To replace the upper fan tray, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FE, NTRX50KD
Fan tray 0 (continued)

Summary of Replacing fan tray 0



NTRX50FE, NTRX50KD
Fan tray 0 (continued)

Replacing fan tray 0

1 Obtain a replacement upper fan tray. Ensure that the replacement has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the left-hand-side locking lever of the fan tray.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

4 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

5 Manually busy the upper fan tray by typing

>BSY 0 FAN
and pressing the Enter key.

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter FAN must be specified as either FAN1 or FAN2, for the main or I/O expansion chassis respectively.

Response:

```
Hardware Bsy – Domain 0 Device FAN

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

6 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

NTRX50FE, NTRX50KD
Fan tray 0 (continued)

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

Response:

```
Hardware Bsy : Domain 0 Device FAN – Command initiated.
Please wait...
```

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

Response:

```
Hardware Bsy : Domain 0 Device FAN – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the fan tray changes to “M”. The out-of-service LED on the fan tray is on (red).

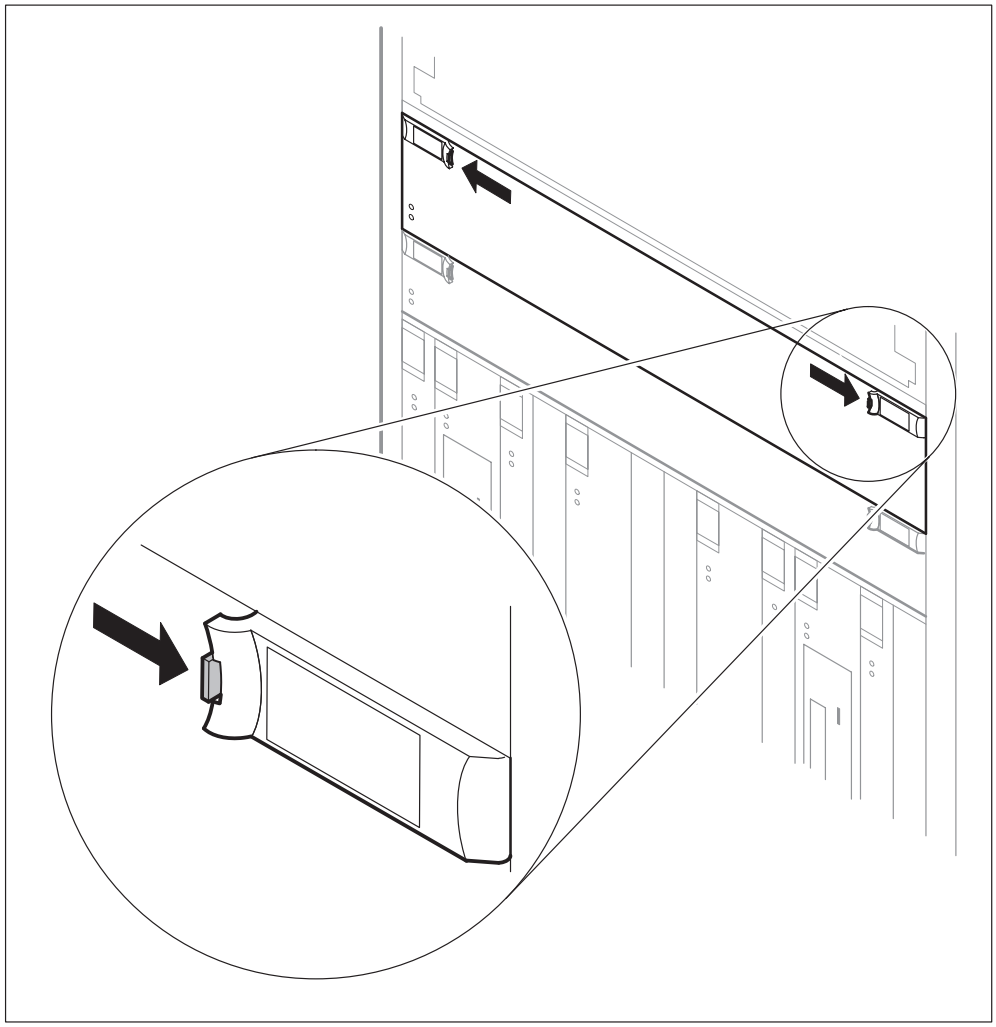
At the front of the SDM

8

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

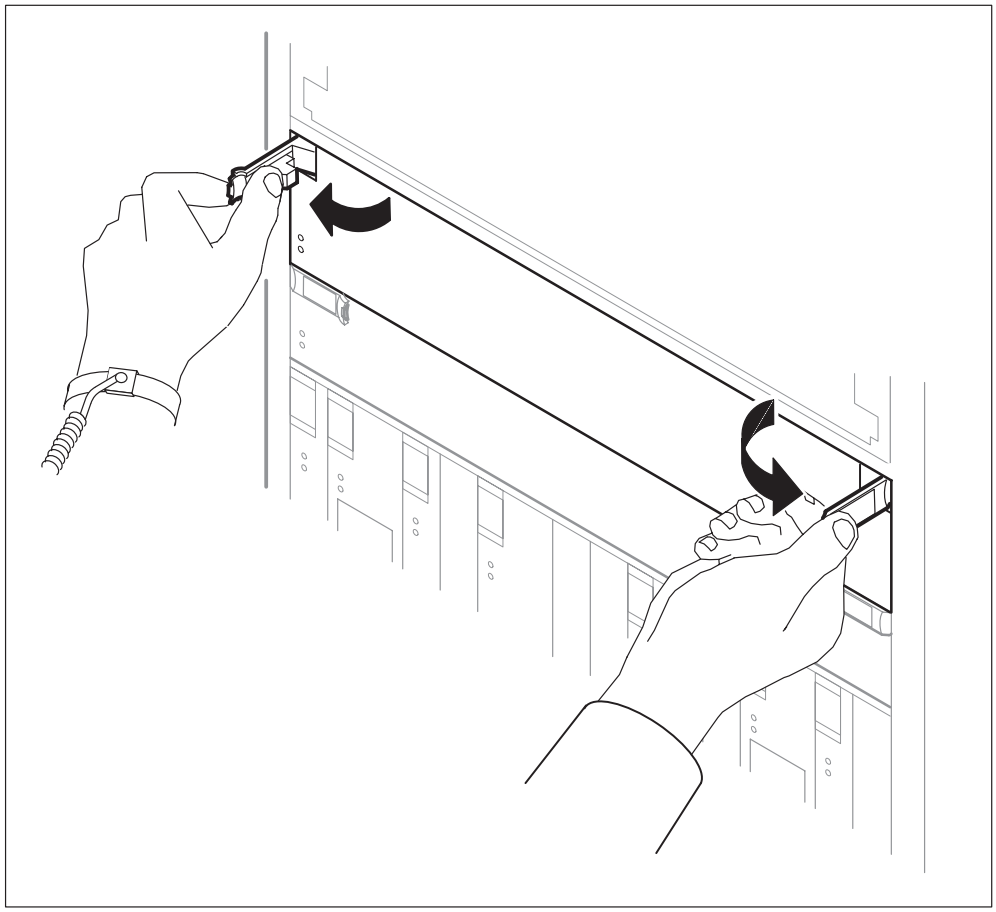
NTRX50FE, NTRX50KD
Fan tray 0 (continued)

9 Depress the tips of the locking levers on the face of the upper fan tray.



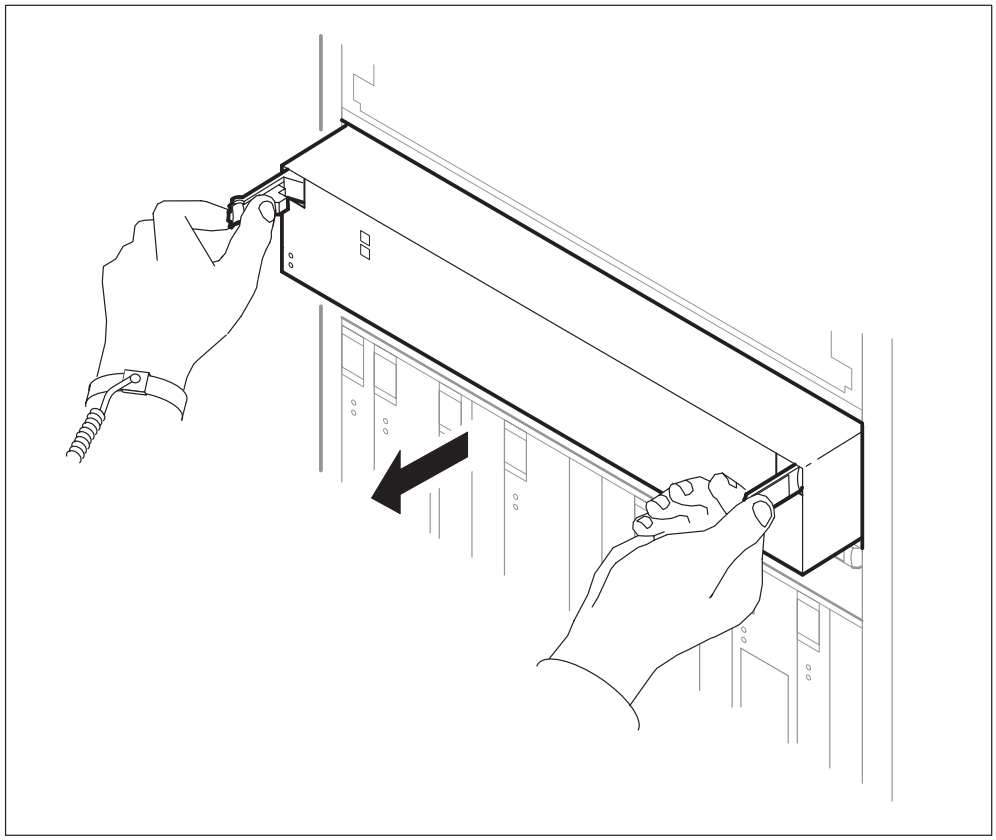
NTRX50FE, NTRX50KD
Fan tray 0 (continued)

10 Open the locking levers on the face of the upper fan tray by moving the levers outwards.



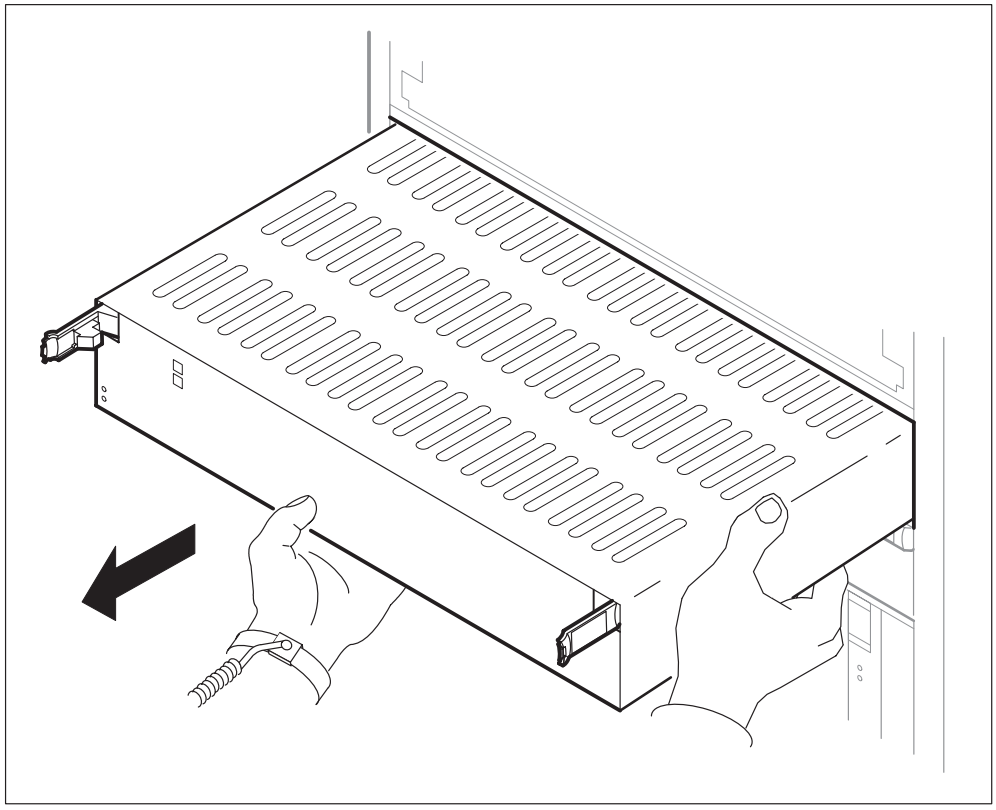
NTRX50FE, NTRX50KD
Fan tray 0 (continued)

11 While grasping the locking levers, gently pull the upper fan tray towards you until the module protrudes about 2 in. (5.1 cm) from the equipment shelf.



NTRX50FE, NTRX50KD
Fan tray 0 (continued)

12 Hold the upper fan tray by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the fan tray toward you until it clears the shelf.

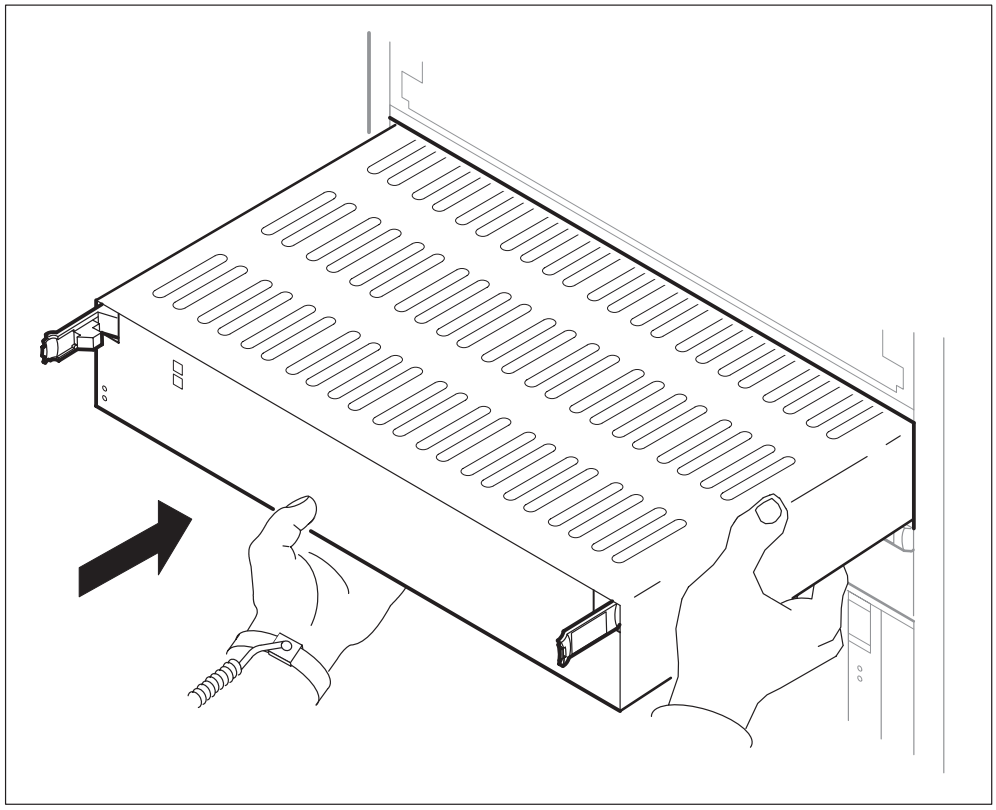


13 Place the fan tray you have removed in an ESD protective container.

14 Insert the replacement fan tray into the shelf.

NTRX50FE, NTRX50KD
Fan tray 0 (continued)

15 Gently slide the fan tray into the shelf until it is almost inserted.



16 Partially close the locking levers, and continue to slide the fan tray until it is fully inserted into the shelf. The locking levers lock by themselves when the fan tray is fully inserted.

NTRX50FE, NTRX50KD
Fan tray 0 (end)

At the local or remote VT100 console

17 At the hardware menu level of the RMI, return the upper fan tray to service by typing

>RTS 0 FAN
and pressing the Enter key.

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter FAN must be specified as either FAN1 or FAN2, for the main or I/O expansion chassis respectively.

Response:

```
Hardware RTS : Domain 0 Device FAN – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device FAN – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the fan tray changes to a dot (.), indicating the fan tray has returned to service. The in-service LED on the fan tray is on (green).

18 You have completed this procedure.

NTRX50FF
Fan tray 1

Application

Use this procedure to replace the lower fan tray (fan tray 1), located at the front of the main and I/O expansion chassis of a fault-tolerant SDM.

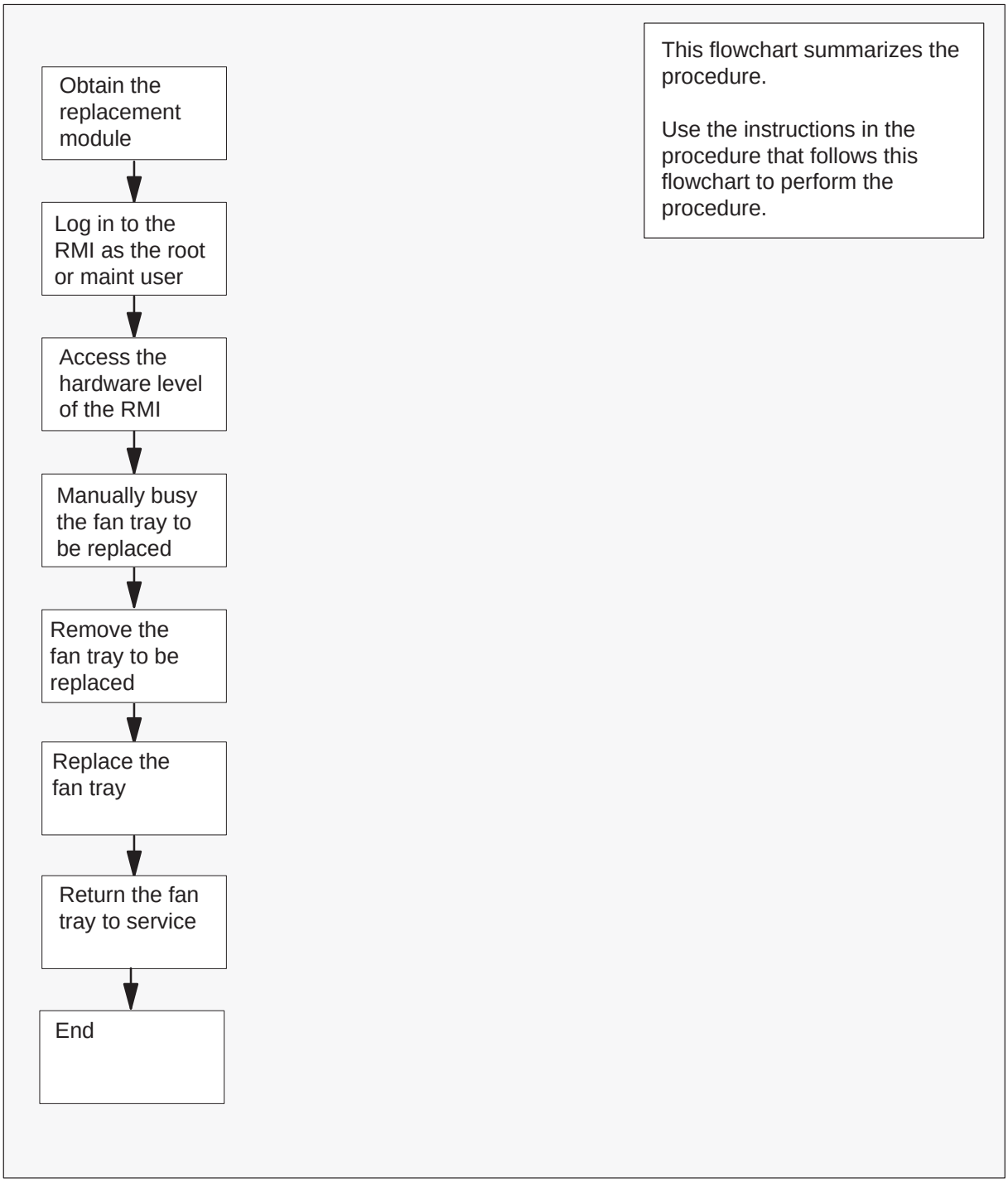
Nortel PEC	Name
NTRX50FF	Fan tray 1 in main or optional I/O expansion chassis

Action

The following flowchart is only a summary of the procedure. To replace the lower fan tray, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FF
Fan tray 1 (continued)

Summary of Replacing fan tray 1



NTRX50FF
Fan tray 1 (continued)

Replacing fan tray 1

1 Obtain a replacement lower fan tray module. Ensure that the replacement has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the left-hand-side locking lever of the fan tray.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

4 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

5 Manually busy the lower fan tray module by typing

>BSY 1 FAN
and pressing the Enter key.

Example response:

```
Hardware Bsy – Domain 1 Device FAN

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter FAN must be specified as either FAN1 or FAN2, for the main or I/O expansion chassis respectively.

6 Confirm the Bsy command by typing

>Y

and pressing the Enter key.

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

Response:

```
Hardware Bsy : Domain 1 Device FAN – Command initiated.
Please wait...
```

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

Response:

```
Hardware Bsy : Domain 1 Device FAN – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the fan tray changes to “M”. The out-of-service LED on the fan tray is on (red).

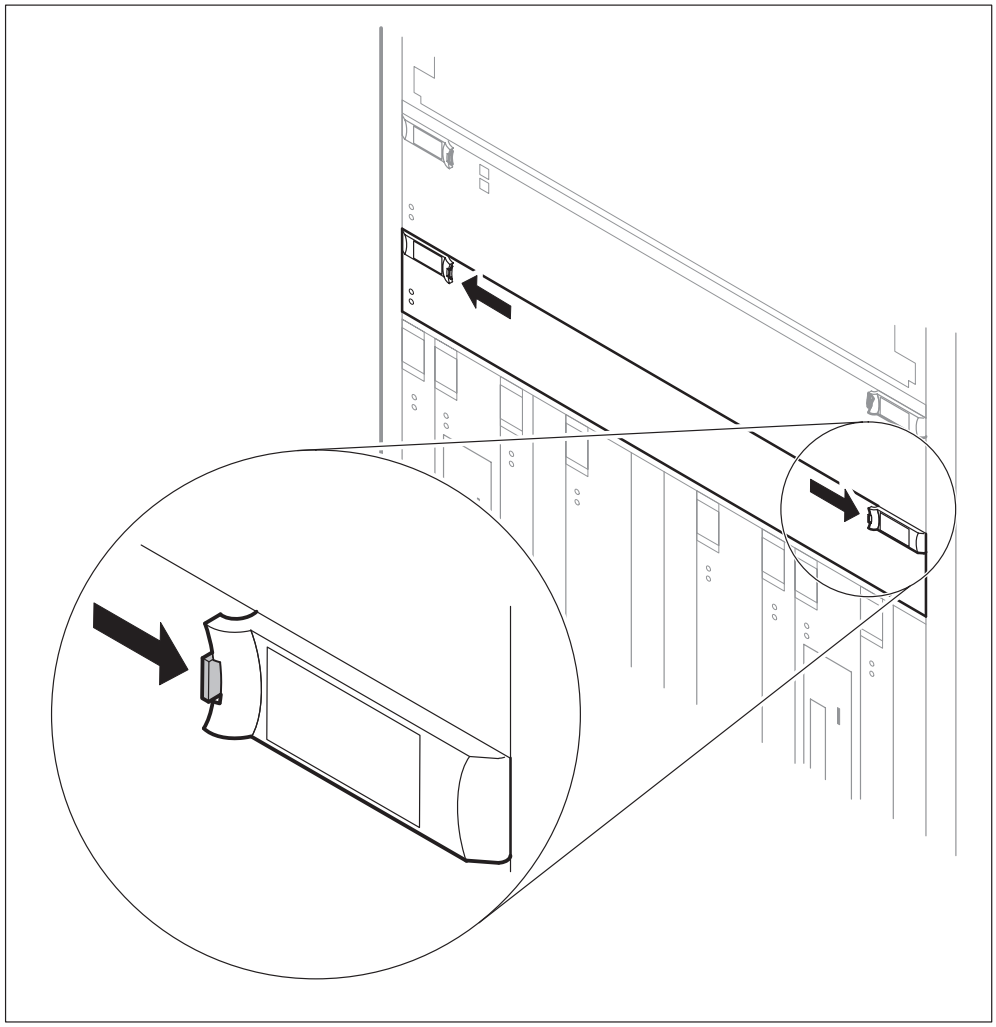
At the front of the SDM

8

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

NTRX50FF
Fan tray 1 (continued)

9 Depress the tips of the locking levers on the face of the lower fan tray.

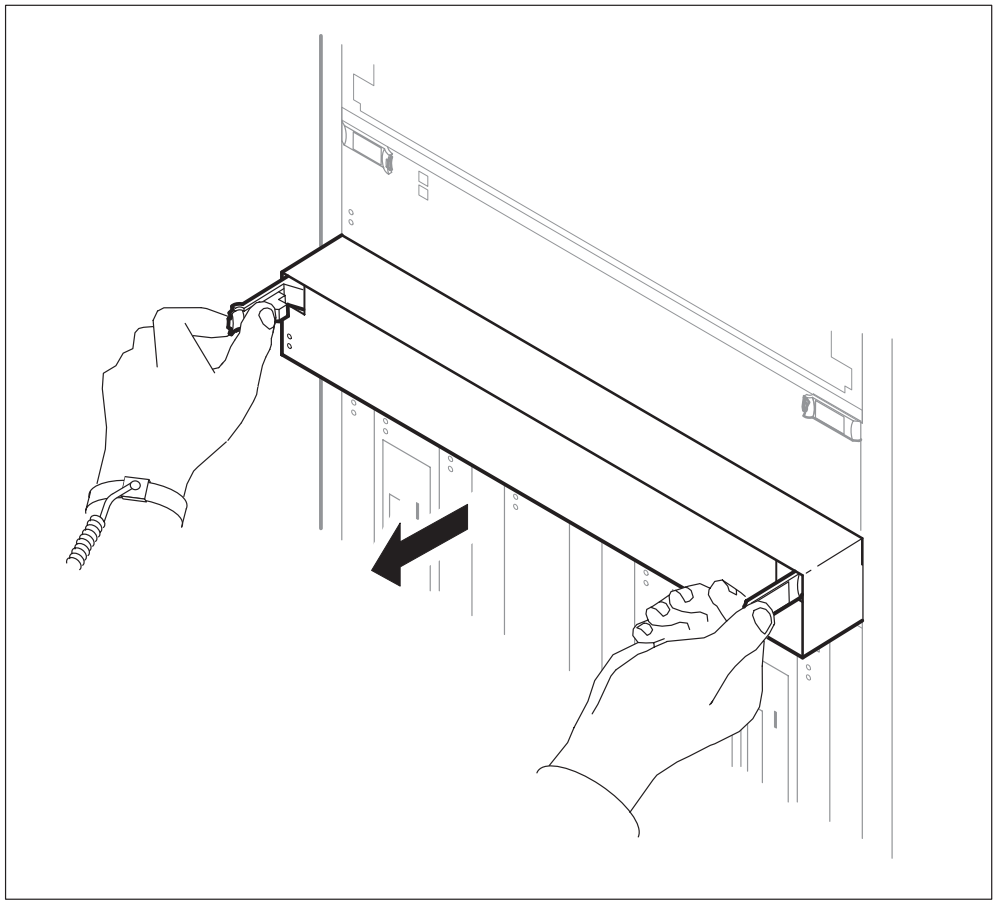


NTRX50FF
Fan tray 1 (continued)

10 Open the locking levers on the face of the lower fan tray by moving the levers outwards.

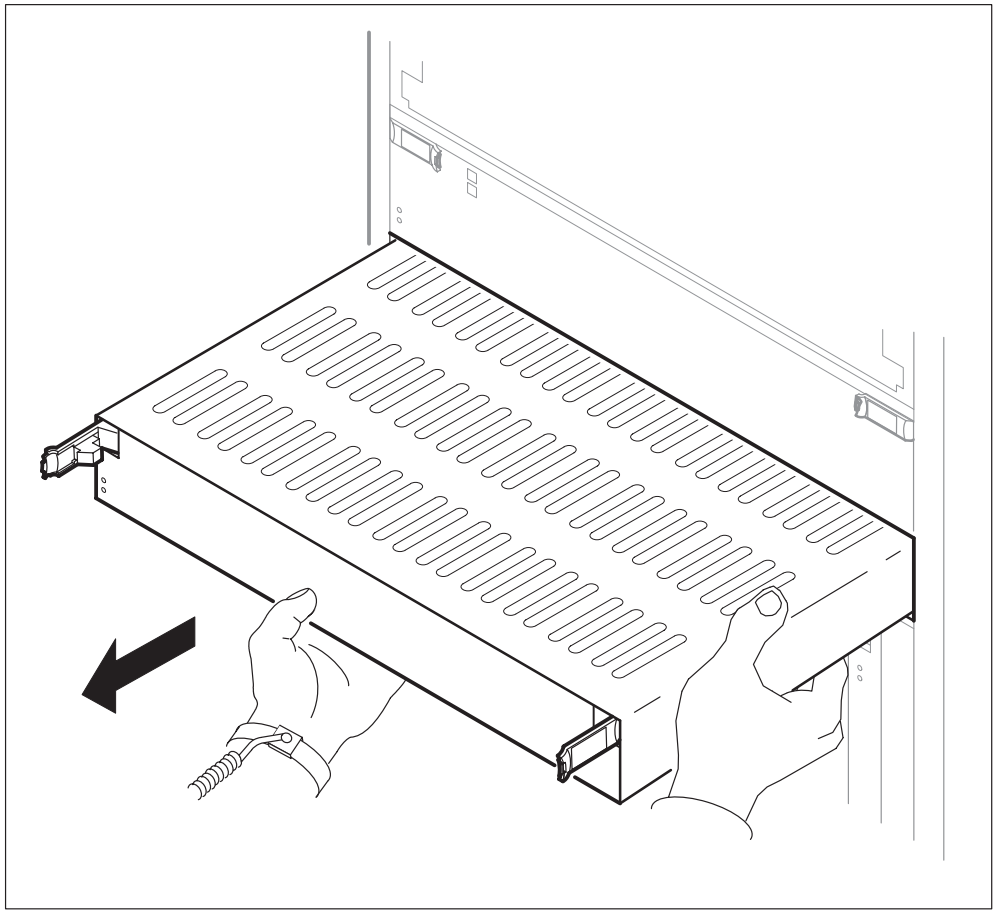
NTRX50FF
Fan tray 1 (continued)

11 While grasping the locking levers, gently pull the lower fan tray towards you until the fan tray protrudes about 2 in. (5.1 cm) from the equipment shelf.



NTRX50FF
Fan tray 1 (continued)

12 Hold the lower fan tray by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the fan tray toward you until it clears the shelf.

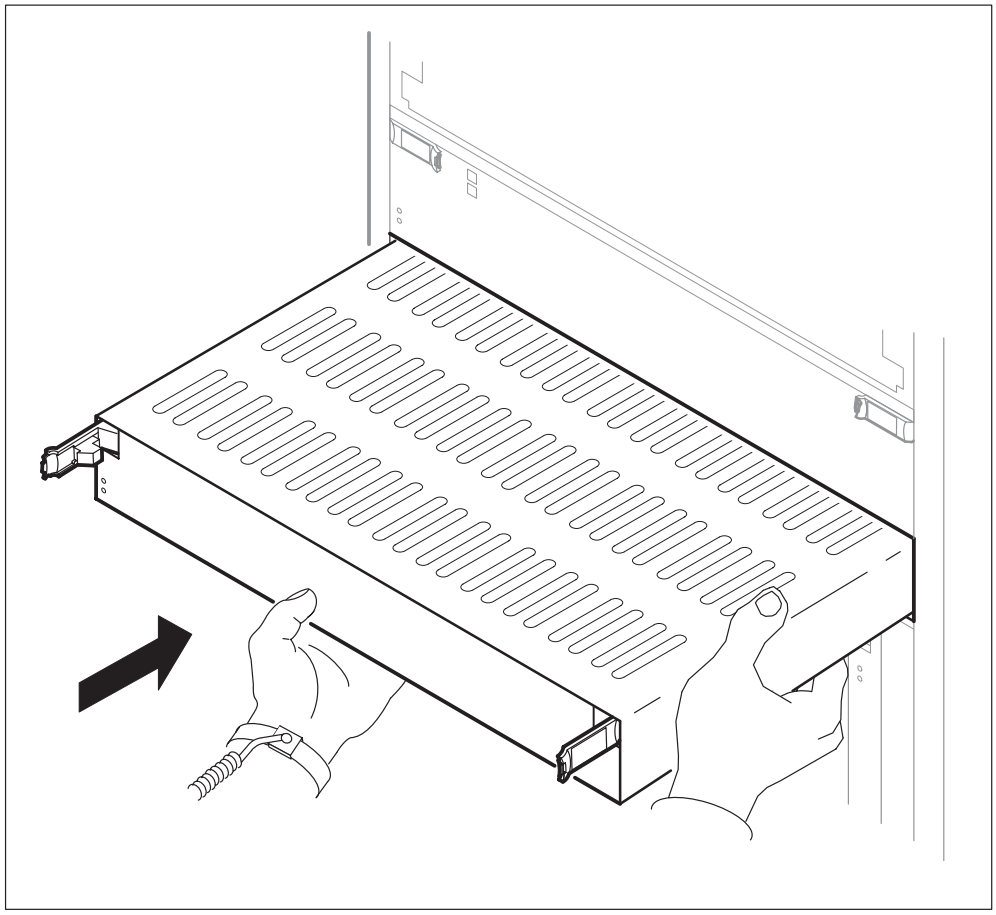


13 Place the fan tray you have removed in an ESD protective container.

14 Insert the replacement fan tray into the shelf.

NTRX50FF
Fan tray 1 (continued)

15 Gently slide the fan tray into the shelf until it is almost inserted.



16 Partially close the locking levers, and continue to slide the fan tray until it is fully inserted into the shelf. The locking levers lock by themselves when the fan tray is fully inserted.

At the local or remote VT100 console

17 At the hardware level of the RMI, return the lower fan tray to service by typing

>RTS 1 FAN

and press the Enter key.

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter FAN must be specified as either FAN1 or FAN2, for the main or I/O expansion chassis respectively.

Response:

```
Hardware RTS : Domain 1 Device FAN – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 1 Device FAN – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the fan tray changes to a dot (.), indicating the fan tray has returned to service. The in-service LED on the fan tray is on (green).

18 You have completed this procedure.

NTRX50FG
Interconnect module 0

Application

Use this procedure to replace an interconnect module (ICM) in domain 0, located at the right hand side at the rear of the main or I/O expansion chassis of a fault-tolerant SDM.

Nortel PEC	Name
NTRX50FG	Interconnect module 0

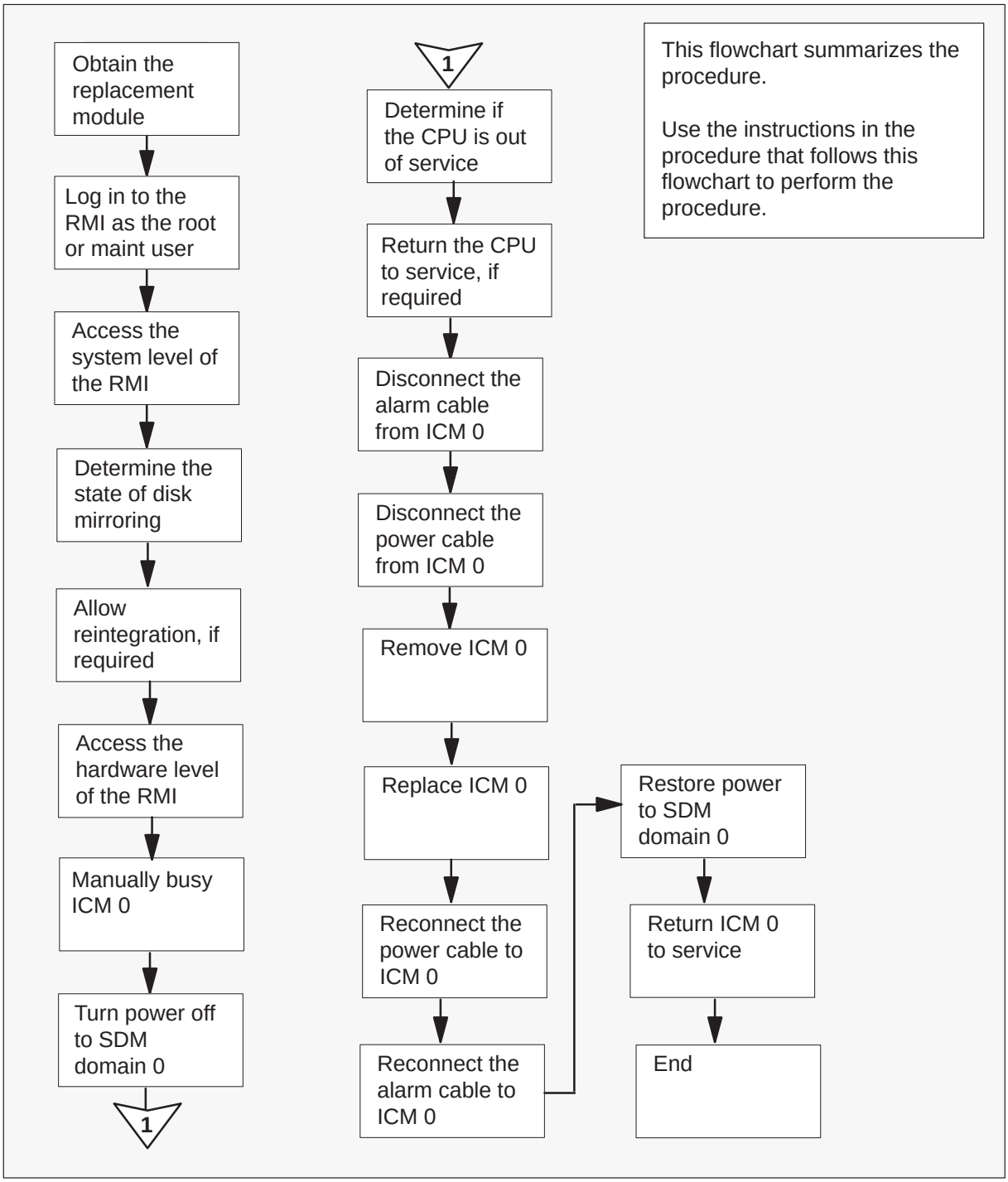
Note: If you are replacing the ICM because it is indicated as failed (F) at the hardware menu level of the remote maintenance interface (RMI), verify that the ICM failure has not been caused by a loss of DC input power.

Action

The following flowchart is only a summary of the procedure. To replace interconnect module 0, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FG
Interconnect module 0 (continued)

Summary of Replacing interconnect module 0



NTRX50FG
Interconnect module 0 (continued)

Replacing an interconnect module 0

1 Obtain a replacement interconnect module. Ensure that the replacement has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written at the top, left-hand side of the ICM.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

4 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

5 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):        Integrating
```

6 Determine the disk mirroring status for each volume group commissioned on the SDM.

7 Proceed according to the disk mirroring state.

If disk mirroring is in the	Do
Integrating state	step 8
Mirrored or Not Mirrored state	step 9

NTRX50FG
Interconnect module 0 (continued)

8 The hard disks that provide mirrored storage for the system are reintegrating. Allow the reintegration process to complete before continuing this procedure. The reintegration process takes about 30 min per Gbyte. (The actual time required varies depending on the amount of data in the volume group, and the current processor load.)

CAUTION
Potential loss of service
Do not continue this procedure beyond this point while the disks are reintegrating. If you interrupt power to one ICM (step 10) during the reintegration process, you will cause a reintegration failure that may require service-affecting manual recovery action.

Go to step 6.

9 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

10 Manually busy ICM 0 by typing

>BSY 0 ICM
and pressing the Enter key.

Response:

```
Hardware Bsy – Domain 0 Device ICM
This action will affect all devices in I/O domain 0.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

11 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

Note: When you manually busy ICM 0, all subtending devices (FAN, ETH, DSK1, DSK2, DSK3, DAT, and 512) in domain 0 are also put in the CBsy state.

NTRX50FG
Interconnect module 0 (continued)

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

Response:

```
Hardware Bsy : Domain 0 Device ICM – Command initiated.
Please wait...
```

Several warnings are displayed. The “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Response:

```
Hardware Bsy : Domain 0 Device ICM – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the interconnect module changes and all subtending devices changes to “M”. The out-of-service LED on the module is on (red).

At the back of the SDM

13

CAUTION
Potential service interruption
Ensure that you disconnect power to ICM 0. If you disconnect power to the remaining in-service ICM (ICM 1), the entire SDM shuts down.

At the front of the MSP

14 Turn off power to SDM domain 0 at the appropriate modular supervisory panel (MSP) breaker. Proceed according to where ICM 0 is located.

If ICM0 is located in	Do
the main chassis	turn top left breaker off
the I/O expansion chassis	turn bottom left breaker off

NTRX50FG
Interconnect module 0 (continued)

At the local or remote VT100 console

15 Determine if one CPU controller module has dropped out of service (indicated by an “F” (failed) under its header at the RMI hardware menu level).

If	Do
both CPUs are in service	step 17
one CPU is out of service	step 16

16

CAUTION
Possible service degradation
If an ICM fails, the corresponding CPU controller module may be brought down by the system and must be returned to service manually. Return the CPU controller module to service at the hardware (Hw) menu level of the RMI, or the platform MAP level under the SDM MAP level.

Return the out-of-service CPU to service, and start CPU reintegration by typing

>RTS *n* CPU
and pressing the Enter key.

where

n is the domain number (0 or 1) of the CPU controller module that you are returning to service

Example response:

```
Hardware RTS : Domain 0 Device CPU – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 0 Device CPU – Command submitted.
```

Note: At the hardware menu level of the RMI, the CPU state changes to “S”, indicating that the CPUs are reintegrating. the reintegration process takes about 2 min to complete, after which the CPU status changes to in-service (indicated by a dot). The in-service LED on ICM 0 is on (green).

NTRX50FG
Interconnect module 0 (continued)

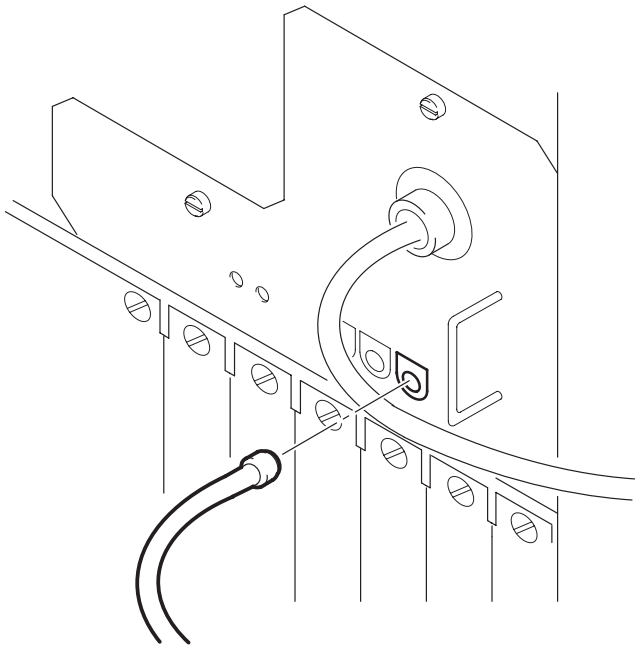
At the back of the SDM

17

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

18 Disconnect the alarm cable from ICM 0.

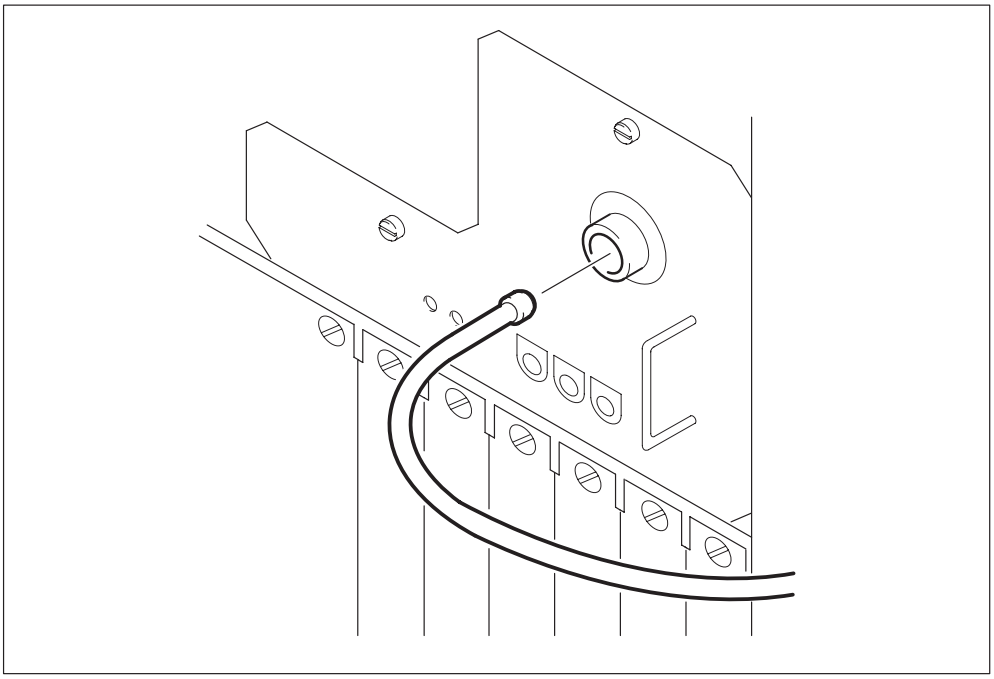
Note: If you are replacing an ICM in an I/O expansion chassis, the alarm cable is not present. Go to step 19.



NTRX50FG
Interconnect module 0 (continued)

19 Disconnect the power cable from ICM 0.

CAUTION
Potential service interruption
Ensure that you disconnect the power cable from ICM 0. If you disconnect the power cable to the remaining in-service ICM (ICM 1), the entire SDM shuts down.

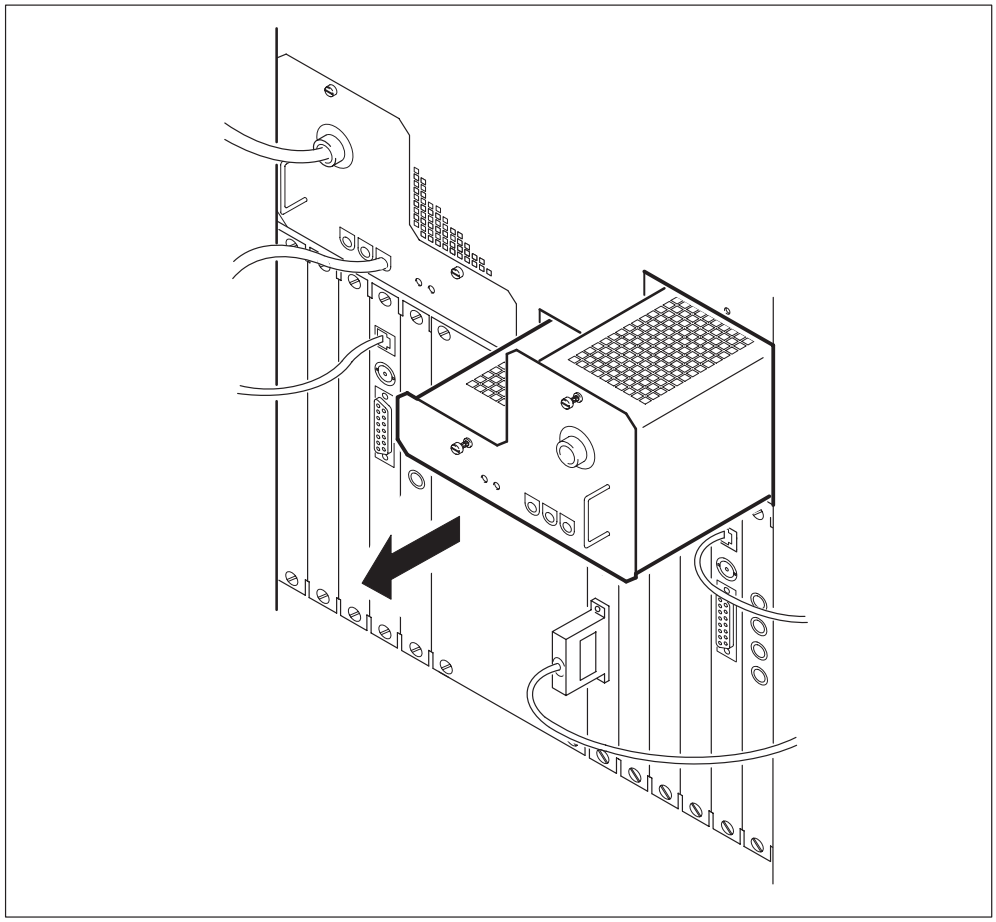


20 Loosen the two thumbscrews on ICM 0.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

NTRX50FG
Interconnect module 0 (continued)

21 Remove ICM 0 by gently sliding it out of the chassis.



22 Place the module you have removed in an ESD protective container.

23 Gently insert and seat the replacement ICM 0.

24 Secure the replacement ICM by tightening the two captive screws.

25 Reconnect the power cable to ICM 0.

26 Reconnect the alarm cable to ICM 0, if required (see step18).

At the front of the MSP

27 Restore power to SDM domain 0 by switching on the MSP breaker turned off in step 13.

NTRX50FG
Interconnect module 0 (end)

At the local or remote VT100 console

28 At the hardware menu level of the RMI, return ICM 0 to service by typing

>RTS 0 ICM
and pressing the Enter key

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

Response:

```
Hardware RTS : Domain 0 Device ICM – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 0 Device ICM – Command submitted.
```

29 Allow 5 min for the interconnect modules to reintegrate. Check the LEDs on the ICM that you replaced.

Note: If your SDM contains an I/O expansion chassis, the reintegration of the interconnect modules takes about 20 min.

If	Do
the ICM in-service LED is on (solid green), and the out-of-service LED is off	step 32
the ICM in-service LED is off, and the out-of-service LED is on (solid red or flashing red)	step 31
both LEDs on the CPU controller module are off	step 30

30 Reseat the ICM that you replaced, then go to step 28.

31 Contact the personnel responsible for the next level of support.

32 You have completed this procedure.

NTRX50FH
Interconnect module 1

Application

Use this procedure to replace an interconnect module in domain 1, located at the left hand side at the rear of the main or I/O expansion chassis of a fault-tolerant SDM.

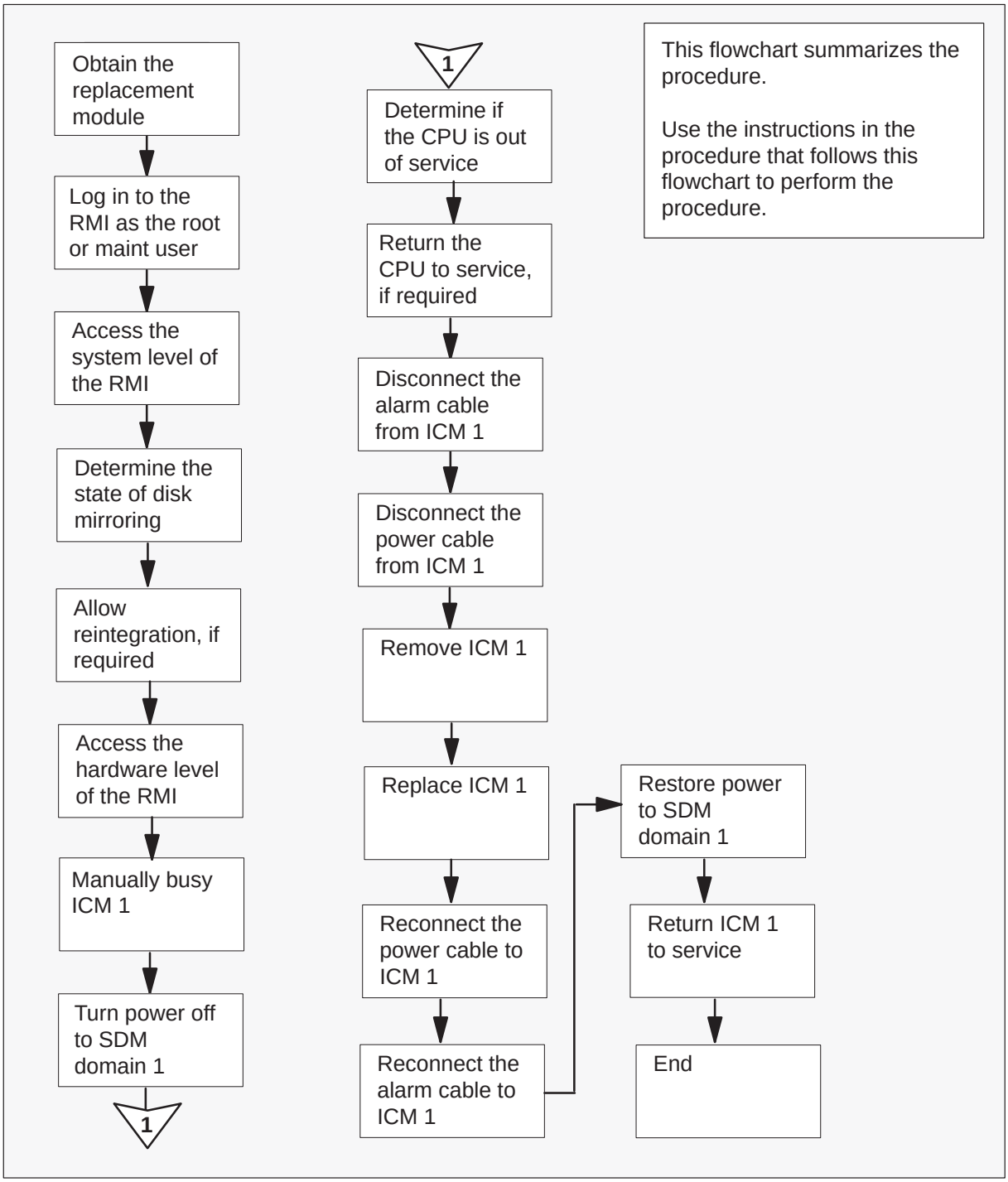
Nortel PEC	Name
NTRX50FH	Interconnect module 1

Action

The following flowchart is only a summary of the procedure. To replace interconnect module 1, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FH
Interconnect module 1 (continued)

Summary of Replacing interconnect module 1



NTRX50FH
Interconnect module 1 (continued)

Replacing interconnect module 1

1 Obtain a replacement interconnect module. Ensure that the replacement has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written at the top, left-hand side of the ICM.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

4 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

5 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):        Integrating
```

6 Determine the disk mirroring status for each volume group commissioned on the SDM.

7 Proceed according to the disk mirroring state.

If disk mirroring is in the	Do
Integrating state	step 8
Mirrored or Not Mirrored state	step 9

NTRX50FH
Interconnect module 1 (continued)

8 The hard disks that provide mirrored storage for the system are reintegrating. Allow the reintegration process to complete before continuing this procedure. The reintegration process takes about 30 min per Gbyte. (The actual time required varies depending on the amount of data in the volume group, and the current processor load.)

CAUTION
Potential loss of service
Do not continue this procedure beyond this point while the disks are reintegrating. If you interrupt power to one ICM (step 10) during the reintegration process, you will cause a reintegration failure that may require service-affecting manual recovery action.

Go to step 6.

9 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

10 Manually busy ICM 1 by typing

>BSY 1 ICM
and pressing the Enter key.

Response:

```
Hardware Bsy – Domain 1 Device ICM
This action will affect all devices in I/O domain 1.

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

11 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

Note: When you manually busy ICM 1, all subtending devices in (FAN, ETH, DSK1, DSK2, DSK3, DAT. and 512) in domain 1 are put in the CBsy state.

NTRX50FH
Interconnect module 1 (continued)

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

Response:

```
Hardware Bsy : Domain 1 Device ICM – Command initiated.
Please wait...
```

Several warnings are displayed. The “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”.

Response:

```
Hardware Bsy: Domain 1 Device ICM – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the interconnect module and all subtending devices changes to “M”. The out-of-service LED on the module is on (red).

At the back of the SDM

13

CAUTION
Potential service interruption
Ensure that you disconnect power to ICM 1. If you disconnect power to the remaining in-service ICM (ICM 0), you will shut down the entire SDM.

At the front of the MSP

14 Turn off power to SDM domain 1 at the appropriate modular supervisory panel (MSP) breaker. Proceed according to where ICM 1 is located.

If ICM1 is located in	Do
the main chassis	turn top right breaker off
the I/O expansion chassis	turn bottom right breaker off

NTRX50FH
Interconnect module 1 (continued)

At the local or remote VT100 console

15 Determine if one CPU controller module has dropped out-of-service (indicated by an “F” under its header at the RMI hardware menu level).

If	Do
one CPU is out of service	step 16
both CPUs are in service	step 17

16

CAUTION
Possible service degradation
If an ICM fails, the corresponding CPU controller module may be brought down by the system and must be returned to service manually. Return the CPU controller module to service at the hardware (Hw) menu level of the RMI, or the platform MAP level under the SDM MAP level.

Return the out-of-service CPU to service, and start CPU reintegration by typing

>RTS *n* CPU
and pressing the Enter key.

where

n is the domain number (0 or 1) of the CPU controller module that you are returning to service

Example response:

```
Hardware RTS : Domain 0 Device CPU – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 0 Device CPU – Command submitted.
```

Note: At the hardware menu level of the RMI, the CPU state changes to “S”, indicating that the CPUs are reintegrating. The reintegration process takes about 2 min to complete, after which the CPU status changes to in-service (indicated by a dot). The in-service LED on ICM 1 is on (green).

NTRX50FH
Interconnect module 1 (continued)

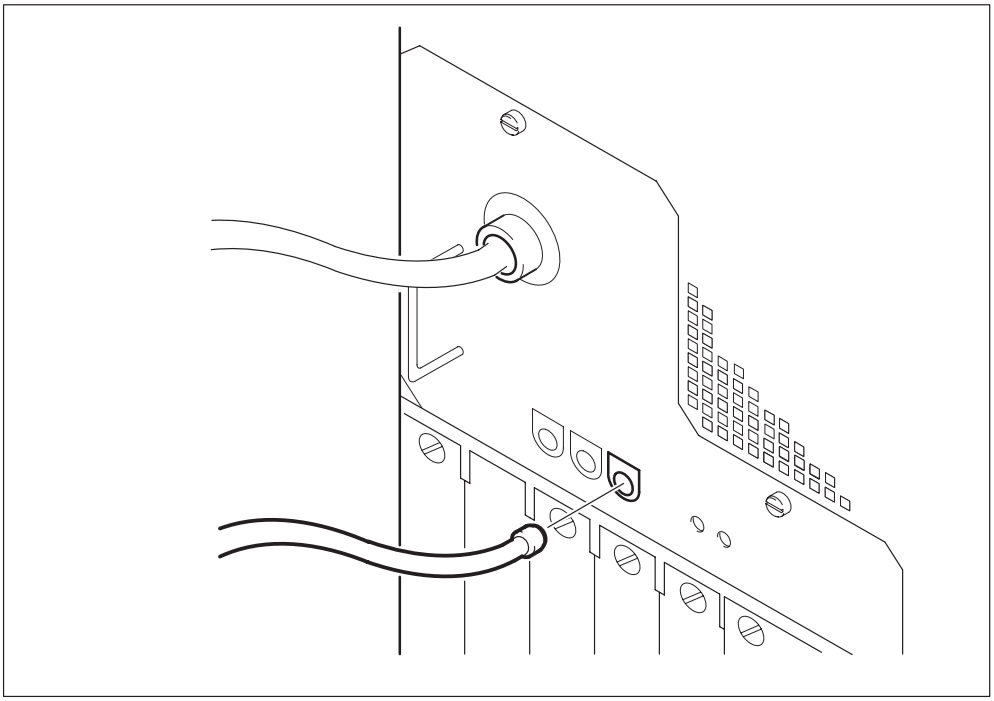
At the back of the SDM

17

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

18 Disconnect the alarm cable from ICM 1.

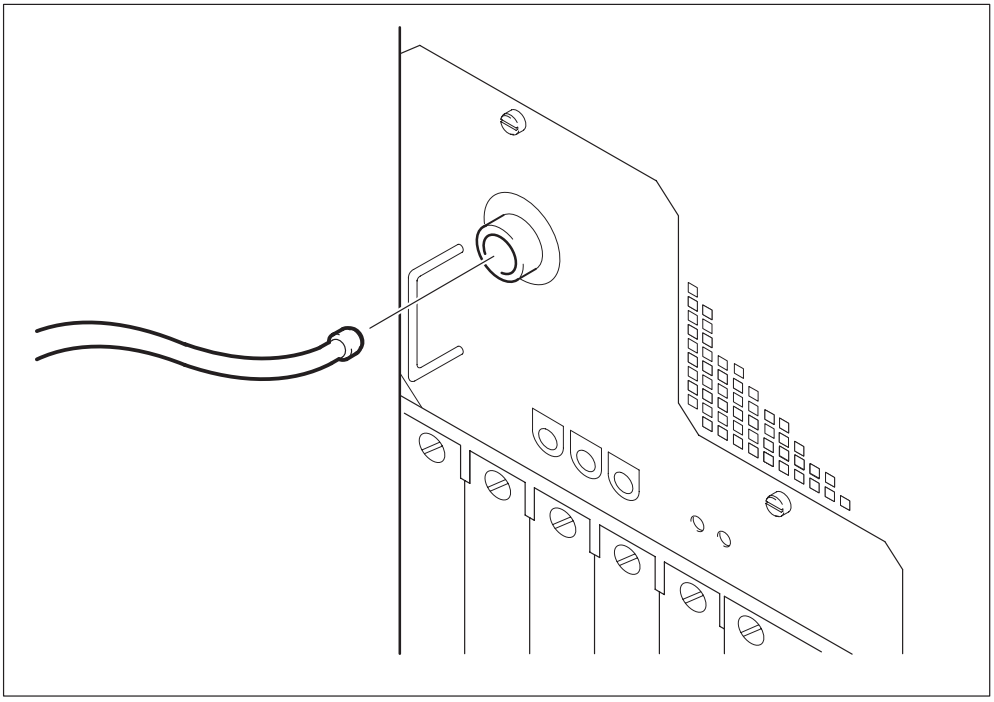
Note: If you are replacing an ICM in an I/O expansion chassis, the alarm cable is not present. Go to step 19.



NTRX50FH
Interconnect module 1 (continued)

19 Disconnect the power cable from ICM 1.

CAUTION
Potential service interruption
Ensure that you disconnect the power cable from ICM 1. If you disconnect the power cable to the remaining in-service ICM (ICM 0), you will shut down the entire SDM.

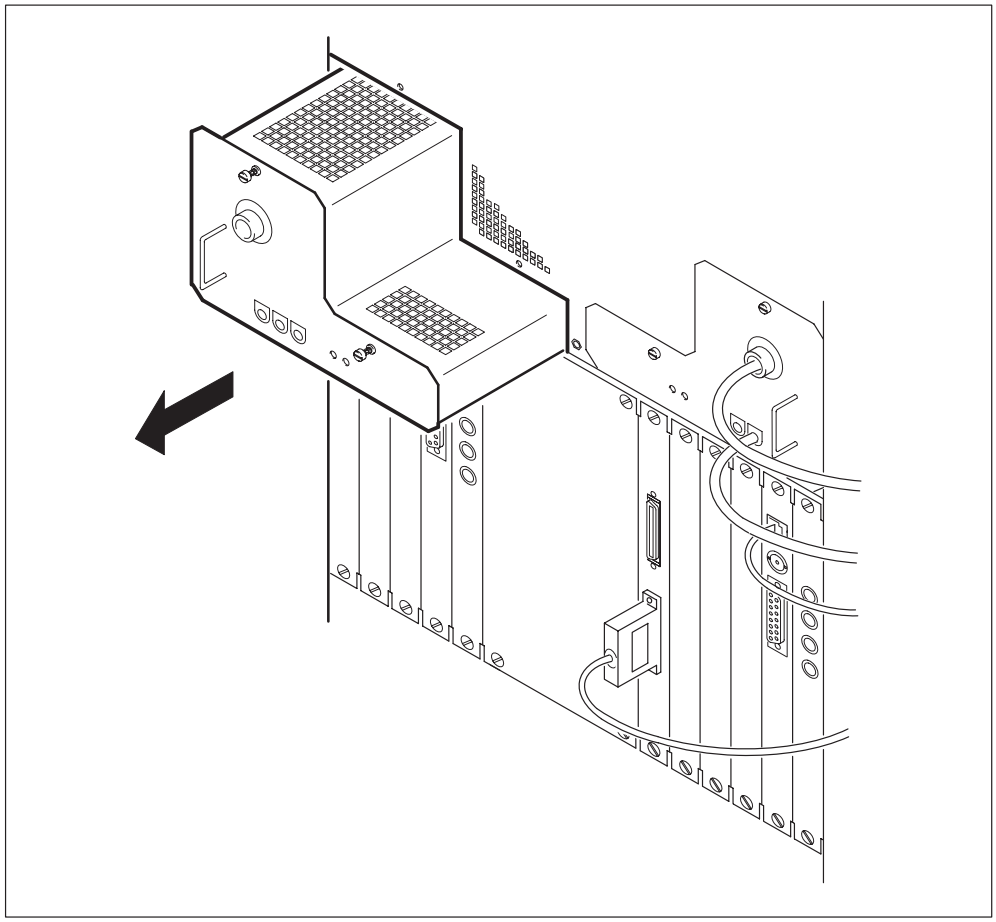


20 Loosen the two thumbscrews on ICM 1.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

NTRX50FH
Interconnect module 1 (continued)

21 Remove ICM 1 by gently sliding it out of the chassis.



22 Place the module you have removed in an ESD protective container.

23 Gently insert and seat the replacement ICM 1.

24 Secure the replacement ICM by tightening the two captive screws.

25 Reconnect the power cable to ICM 1.

26 Reconnect the alarm cable to ICM 1, if required (see step 18).

At the front of the MSP

27 Restore power to SDM domain 1 by switching on the MSP breaker turned off in step 13.

NTRX50FH
Interconnect module 1 (end)

At the local or remote VT100 console

28 At the hardware menu level of the RMI, return ICM 1 to service by typing

>RTS 1 ICM
and pressing the Enter key

Note: This syntax is valid for single-chassis configuration only. For systems with an I/O expansion chassis, the parameter ICM must be specified as ICM1 for the main chassis.

Response:

```
Hardware RTS : Domain 1 Device ICM – Command initiated.
Please wait...
```

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

Response:

```
Hardware RTS : Domain 1 Device ICM – Command submitted.
```

At the back of the SDM

29 Allow 5 min for the interconnect modules to reintegrate. Check the LEDs on the ICM that you replaced.

Note: If your SDM contains an I/O expansion chassis, the reintegration of the interconnect modules takes about 20 min.

If	Do
both LEDs on the CPU controller module are off	step 30
the ICM in-service LED is off, and the out-of-service LED is on (solid red or flashing red)	step 31
the ICM in-service LED is on (solid green), and the out-of-service LED is off	step 32

30 Reseat the ICM that you replaced, then go to step 28.

31 Contact the personnel responsible for the next level of support.

32 You have completed this procedure.

NTRX50FK, NTRX50FL, NTRX50FM CPU controller module

Application

Use this procedure to replace the CPU controller modules, located at the front of the main chassis (slots 6 and 7, and slots 10 and 11) of a fault-tolerant SDM.

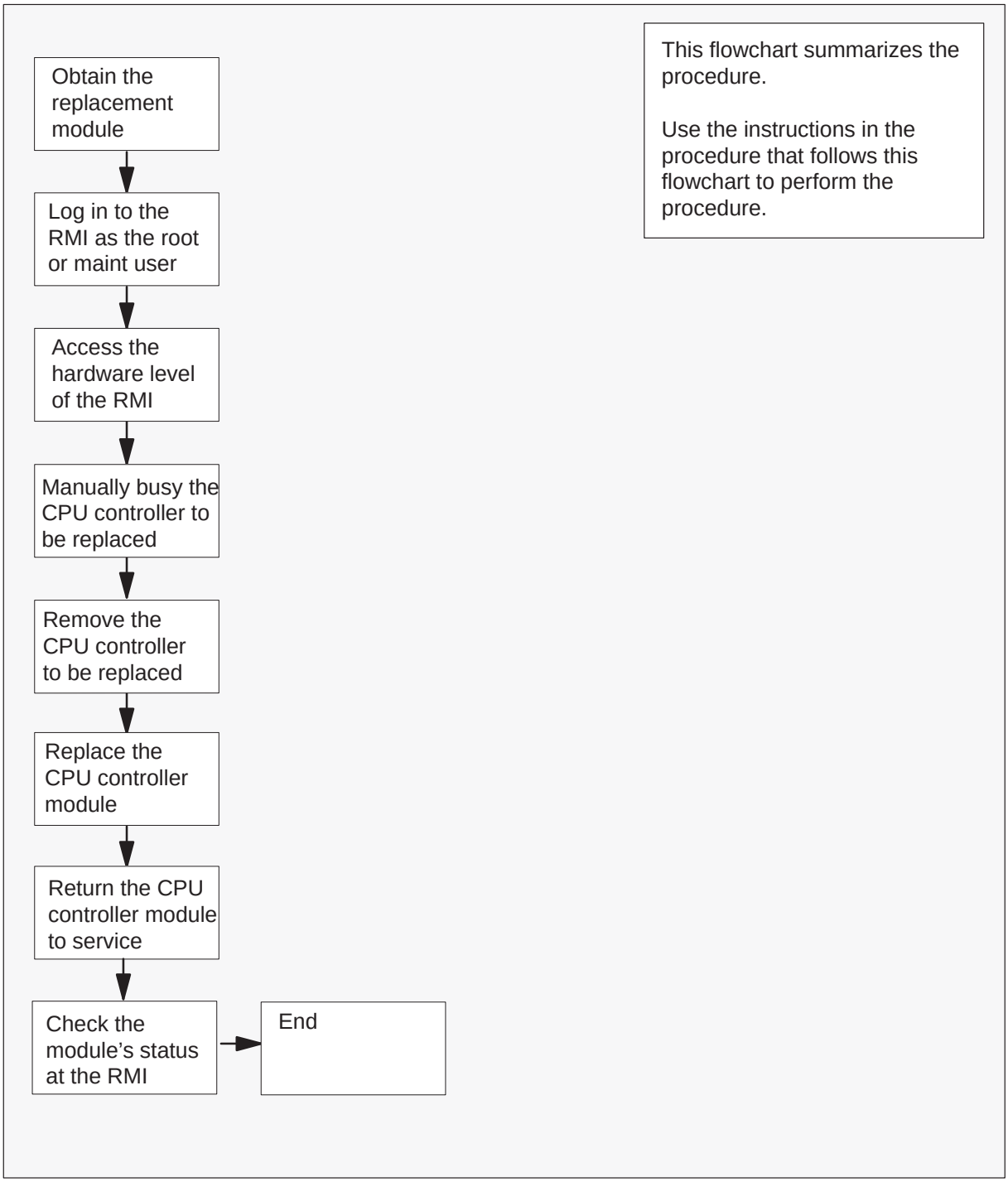
Nortel PEC	Name
NTRX50FK	CPU controller module with 128 MByte DRAM
NTRX50FL	CPU controller module with 256 MByte DRAM
NTRX50FM	CPU controller module with 512 MByte DRAM

Action

The following flowchart is only a summary of the procedure. To replace the CPU controller module, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (continued)

Summary of Replacing a CPU controller module



NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (continued)

Replacing a CPU controller module

1 Obtain a replacement CPU controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the module's top locking lever.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

4 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

5 Manually busy the CPU controller module you wish to replace by typing

>BSY *n* CPU
and pressing the Enter key.

where

n is the domain number (0 or 1) of the CPU controller module that you are replacing

Note: The domain is 0 if the CPU controller module is in slots 6 and 7, and 1 if it is in slots 10 and 11 of the main chassis.

Example response:

```
Hardware Bsy – Domain 0 Device CPU

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N"):
```

6 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (continued)

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

Example response:

```
Hardware Bsy : Domain 0 Device CPU – Command initiated.
Please wait...
```

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

Example response:

```
Hardware Bsy : Domain 0 Device CPU – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the CPU controller module changes to “M”.

At the front of the SDM

8

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

CAUTION
Potential service interruption
Remove only the CPU controller module that you busied in step 5. The in-service LED on this module is off, and the out-of-service LED is on (red).

Do not remove the remaining, in-service module. The in-service LED on the in-service module is on (green), and the out-of-service LED is off. If you remove this module, the SDM shuts down and an automatic reboot occurs.

Note 1: When a CPU controller module is pulled from the SDM, automatic message accounting (AMA) may go into backup, depending on the scenario:

NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (continued)

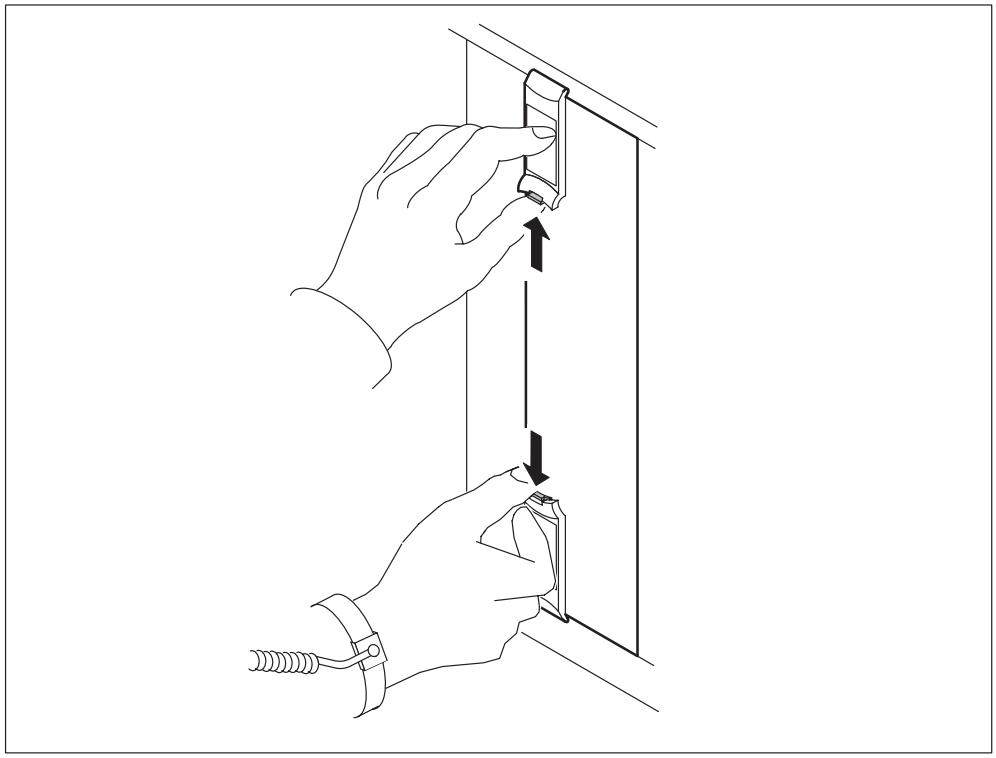
- When an active CPU controller module is pulled, AMA goes into backup immediately at the CM level. When the CPU controller module is reinserted and manually returned to service, the module starts integrating. AMA does not go into backup.
- When an inactive CPU controller module is pulled from the SDM, AMA does not go into backup immediately. However, when the module is inserted and starts reintegrating, AMA goes into backup.

Note 2: This behaviour is normal. The reintegration time (approximately 1.5 min) is longer than the SuperNode Billing Application (SBA) tolerance to waiting for acknowledgement for storage of billing data.

Undo the thumbscrews located on the top and the bottom of the CPU controller module.

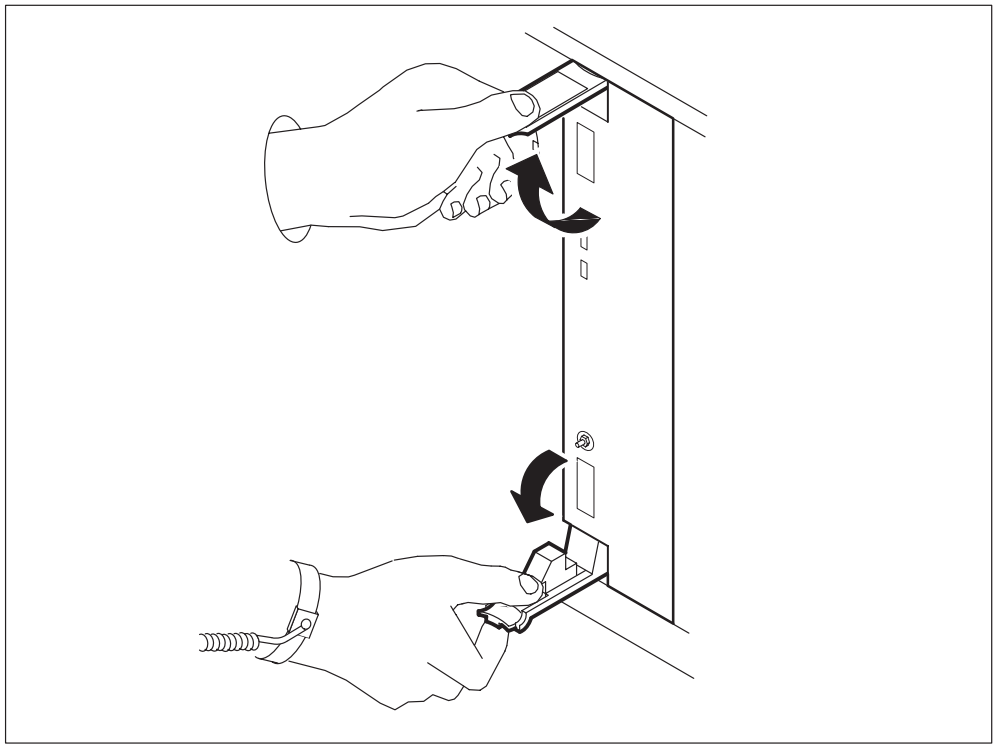
Note: The thumbscrews are the captive type, and cannot be removed from the module.

9 Depress the tips of the locking levers on the face of the CPU controller module.



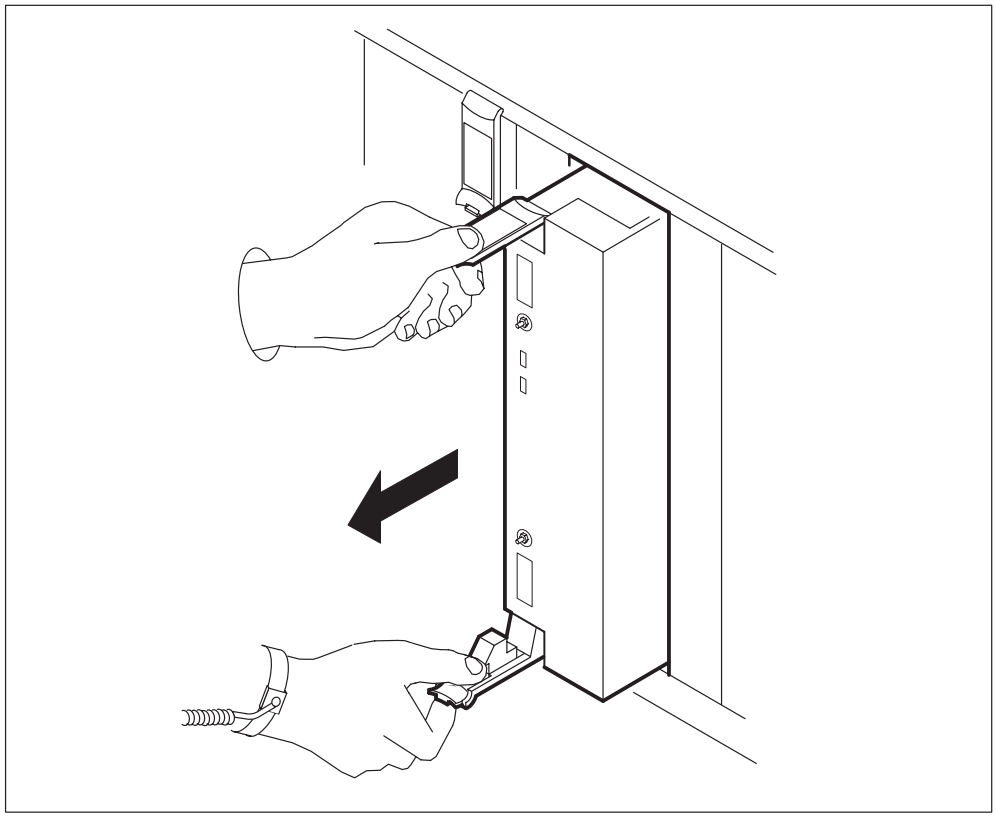
NTRX50FK, NTRX50FL, NTRX50FM
CPU controller module (continued)

10 Open the locking levers on the face of the module by moving the levers outwards.



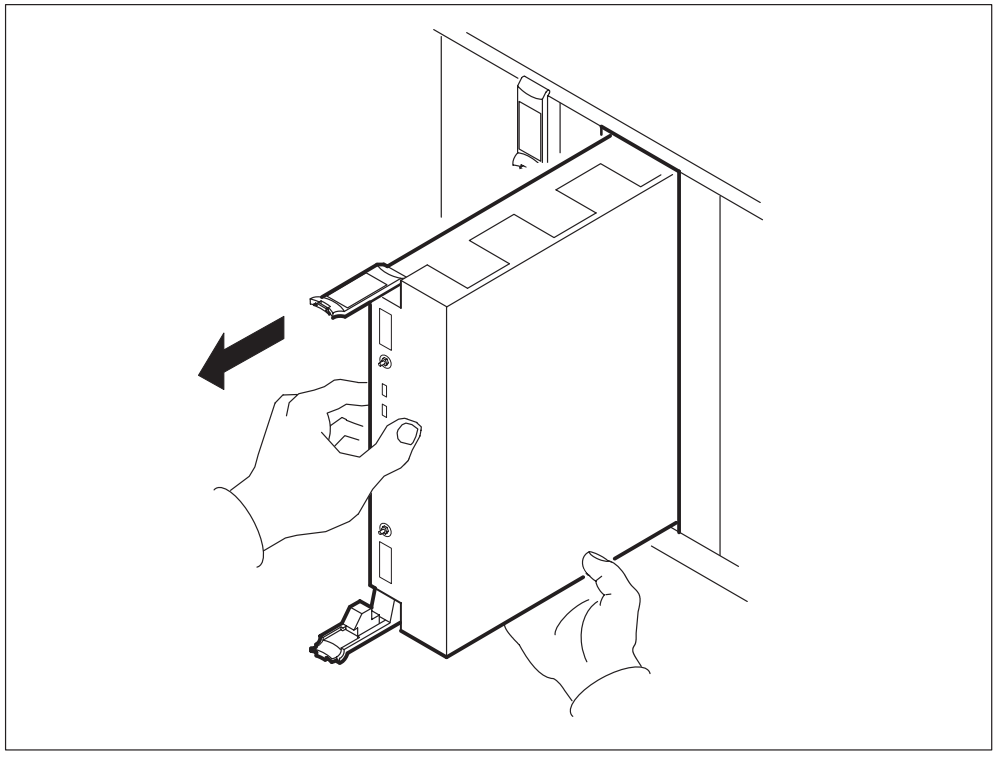
NTRX50FK, NTRX50FL, NTRX50FM
CPU controller module (continued)

11 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (continued)

12 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.

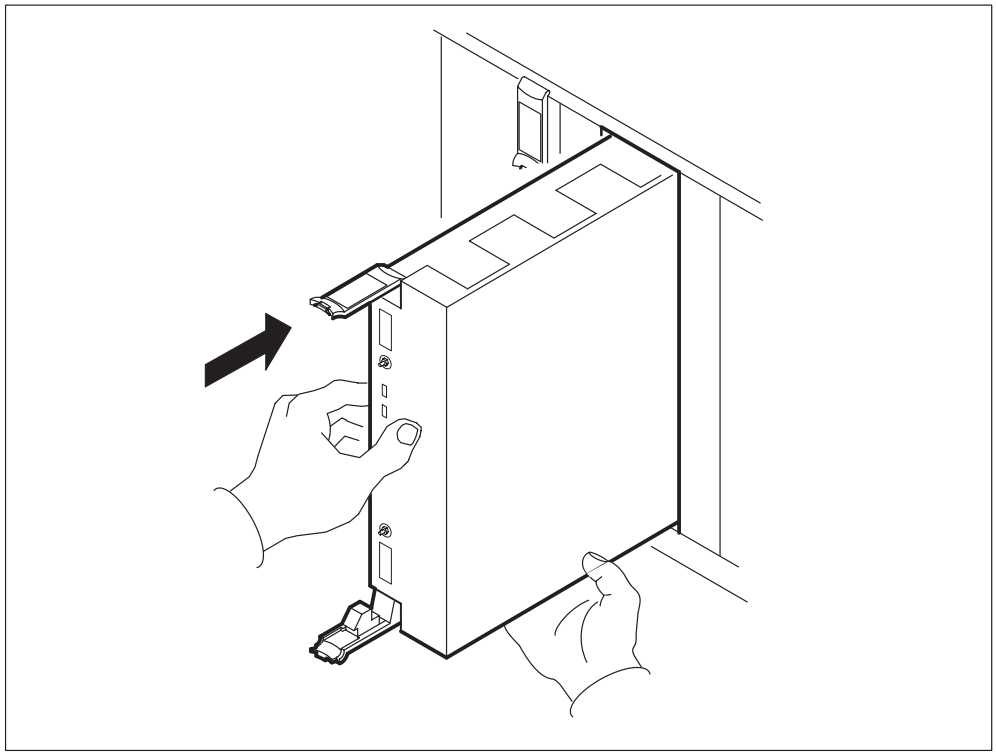


13 Place the module you have removed in an ESD protective container.

14 Insert the replacement module into the SDM shelf.

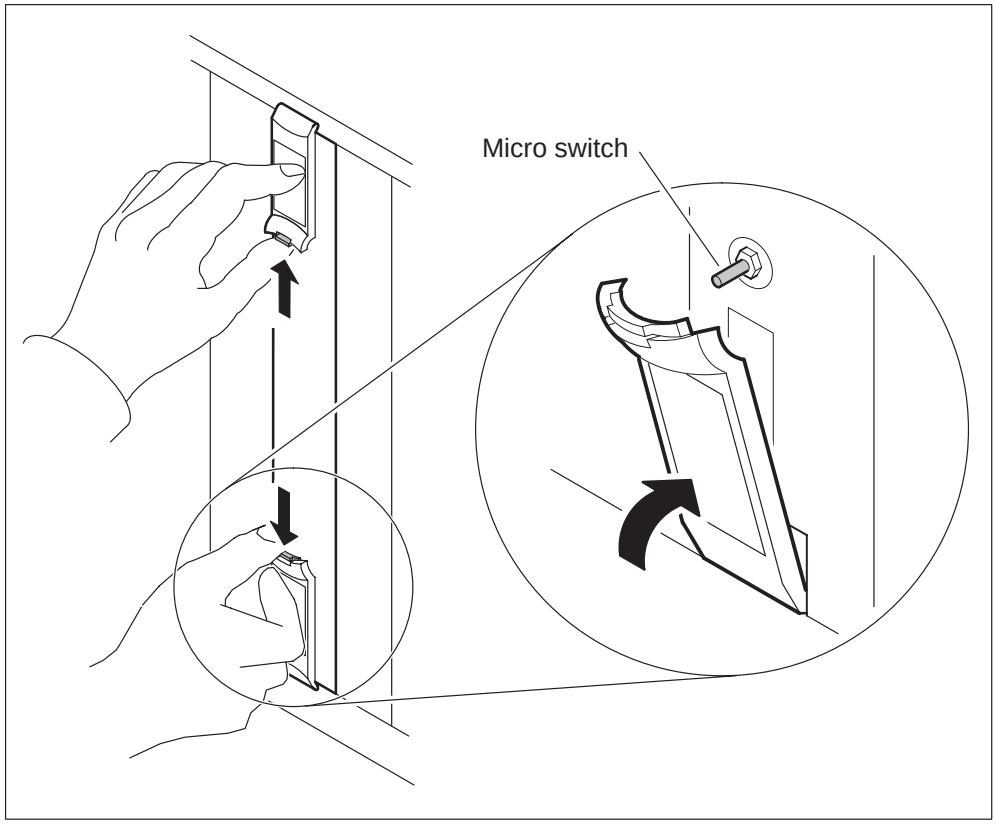
NTRX50FK, NTRX50FL, NTRX50FM
CPU controller module (continued)

15 Gently slide the module into the shelf until it is fully inserted.



NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (continued)

16 Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



17 Tighten the thumbscrews on the module.

Note: When the replacement CPU controller module is inserted, both LEDs on the module turn on and off briefly, indicating that the module is seated correctly, is receiving power, and has passed its self tests. The in-service light on the CPU controller module then turns off, and the out-of-service light turns on.

NTRX50FK, NTRX50FL, NTRX50FM CPU controller module (end)

At the local or remote VT100 console

18 At the hardware menu level of the RMI, return the CPU controller module to service by typing

>RTS *n* CPU
and pressing the Enter key.

where

n is the domain number of the CPU controller module that you replaced

Note: The domain is 0 if the CPU controller module is in slots 6 and 7, and 1 if it is in slots 10 and 11 of the main chassis.

Example response:

```
Hardware RTS : Domain 0 Device CPU – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS: Domain 0 Device CPU – Command submitted.
```

Note: At the hardware menu level of the RMI, the CPU state changes to “S”, indicating that the CPUs are reintegrating. The reintegration process takes about 2 min to complete, after which the CPU status changes to in-service, indicated by a dot (.). The in-service LED on the CPU controller module is on (green).

19 Allow 5 min for the CPU controller module to complete reintegration and return to service. Then check the status of the CPU controller module, as described in step 18.

If the CPU controller module is	Do
in-service	step 21
not in-service	step 20

20 Contact the personnel responsible for the next level of support.

21 You have completed this procedure.

NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module

Application

Use this procedure to replace the I/O controller module, located at the front of the main chassis (slots 2 and 3, and 13 and 14) or the I/O expansion chassis of a fault-tolerant SDM. (The slot number in the I/O expansion chassis is not restricted.)

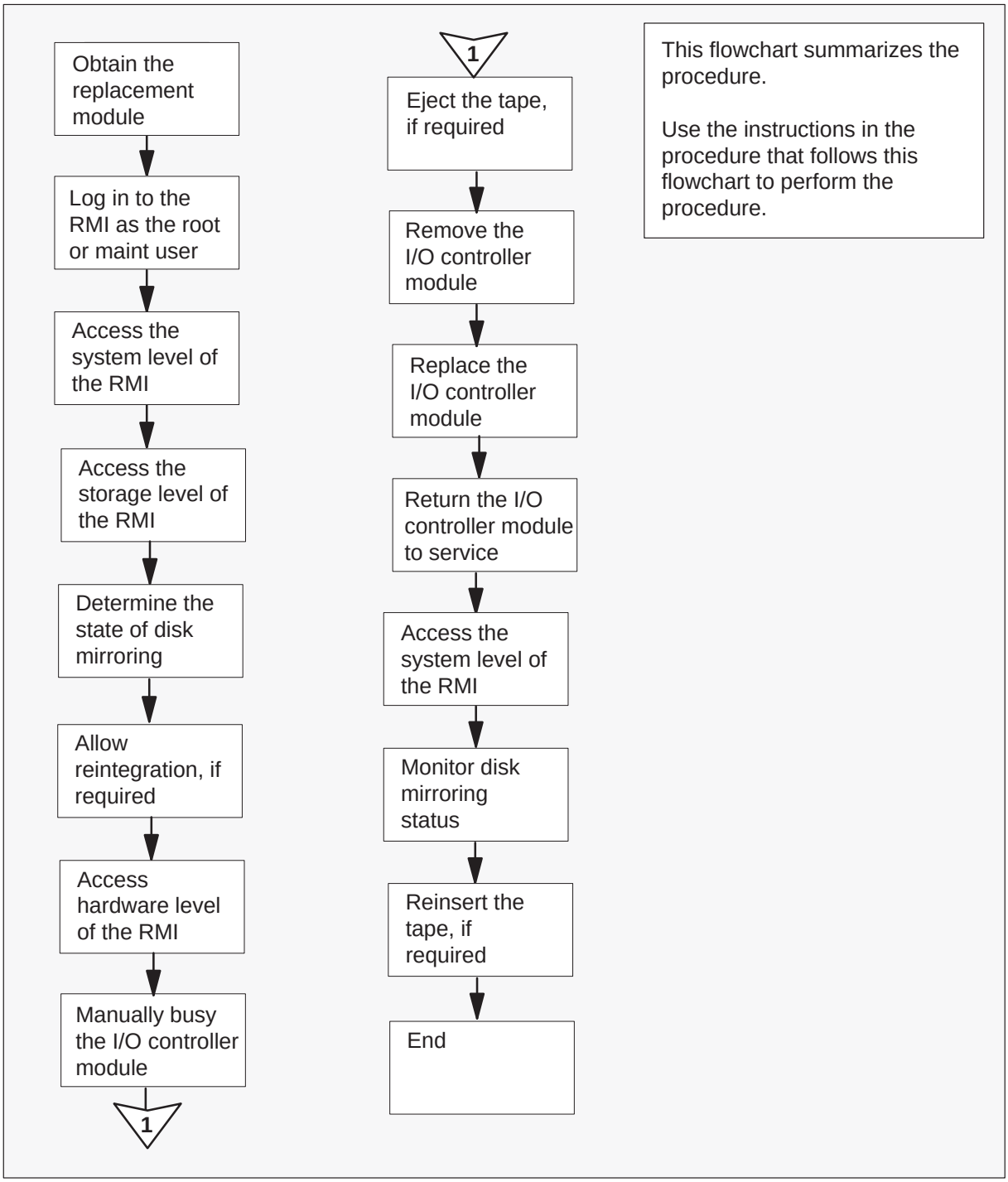
Nortel PEC	Name
NTRX50FQ	I/O controller module with 2-Gbyte disk drive, digital audio tape (DAT), and Ethernet
NTRX50FU	I/O controller module with two 2-Gbyte disk drives and Ethernet
NTRX50GN	I/O controller module with 4-Gbyte disk drive, DAT and Ethernet
NTRX50GP	I/O controller module with two 4-Gbyte disk drives and Ethernet

Action

The following flowchart is only a summary of the procedure. To replace the I/O controller module, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

Summary of Replacing an I/O controller module



NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

Replacing an I/O controller module

1 Obtain a replacement I/O controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the module's top locking lever.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

4 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

5 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

6 Determine the disk mirroring status for each volume group commissioned on the SDM.

Example response:

```
Disk mirroring (rootvg):        Integrating
```

7 Proceed according to the disk mirroring state.

If disk mirroring is in the	Do
Integrating state	step 8
Mirrored or Not Mirrored state	step 9

NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

8 The hard disks that provide mirrored storage for the system are reintegrating. Allow the reintegration process to complete before continuing this procedure. The reintegration process takes about 30 min per Gbyte. (The actual time required varies depending on the amount of data in the volume group, and the current processor load.)

Note: When the disk drive in an I/O controller module (NTRX50GN or NTRX50GN) is being reintegrated, the controller in-service green LED does not flash. Do not attempt to change state or remove any modules when the LED is flashing.

CAUTION
Potential loss of service
Do not continue this procedure beyond this point while the disks are reintegrating. If you remove an I/O controller module from service during the reintegration process, you will cause a reintegration failure which may require service-affecting manual recovery action.

Go to step 6.

9 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

Note: If there is a tape in the tape drive, eject it now.

10 Manually busy the I/O controller module that you wish to replace by typing

>BSY *domain* DSK*n*
and pressing the Enter key.

where

domain is the domain number (0 or 1) of the I/O controller module that you are replacing

n is the disk number that you are replacing (Use the Locate command to determine the disk number of the module.)

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slots 2 and 3 or slots 4 and 5, of the main chassis
- 1 if the module is located in slots 13 and 14 or slots 15 and 16, of the main chassis

- 0 if the module is located in any two slots from 1 to 8 in the I/O expansion chassis
- 1 if the module is located in any two slots from 9 to 16 of the I/O expansion chassis

Note: The parameter “DSK” selects the disk on the I/O controller module. All other devices on the I/O controller module are busied automatically. (The example response shown is displayed when you busy the devices on the NTRX50FQ module.)

Example response:

```
Hardware Bsy – Domain 0 Device DSK2

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

11 Confirm the Bsy command by typing

>Y

and pressing the Enter key.

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

Example response:

```
Hardware Bsy : Domain 0 Device DSK2 – Command initiated.
Please wait...
```

When the Bsy command is finished, the “Please wait...” message and the command confirmation disappear. The word “initiated” also changes to “submitted”. (The example response shown is displayed when you busy the devices on the NTRX50FQ module.)

Example response:

```
Hardware Bsy : Domain 0 Device DSK2 – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of all devices on the I/O controller module changes to “M”.

At the front of the SDM

13

WARNING

Static electricity damage

Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

14

CAUTION
Potential service interruption
Remove only the I/O controller module that you busied in step 10. The in-service LED on this module is off, and the out-of-service LED is on (red).

Do not remove the remaining, in-service module. The in-service LED on the in-service module is on (green), and the out-of-service LED is off.

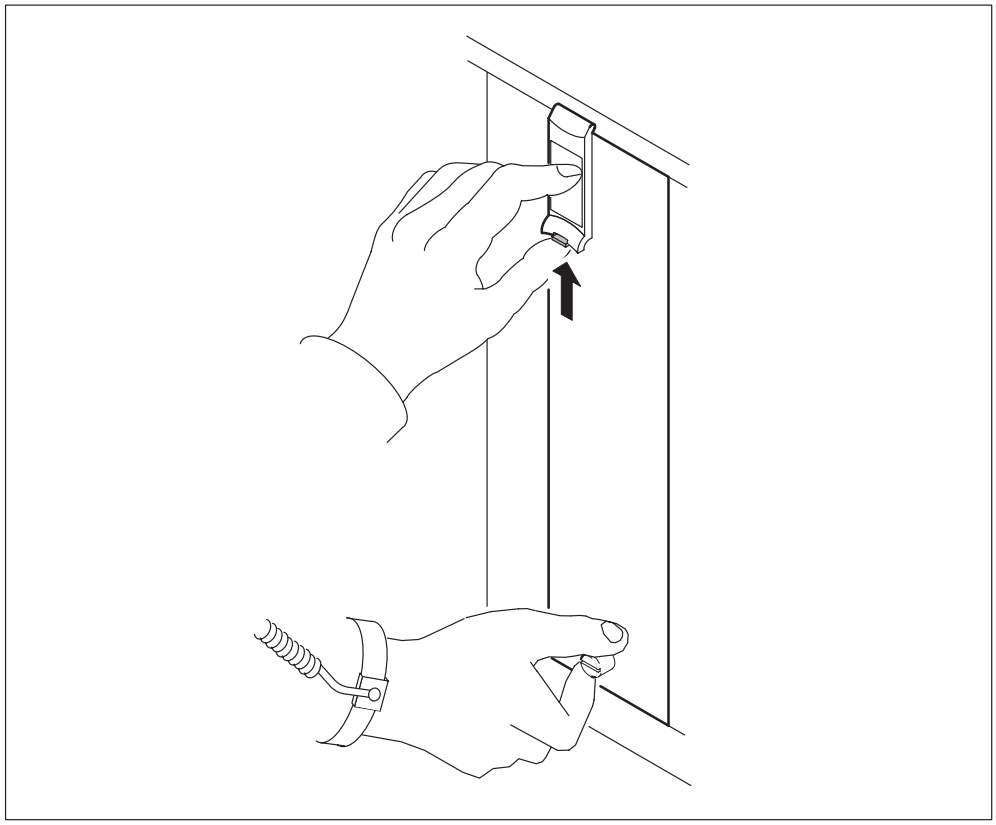
CAUTION
Potential service interruption
I/O controller modules provide mirrored disk storage for the root or data volume groups. If you remove the in-service I/O controller module, you will cause a complete loss of service on the SDM. If you remove the in-service NTRX50FQ module, you will also cause an automatic reboot of the SDM.

Undo the thumbscrews located on the top and the bottom of the I/O controller module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

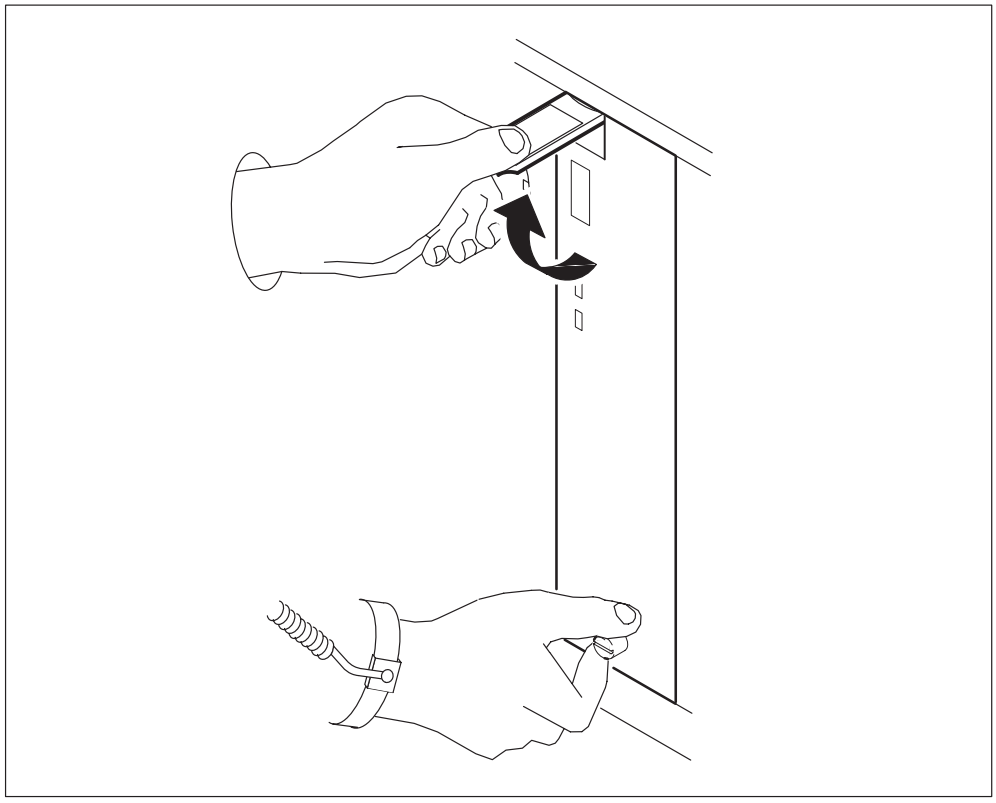
NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

15 Depress the tip of the locking lever on the face of the I/O controller module.



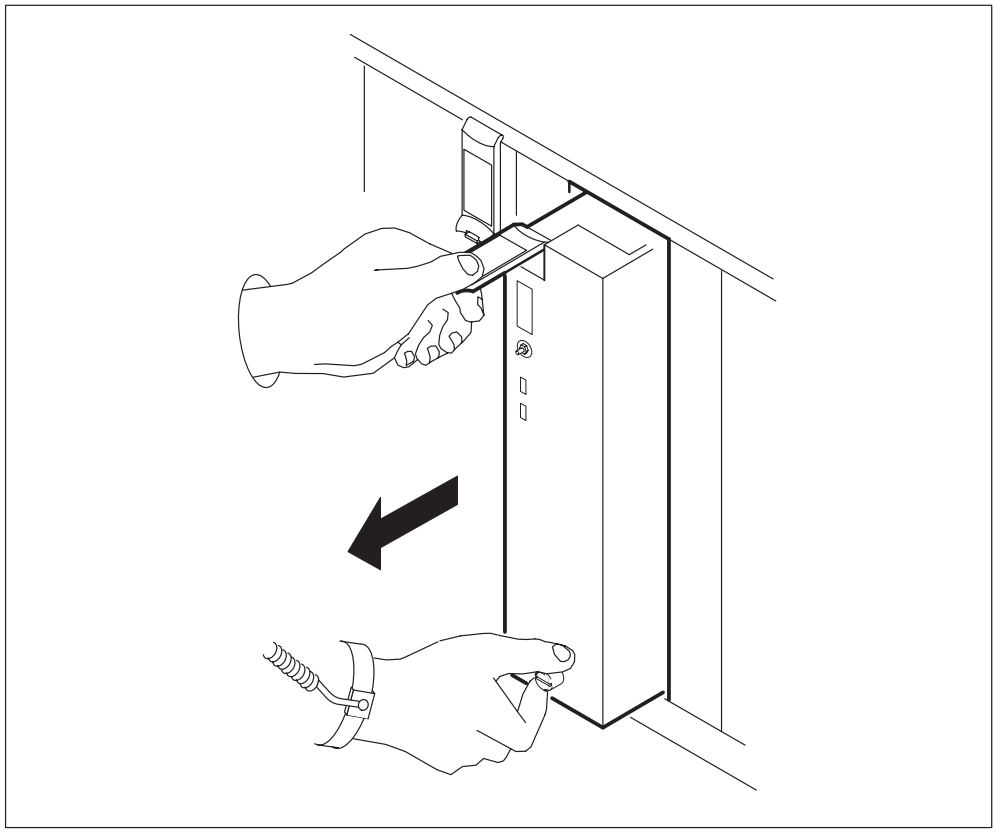
NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP **I/O controller module** (continued)

16 Open the locking lever on the face of the module by moving the lever outwards.



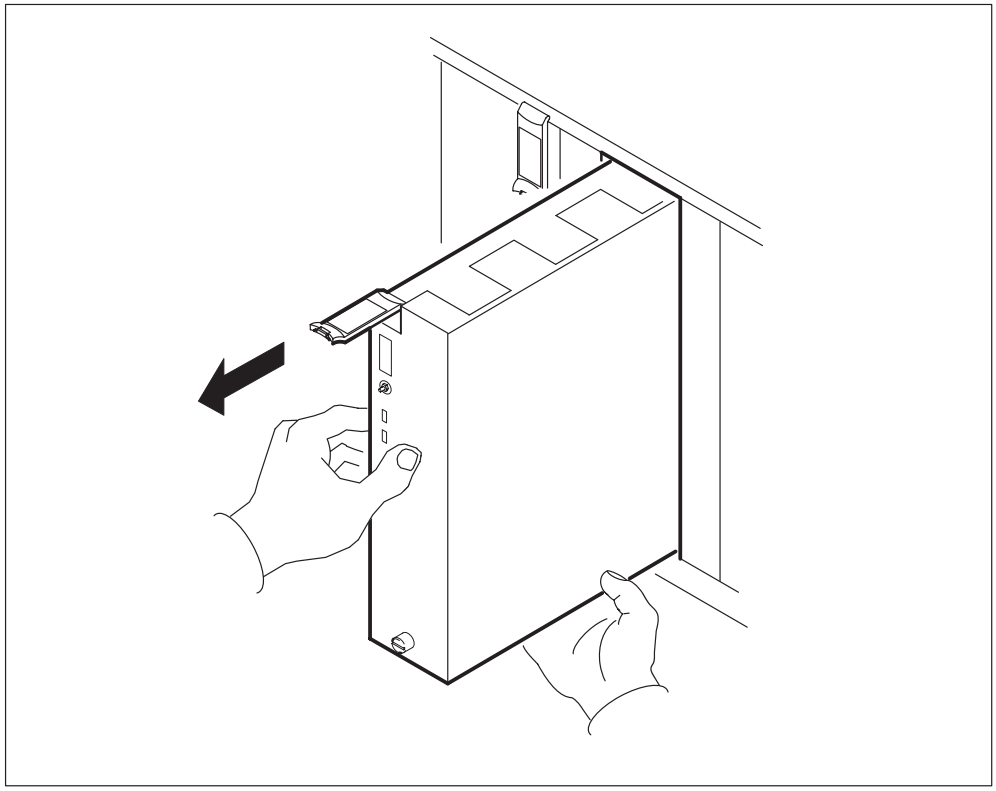
NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

17 While grasping the locking lever, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

18 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.

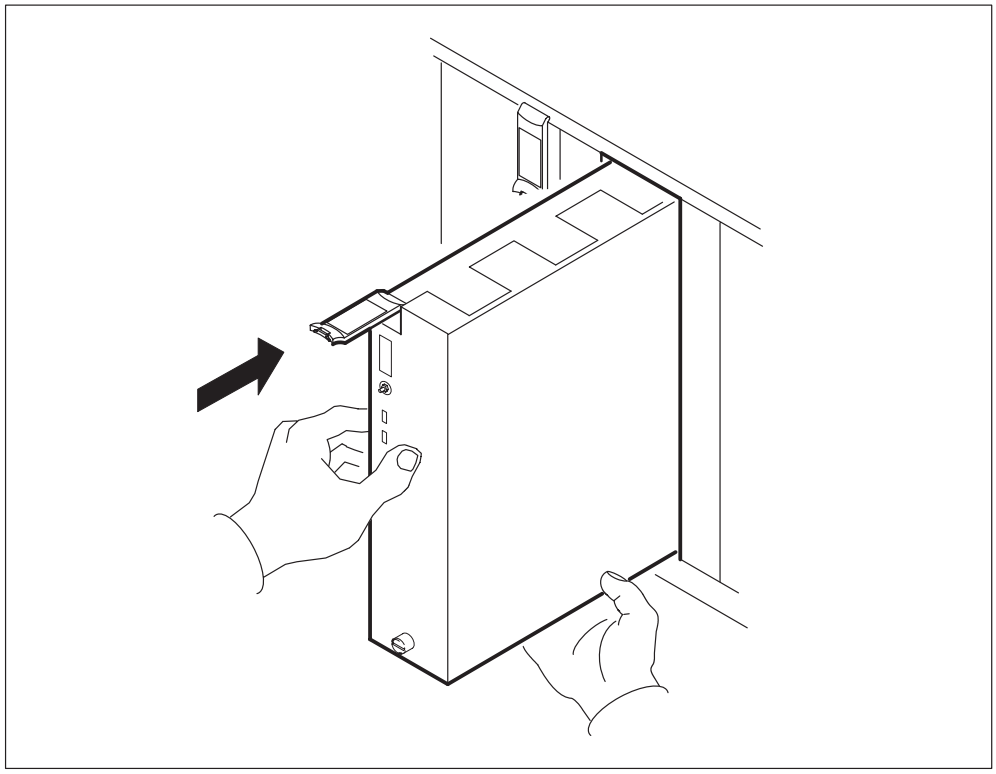


19 Place the module you have removed in an ESD protective container.

20 Insert the replacement module into the SDM shelf.

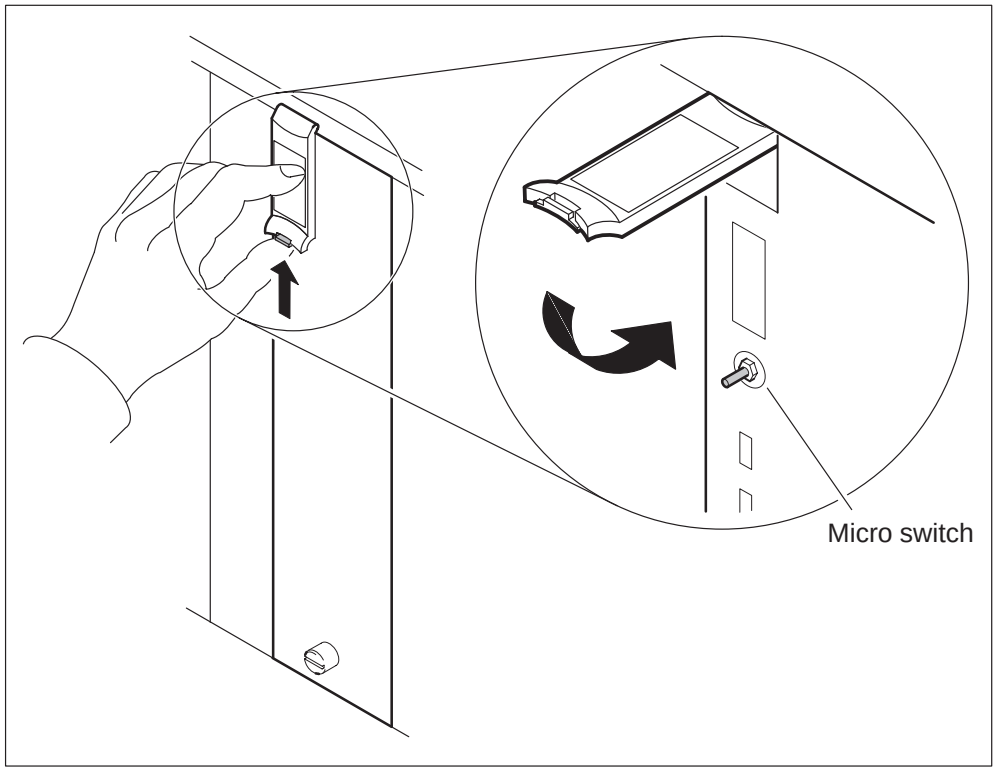
NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

21 Gently slide the module into the shelf until it is fully inserted.



NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (continued)

22 Close the locking lever to secure the module. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.



23 Tighten the thumbscrews on the module.

Note: When the replacement I/O controller module is inserted, both its LEDs turn on and off briefly, indicating that the module is seated correctly, is receiving power, and has passed its self tests. The module's in-service LED then turns off, and its out-of-service LED turns on.

24 At the hardware menu level of the RMI, return the I/O controller module to service by typing

>RTS *domain* DSK*n*
and pressing the Enter key.

where

domain	is the domain number of the I/O controller module that you replaced (see step 10)
n	is the disk number that you are replacing. (Use the Locate command to determine the disk number of the module.

NTRX50FQ, NTRX50FU, NTRX50GN, NTRX50GP I/O controller module (end)

Example response:

```
Hardware RTS : Domain 0 Device DSK2 – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 0 Device DSK2 – Command submitted.
```

25 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

26 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

27 Monitor the disk mirroring status. The mirroring status appears as Integrating, indicating that the hard disks that provide root volume group (rootvg) storage for the system are reintegrating. Allow the reintegration process to complete uninterrupted. This process requires about 30 min per Gbyte. (The actual time varies depending on the amount of data on your system, and the processor load at the time.) When disk integration is complete, the disk mirroring status changes to Mirrored.

Note: During disk reintegration, the System-In-Service light on the upper fan tray in the main chassis flashes, and turns solid when disk reintegration is complete.

28 If you removed a DAT tape from the I/O controller module in step 13, reinsert it into the DAT drive.

29 You have completed this procedure.

NTRX50FS
LAN personality module

Application

Use this procedure to replace a LAN personality module, located at the rear of the main chassis (slots 2 and 13) and the I/O expansion chassis in a fault-tolerant SDM. (The slot number in the I/O expansion chassis is not restricted.)

Nortel PEC	Name
NTRX50FS	LAN personality module

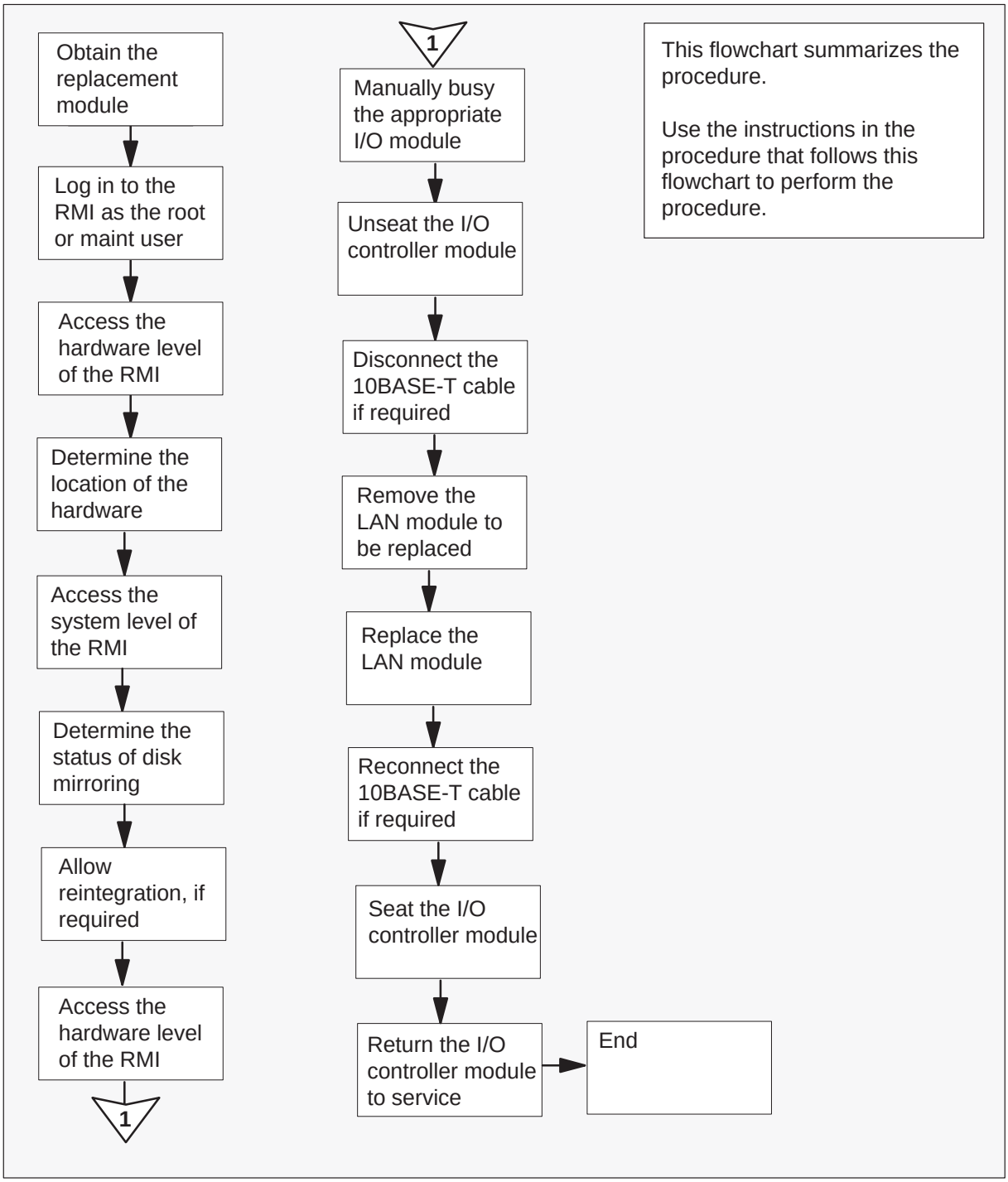
Note: Each I/O controller module must also have an associated LAN personality module (NTRX50FS) installed at the back of the SDM. Ethernet LAN connectivity, however, is only supported by the mandatory NTRX50FQ or NTRX50GN I/O controller modules located in slots 2 and 3, and 13 and 14 at the front of the main chassis.

Action

The following flowchart is only a summary of the procedure. To replace the LAN personality module, use the instructions in the step-action procedure that follows the flowchart.

NTRX50FS
LAN personality module (continued)

Summary of Replacing a LAN personality module



NTRX50FS
LAN personality module (continued)

Replacing a LAN personality module

1 Obtain a replacement LAN personality module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written at the top of the module.

At the local or remote VT100 console

2 Log in to the SDM as the root or maint user.

3 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

4 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

5 Use the Locate command to display the hardware location information for the SDM. Type

>15
and press the Enter key.

6 Determine the PEC and location of the I/O controller module associated with the LAN controller module you wish to locate.

Note: The LAN personality module is indicated by its slot number with location BACK. Its associated I/O controller module is located in the same slot with location FRNT (front).

The example shows a partial display of the information generated from the Locate command. The PEC of the I/O controller module is NTRX50FQ, and the module is located at the front of the main chassis in slot 13.

Press the Enter key to get the command line.

Example response:

```
Site  Flr  RPos Bay_id Shf Description  Slot  EQPEC
HOST  01   A02  CSDM SDMM                13  NTRX50FQ FRNT
HOST  01   A02  CSDM SDMM                13  NTRX50FS BACK
```

7 Access the system (Sys) menu level of the RMI by typing

>SYS
and pressing the Enter key.

8 Access the storage menu level of the RMI by typing

>5
and pressing the Enter key.

NTRX50FS
LAN personality module (continued)

Example response:

```
Disk mirroring (rootvg):        Integrating
```

9 From the RMI display, determine the disk mirroring status for the volume group stored on the I/O controller module determined in step 6.

10 The hard disks that provide mirrored storage for the system are reintegrating. Allow the reintegration process to complete before continuing this procedure. The reintegration process takes about 30 min per Gbyte. (The actual time required varies upwards or downwards depending on the amount of data in the volume group, and the current processor load.)

CAUTION
Potential loss of service
Do not continue this procedure beyond this point while the disks are reintegrating. If you remove an I/O controller module from service during the reintegration process, you will cause a reintegration failure which may require service-affecting manual recovery action.

Go to step 5.

11 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

12 Manually busy the I/O controller module associated with the LAN personality module you wish to replace by typing

>BSY *n* ETH
and pressing the Enter key.

where

n is the domain number (0 or 1) of the LAN personality module that you are replacing

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slot 2 of the main chassis
- 1 if the module is located in slot 13 of the main chassis
- 0 if the module is located in any two slots from 1 to 8 in the I/O expansion chassis
- 1 if the module is located in any two slots from 9 to 16 of the I/O expansion chassis

NTRX50FS
LAN personality module (continued)

Note: The parameter “ETH” selects the Ethernet LAN controller device on the I/O controller module. All other devices on the I/O controller module are busied automatically.

Example response:

```
Hardware Bsy – Domain 0 Device ETH

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

13 If you wish to busy the module, type

>Y

and press the Enter key.

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

Example response:

```
Hardware Bsy : Domain 0 Device ETH – Command initiated.
Please wait...
```

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

Example response:

```
Hardware Bsy : Domain 0 Device ETH – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of all devices on the I/O controller module changes to “M”.

At the front of the SDM

15

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Press the eject button to remove the tape (if present) from the tape drive.

NTRX50FS
LAN personality module (continued)

16

CAUTION
Potential service interruption
Unseat only the I/O controller module that you busied in step 12, and not the corresponding I/O controller module in the other I/O domain. The in-service LED on the module busied in step 12 is off, and the out-of-service LED is on (red).

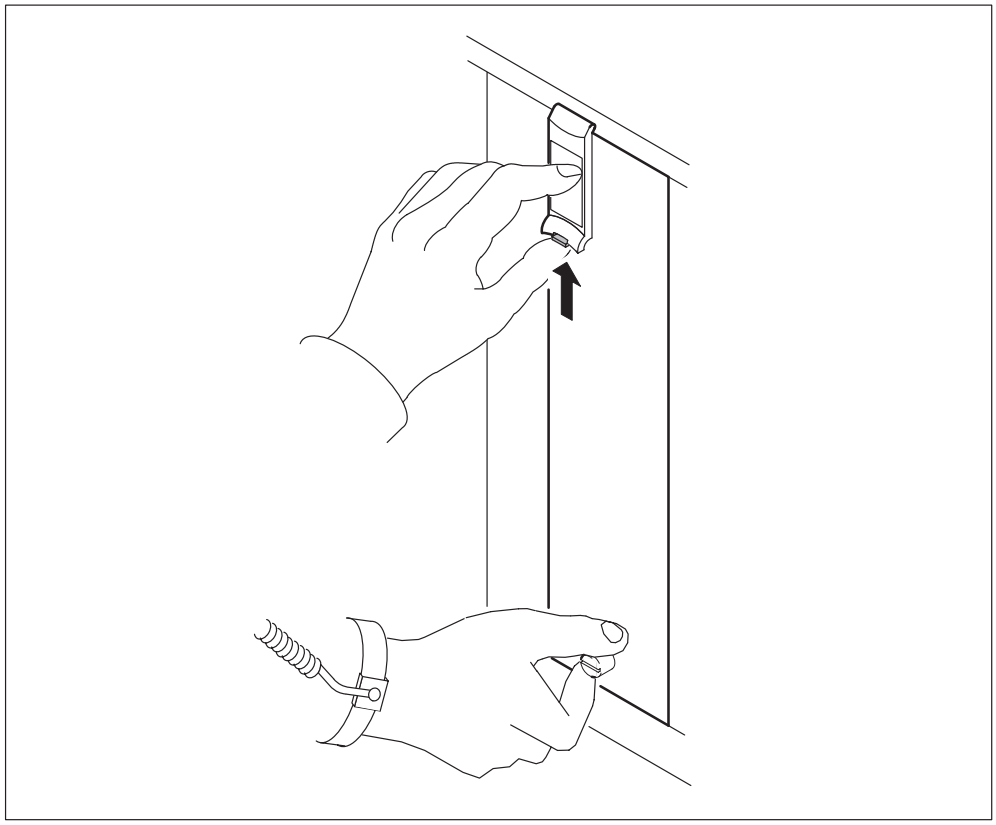
CAUTION
Potential service interruption
The NTRX50FQ I/O controller modules provide mirrored disk storage for the root volume group. If you remove the remaining in-service NTRX50FQ I/O controller module, you will cause an automatic reboot and a complete loss of service on the SDM.

Undo the thumbscrews located on the top and bottom of the I/O controller module associated with the LAN personality module you wish to replace.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

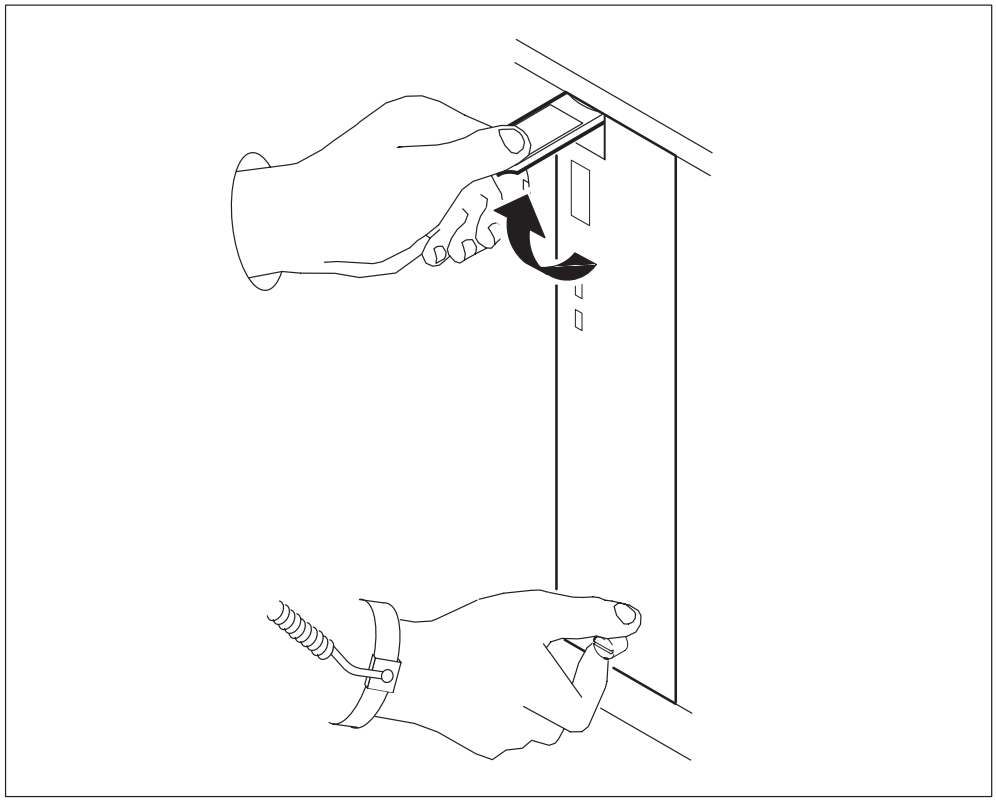
NTRX50FS
LAN personality module (continued)

17 Depress the tip of the locking lever on the face of the I/O controller module.



NTRX50FS
LAN personality module (continued)

18 Open the locking lever on the face of the module by moving the lever outwards.



NTRX50FS
LAN personality module (continued)

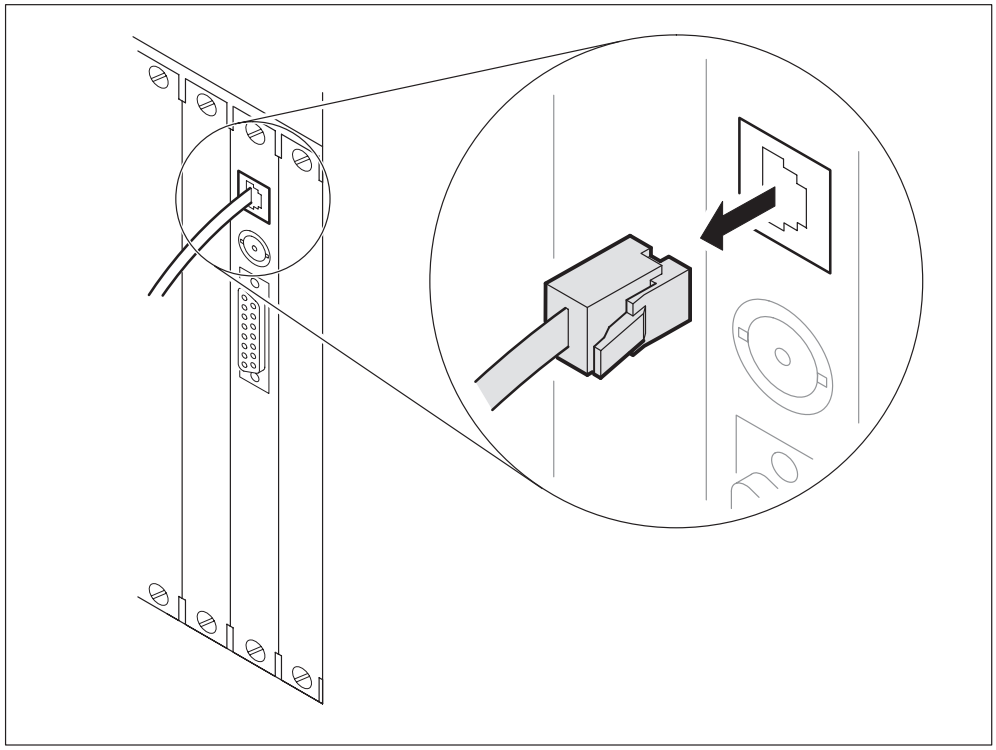
At the back of the SDM

19 Determine what kind of hardware module your SDM has.

If you have	Do
NTRS50FQ or NTRX50GN	step 20
NTRX50FU or NTRX50GP	step 22

20 Label the 10BASE–T cable connected to the LAN personality module you wish to replace.

21 Disconnect the 10BASE-T cable, as shown in the following diagram.

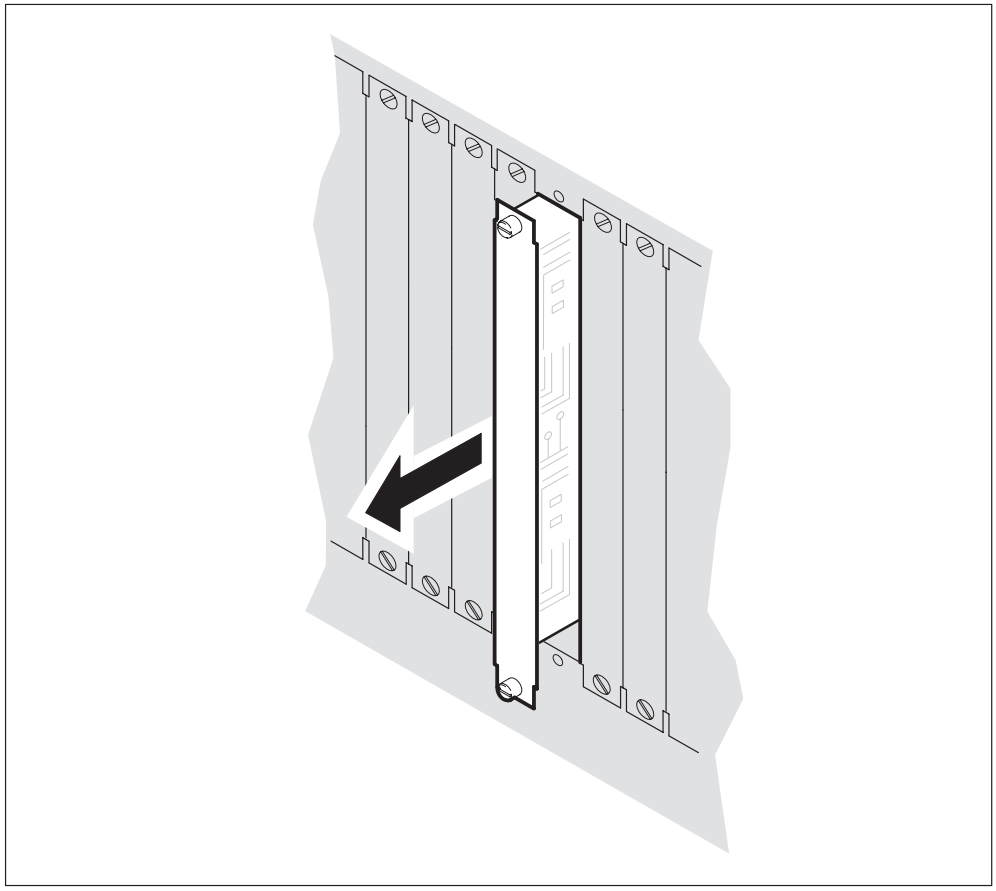


22 Loosen the two thumbscrews located at the top and the bottom of the LAN personality module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

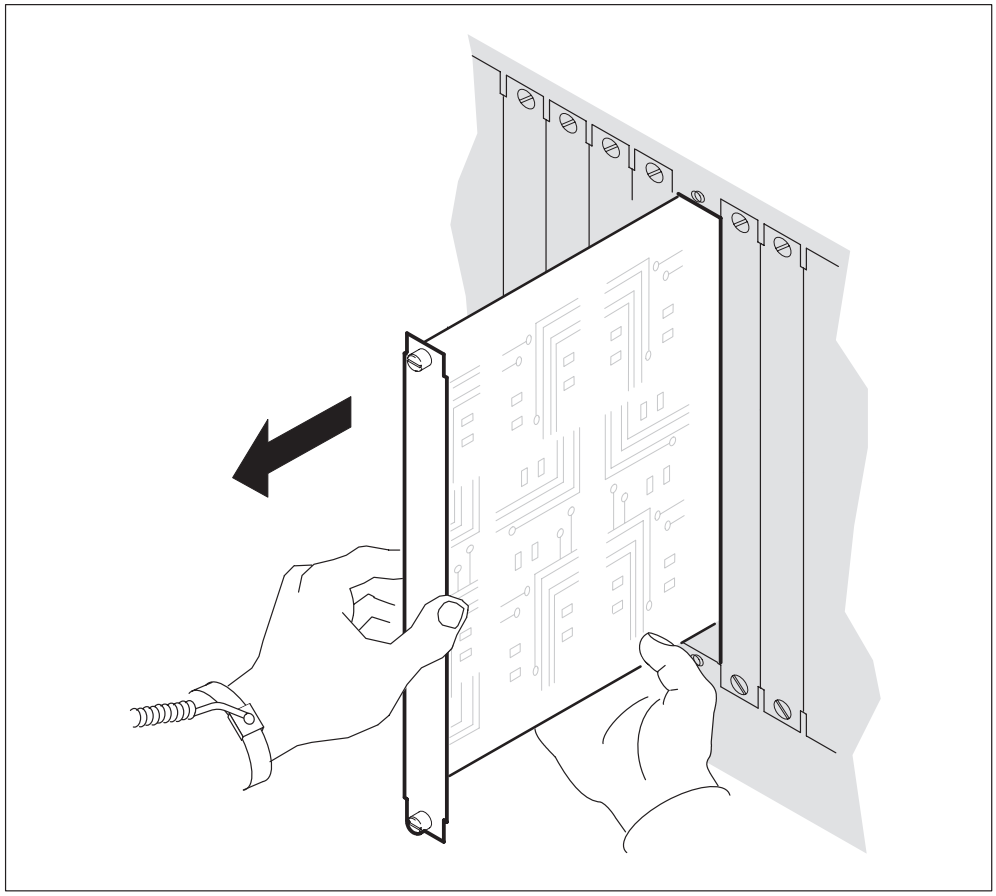
NTRX50FS
LAN personality module (continued)

23 While grasping the thumbscrews, gently pull the LAN personality module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



NTRX50FS
LAN personality module (continued)

24 Hold the LAN personality module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.

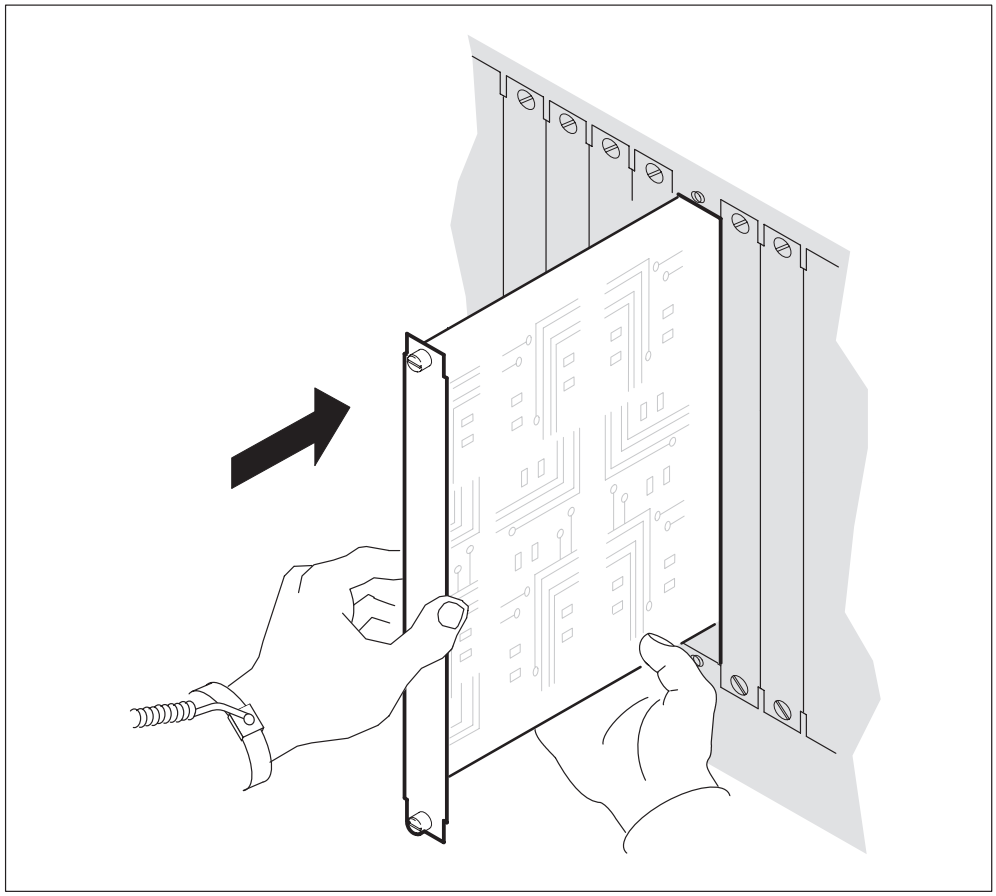


25 Place the LAN personality module you have removed in an ESD protective container.

26 Insert the replacement LAN personality module into the SDM shelf.

NTRX50FS
LAN personality module (continued)

27 Gently slide the LAN personality module into the shelf until it is fully inserted.



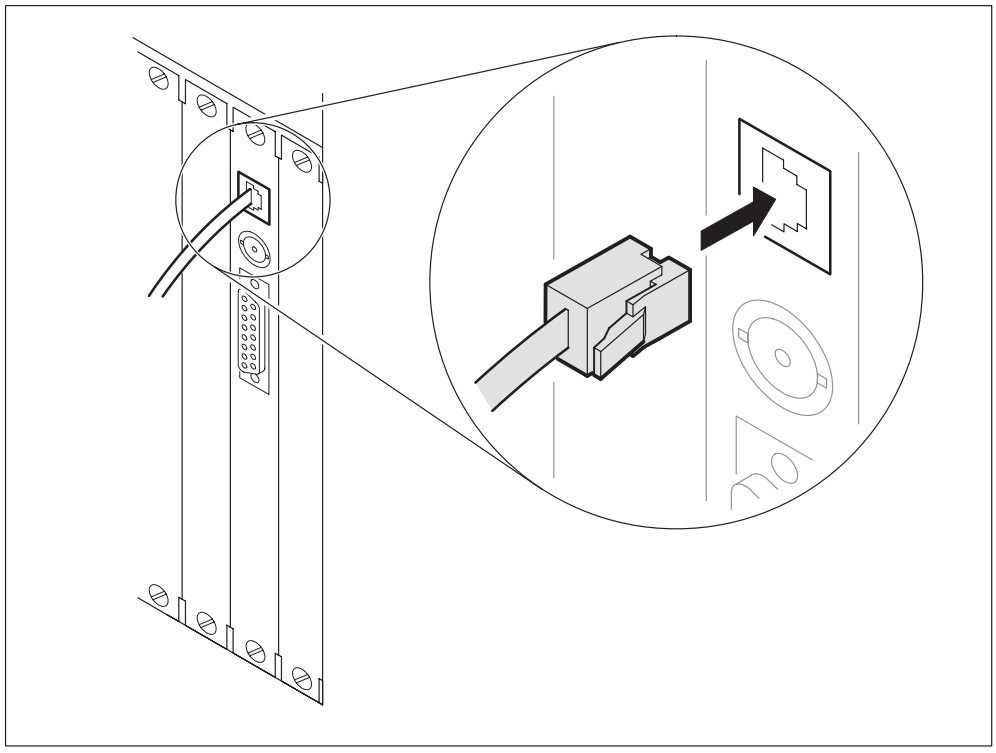
28 Tighten the thumbscrews at the top and the bottom of the LAN personality module.

NTRX50FS
LAN personality module (continued)

29 Determine whether you need to reconnect the 10BASE-T cable.

If you have	Do
NTRS50FQ or NTRX50GN	step 30
NTRX50FU or NTRX50GP	step 31

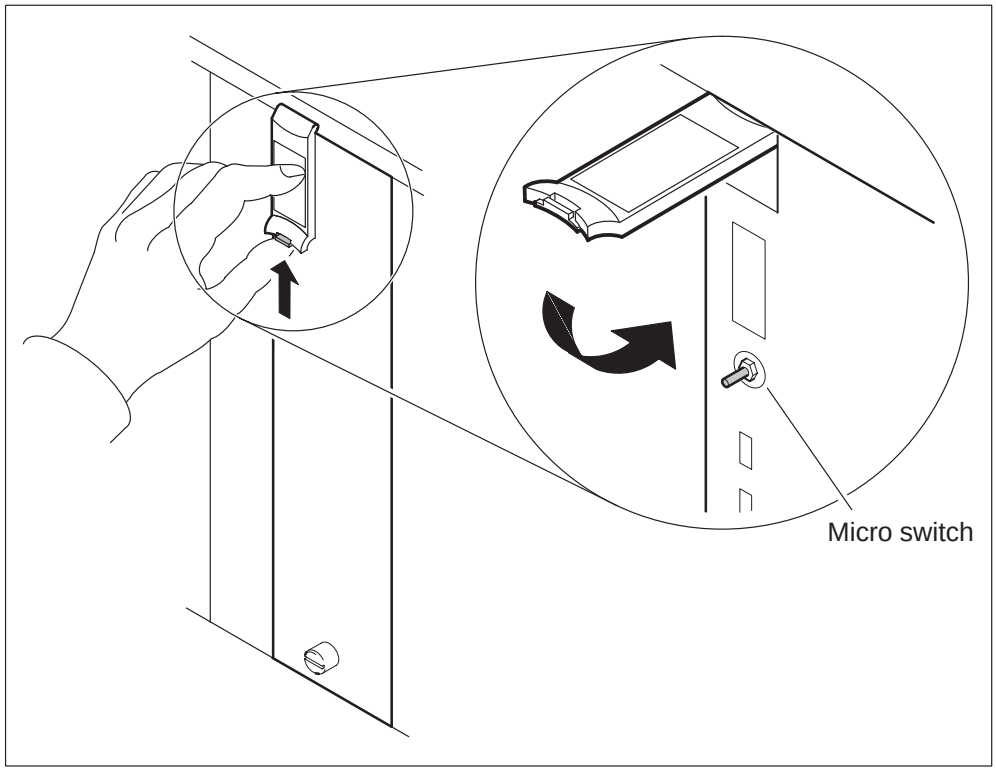
30 Reconnect the 10BASE-T cable to the LAN personality module. If you wish, remove the label that you put on the cable in step 20.



NTRX50FS
LAN personality module (continued)

At the front of the SDM

31 Close the locking lever to secure the I/O controller module you unseated in step 16. Ensure that the top micro switch is lined up with the locking lever to properly seat the module.



32 Tighten the thumbscrews on the I/O controller module.

Note: When the replacement I/O controller module is inserted, both LEDs on the module turn on and off briefly, indicating that the module is seated correctly, is receiving power, and has passed its self tests. The in-service light on the I/O controller module turns off, and its out-of-service light turns on (red).

NTRX50FS
LAN personality module (end)

At the local or remote VT100 console

33 At the hardware menu level of the RMI, return the I/O controller module to service by typing

>RTS *n* ETH
and press the Enter key.

where

n is the domain number (0 or 1) of the I/O controller module you manually busied in step 12.

Example response:

```
Hardware RTS : Domain 0 Device ETH – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 0 Device ETH – Command submitted.
```

34 You have completed this procedure.

NTRX50GA
DS512 controller module

Application

Use this procedure to replace the DS512 controller module, located at the front of the main chassis (slots 1 and 12) of a fault-tolerant SDM.

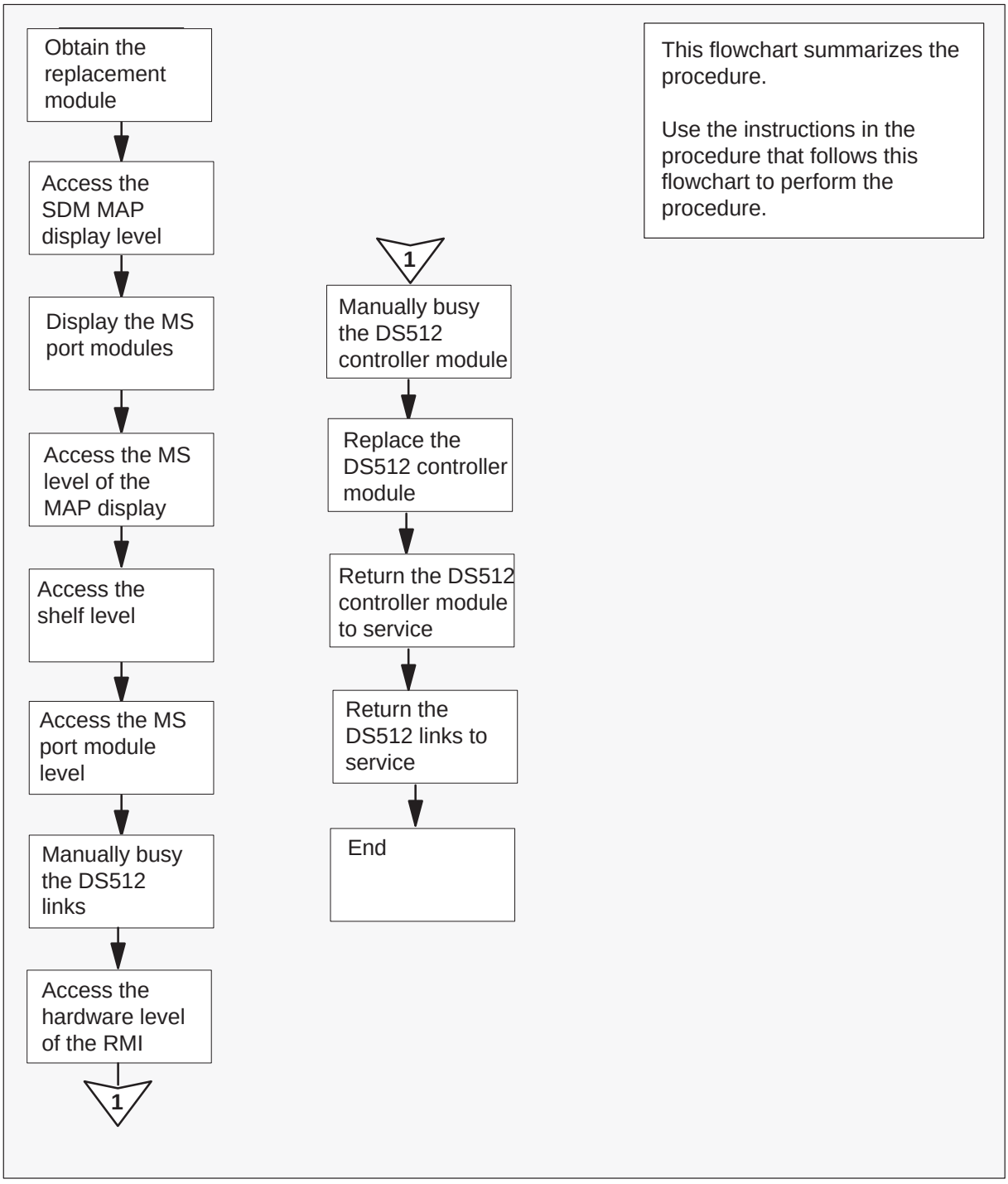
Nortel PEC	Name
NTRX50GA	DS512 controller module

Action

The following flowchart is only a summary of the procedure. To replace the DS512 controller module, use the instructions in the step-action procedure that follows the flowchart.

NTRX50GA
DS512 controller module (continued)

Summary of Replacing a DS512 controller module



NTRX50GA
DS512 controller module (continued)

Replacing a DS512 controller module

1 Obtain a replacement DS512 controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the module's top locking lever.

At the local or remote VT100 console

2 Access the SDM MAP display level by typing

>MAPCI; MTC; APPL; SDM
and pressing the Enter key.

At the MAP display

3 Display the message (MS) port modules which provide the DS512 links to the SDM by typing

>TRNSL
and pressing the Enter key.

Example response:

```
SDM 0 DOMAIN 0 PORT 0 (MS 0:15:0) OK  MsgCnd:Open
SDM 0 DOMAIN 0 PORT 1 (MS 1:15:0) OK  MsgCnd:Open
SDM 0 DOMAIN 1 PORT 0 (MS 0:15:1) OK  MsgCnd:Open
SDM 0 DOMAIN 1 PORT 1 (MS 1:15:1) OK  MsgCnd:Open
```

4 Record the MS port module number associated with the SDM DS512 links. The MS port number is the middle number shown in the parentheses.

Note: In the example response shown in step 3, the port module number is 15.

5 Access the MS level of the MAP display by typing

>MS
and pressing the Enter key.

6 Access the shelf level by typing

>SHELF 0
and pressing the Enter key.

7 Access the MS port module level that is associated with the SDM DS512 links by typing

>CHAIN *cardno*
and pressing the Enter key.

cardno is the MS port module number recorded in step 4

NTRX50GA
DS512 controller module (continued)

8 Manually busy the DS512 link between MS plane 0 and the SDM DS512 controller module you wish to replace by typing

>BSY 0 LINK *link number*
and pressing the Enter key.

where

link number is the MS link number

If	MS link number is
the DS512 controller module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 controller module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to MAN BUSY MS: 0 shelf: 0 chain:19 link:  0 submitted.
Request to MAN BUSY MS: 0 shelf: 0 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane.

9 Manually busy the DS512 link between MS plane 1 and the SDM DS512 controller module you wish to replace by typing

>BSY 1 LINK *link number*
and pressing the Enter key.

where

link number is the MS link number

If	MS link number is
the DS512 controller module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 controller module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to MAN BUSY MS: 1 shelf: 0 chain:19 link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 1 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane 1.

At the local or remote VT100 console

10 Log in to the SDM as the root or maint user.

NTRX50GA
DS512 controller module (continued)

11 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

12 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

13 Manually busy the DS512 controller module by typing

>BSY *n* 512
and pressing the Enter key.

where

n is the domain number (0 or 1) of the DS512 controller module that you are replacing

Use the following list to determine the domain number. The domain number is:

- 0 if the module is located in slot 1 of the main chassis
- 1 if the module is located in slot 12 of the main chassis

Example response:

```
Hardware Bsy – Domain 0 Device 512

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

14 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

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

Example response:

```
Hardware Bsy : Domain 0 Device 512 – Command initiated.
Please wait...
```

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

Example response:

```
Hardware Bsy : Domain 0 Device 512 – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the DS512 controller module changes to “M”.

NTRX50GA
DS512 controller module (continued)

At the front of the SDM

16

WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

17 Undo the thumbscrews located on the top and the bottom of the DS512 controller module.

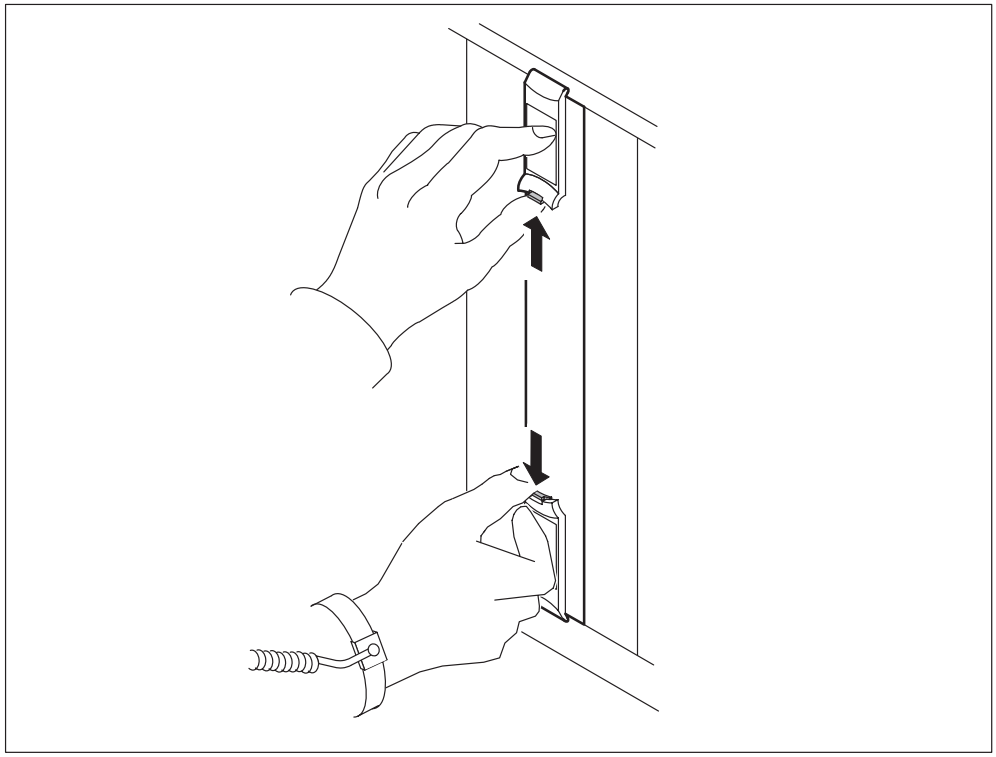
Note: The thumbscrews are the captive type, and cannot be removed from the module.

CAUTION
Potential service interruption
Unseat only the DS512 controller module that you busied in step 13, and not the corresponding DS512 controller module in the other I/O domain. The in-service LED on the module busied in step 13 is off, and the out-of-service LED is on (red).

If you remove the remaining in-service DS512 controller module, you will isolate the SDM from the computing module (CM).

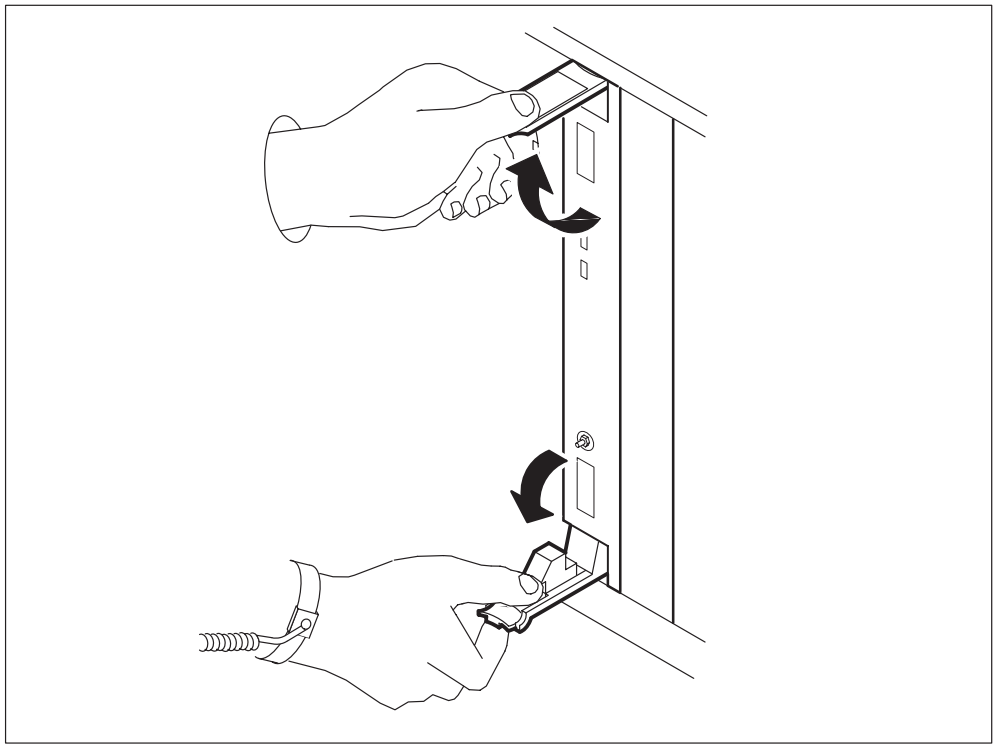
NTRX50GA
DS512 controller module (continued)

18 Depress the tips of the locking levers on the face of the DS512 controller module.



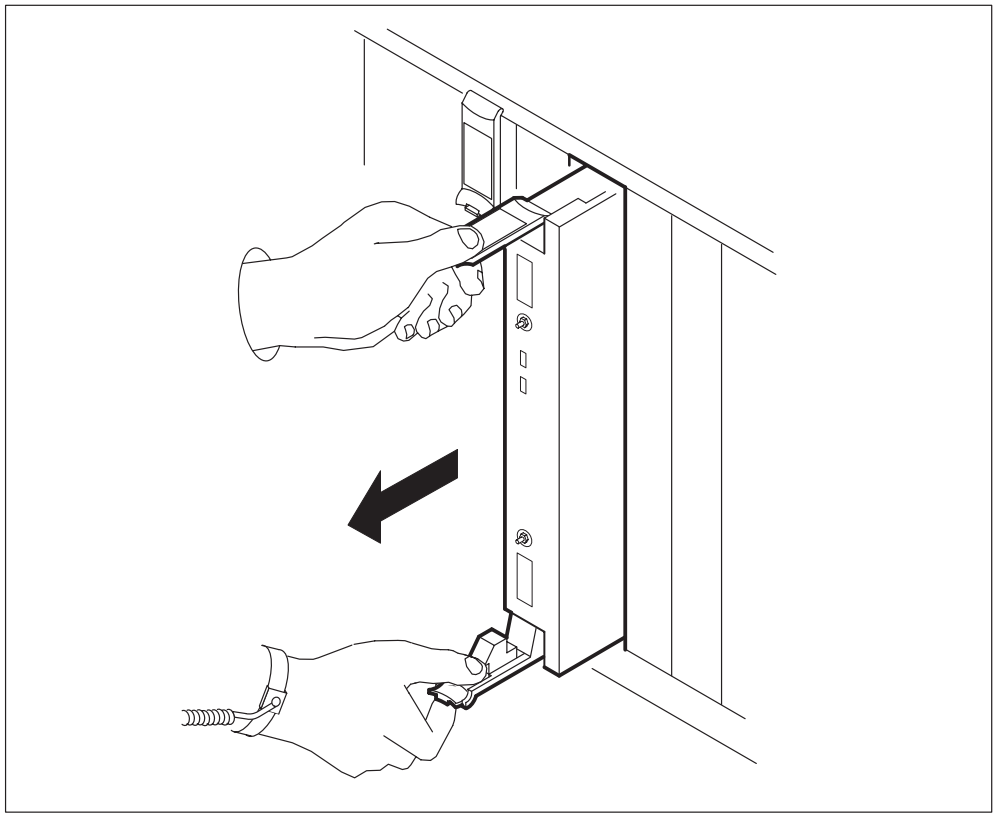
NTRX50GA
DS512 controller module (continued)

19 Open the locking levers on the face of the module by moving the levers outwards.



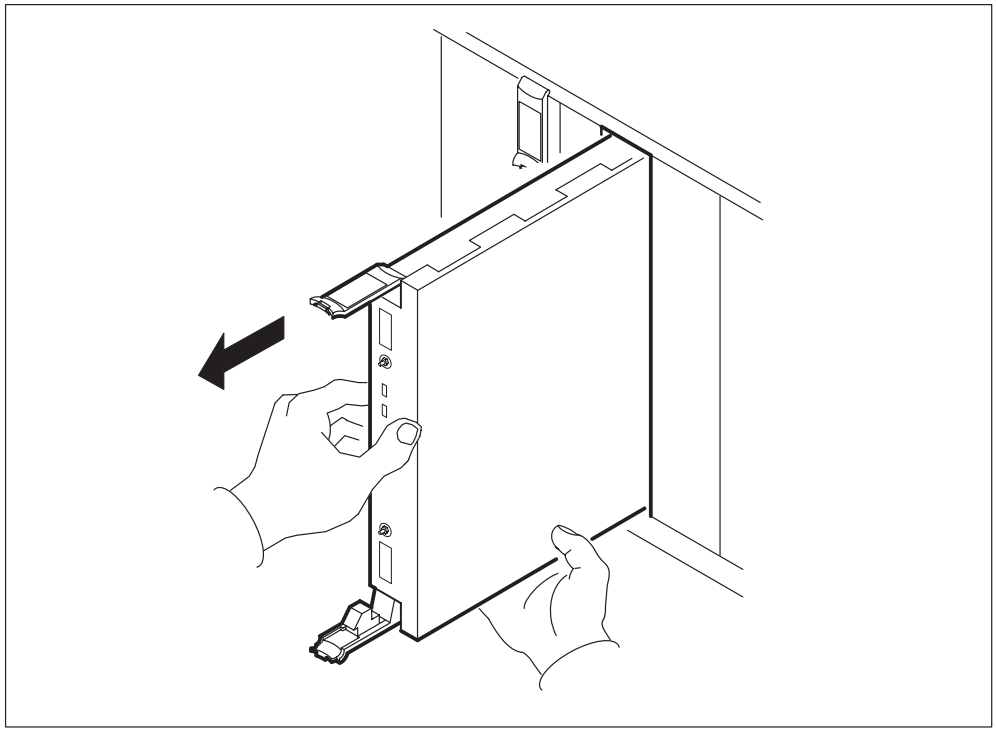
NTRX50GA
DS512 controller module (continued)

20 While grasping the locking levers, gently pull the module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



NTRX50GA
DS512 controller module (continued)

21 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.

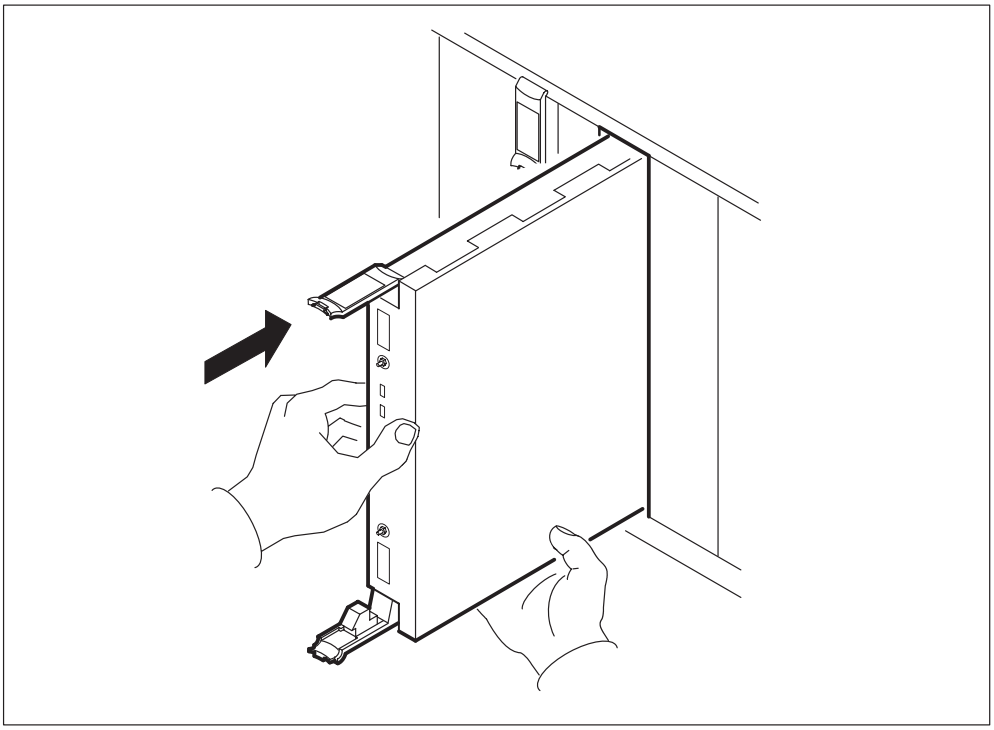


22 Place the module you have removed in an ESD protective container.

23 Insert the replacement module into the SDM shelf.

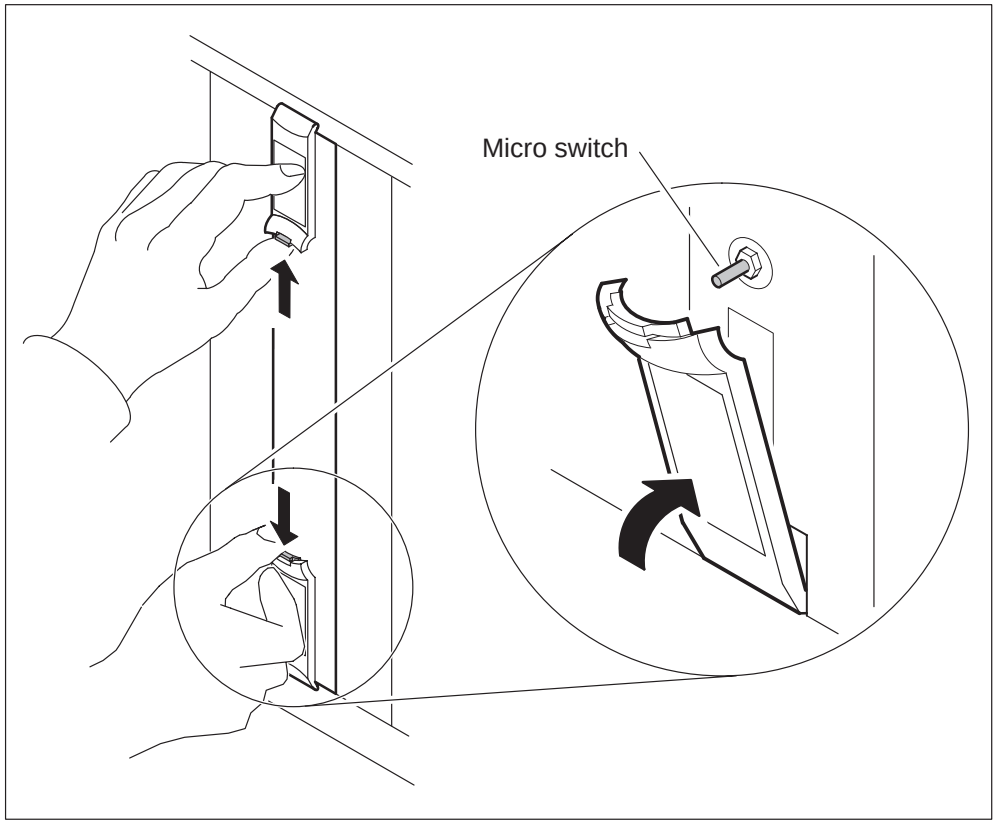
NTRX50GA
DS512 controller module (continued)

24 Gently slide the module into the shelf until it is fully inserted.



NTRX50GA
DS512 controller module (continued)

25 Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



26 Tighten the thumbscrews on the module.

NTRX50GA
DS512 controller module (continued)

At the local or remote VT100 console

27 At the hardware level of the RMI, return the DS512 controller module to service by typing

>RTS *n* 512
and pressing the Enter key.

where

n is the SDM domain number (0 or 1) of the DS512 controller module you replaced. (See step 13.)

Example response:

```
Hardware RTS : Domain 0 Device 512 – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 0 Device 512 – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the DS512 controller module changes to a dot (.), indicating the module has returned to service. The in service LED on the DS512 controller module is on (green).

At the MAP display

28 At the MS port module level of the MAP display (accessed in step 7), return to service the DS512 link between MS plane 0 and the DS512 controller module you replaced by typing

>RTS 0 LINK *linknumber*
and pressing the Enter key.

where

link number is the MS link number you busied in step 8

If	MS link number is
the DS512 controller module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 controller module to be replaced is in SDM domain 1 (slot 12)	1

NTRX50GA
DS512 controller module (end)

Example response:

```
Request to RTS MS: 0 shelf: 0 chain:19 link:  0 submitted.
Request to RTS MS: 0 shelf: 0 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to a dot (.) if the SDM DS512 link is in service. Otherwise, the state for DS512 link changes to a "P".

29 At the MS port module level of the MAP (accessed in step 7), return to service the DS512 link between MS plane 1 and the DS512 controller module you replaced by typing

>RTS 1 LINK *linknumber*

and pressing the Enter key.

where

link number is the MS link number you busied in step 9

If	MS link number is
the DS512 controller module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 controller module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to RTS MS: 1 shelf: 0 chain:19 link:  1 submitted.
Request to RTS MS: 1 shelf: 0 chain:19 link: 1 passed.
```

Note: The state for the DS512 link changes to a dot (.) if the SDM DS512 link is in-service. Otherwise, the state for DS512 link changes to a "P".

30 You have completed this procedure.

NTRX50GH
DS512 personality module

Application

Use this procedure to replace the DS512 personality module, located at the rear of the main chassis (slots 1 and 12) of a fault-tolerant SDM.

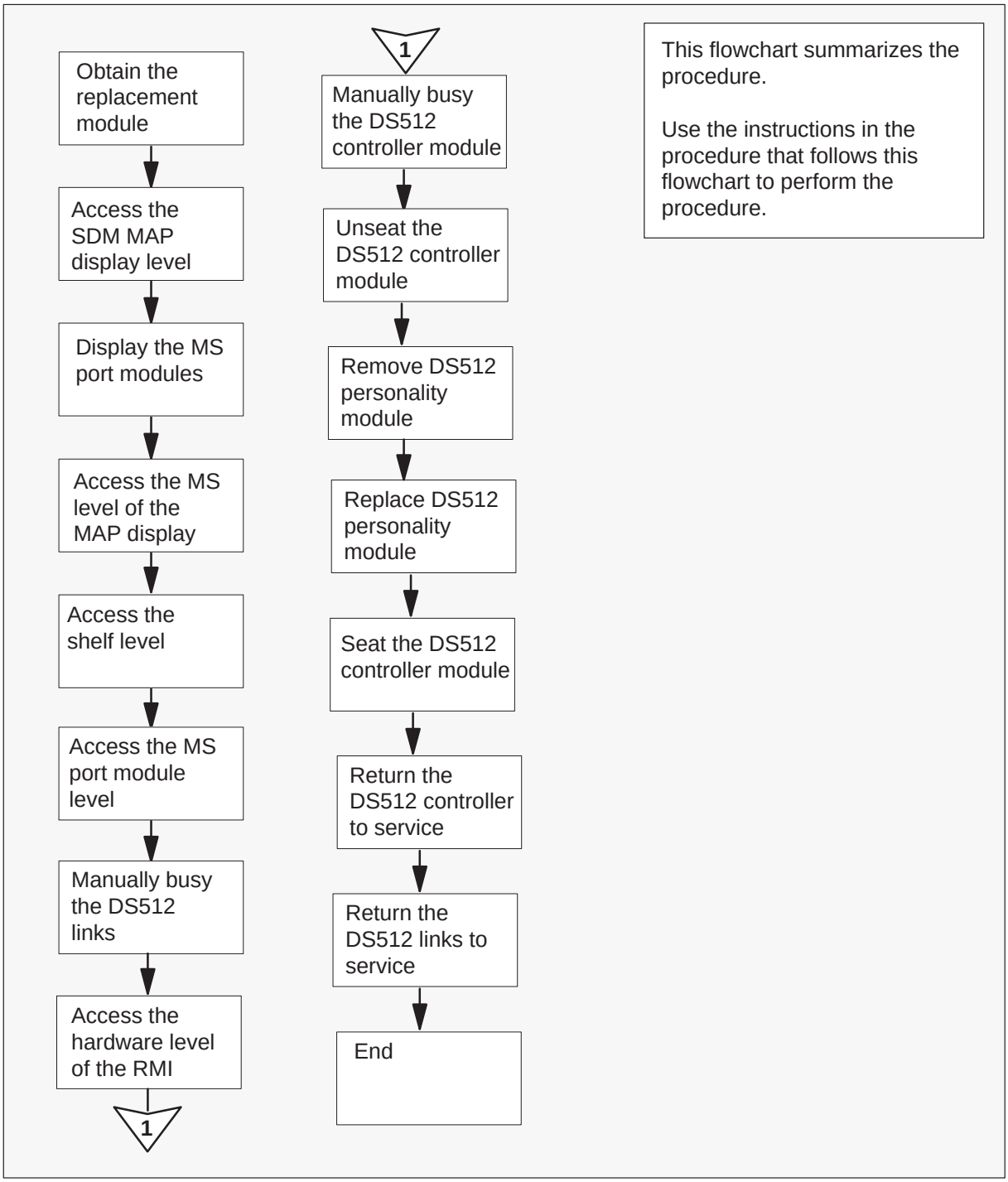
Nortel PEC	Name
NTRX50GH	DS512 personality module

Action

The following flowchart is only a summary of the procedure. To replace the DS512 personality module, use the instructions in the step-action procedure that follows the flowchart.

NTRX50GH
DS512 personality module (continued)

Summary of Replacing a DS512 personality module



NTRX50GH
DS512 personality module (continued)

Replacing a DS512 personality module

1 Obtain a replacement DS512 personality module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written at the top of the module.

At the local or remote VT100 console

2 Access the SDM MAP display level by typing

>MAPCI; MTC; APPL;SDM
and pressing the Enter key.

At the MAP display

3 Display the message (MS) port modules which provide the DS512 links to the SDM by typing

>TRNSL
and pressing the Enter key.

Example response:

```
SDM 0 DOMAIN 0 PORT 0 (MS 0:15:0) OK  MsgCnd:Open
SDM 0 DOMAIN 0 PORT 1 (MS 1:15:0) OK  MsgCnd:Open
SDM 0 DOMAIN 1 PORT 0 (MS 0:15:1) OK  MsgCnd:Open
SDM 0 DOMAIN 1 PORT 1 (MS 1:15:1) OK  MsgCnd:Open
```

4 Record the MS port module number associated with the SDM DS512 links. The MS port number is the middle number shown in the parentheses.

Note: In the example response shown in step 3, the port module number is 15.

5 Access the MS level of the MAP display by typing

>MS
and pressing the Enter key.

6 Access the shelf level by typing

>SHELF 0
and pressing the Enter key.

7 Access the MS port module level associated with the SDM DS512 links by typing

>CHAIN *cardno*
and pressing the Enter key.

cardno is the MS module port number recorded in step 4

NTRX50GH
DS512 personality module (continued)

8 Manually busy the DS512 link between MS plane 0 and the SDM DS512 personality module you wish to replace by typing

>BSY 0 LINK *link number*
and pressing the Enter key.

where

link number is the MS link number

If	MS link number is
the DS512 personality module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 personality module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to MAN BUSY MS: 0 shelf: 0 chain:19 link:  0 submitted.
Request to MAN BUSY MS: 0 shelf: 0 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane.

9 Manually busy the DS512 link between MS plane 1 and the SDM DS512 personality module you wish to replace by typing

>BSY 1 LINK *link number*
and pressing the Enter key.

where

link number is the MS link number

If	MS link number is
the DS512 personality module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 personality module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to MAN BUSY MS: 1 shelf: 0 chain:19 link:  0 submitted.
Request to MAN BUSY MS: 1 shelf: 1 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to “M” for MS plane 1.

At the local or remote VT100 console

10 Log in to the SDM as the root or maint user.

NTRX50GH
DS512 personality module (continued)

11 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

12 Access the hardware (Hw) menu level of the RMI by typing

>HW
and pressing the Enter key.

13 Manually busy the DS512 controller module by typing

>BSY *n* 512
and pressing the Enter key.

where

n is the SDM domain number (0 or 1) of the DS512 personality module you are replacing.

Use the following list to determine the domain number. The domain number is

- 0 if the module is located in slot 1 of the main chassis
- 1 if the module is located in slot 12 of the main chassis

Example response:

```
Hardware Bsy – Domain 0 Device 512

Do you wish to proceed?
Please confirm (“YES”, “Y”, “NO”, “N”)
```

14 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

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

Response:

```
Hardware Bsy : Domain 0 Device 512 – Command initiated.
Please wait...
```

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

Response:

```
Hardware Bsy : Domain 0 Device 512 – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the DS512 controller module changes to “M”. The out-of-service LED on the module is on (red).

NTRX50GH
DS512 personality module (continued)

At the front of the SDM

16

WARNING
Static electricity damage
Wear an electrostatic (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

17 Undo the thumbscrews located on the top and bottom of the DS512 controller module associated with the DS512 personality module you wish to replace.

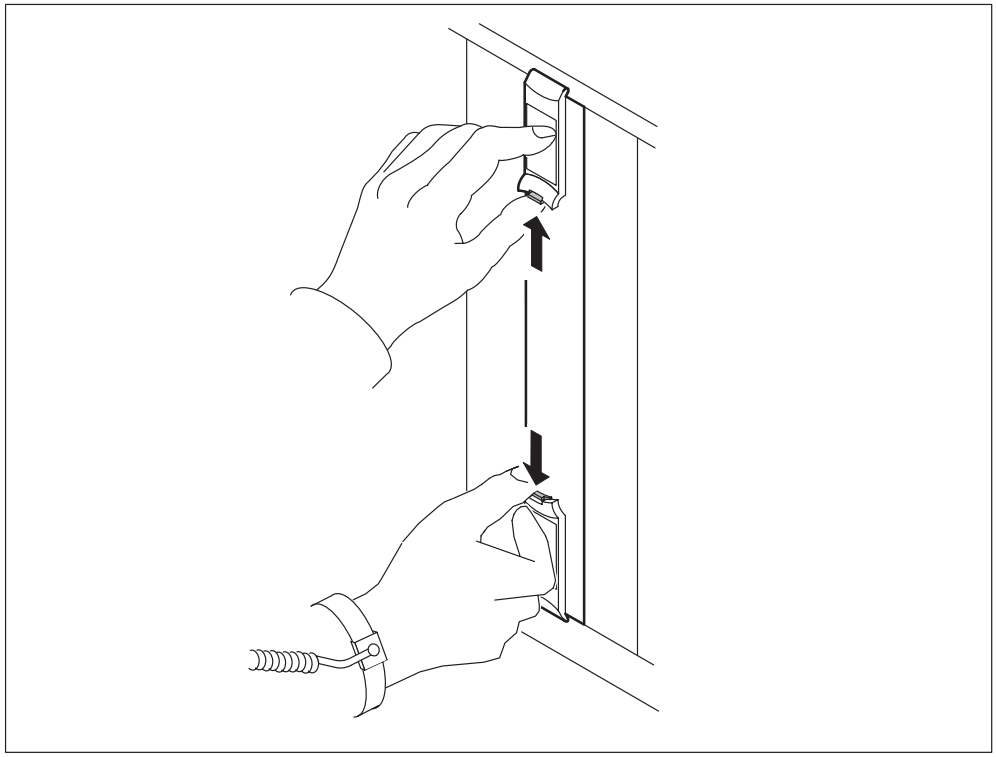
Note: The thumbscrews are the captive type, and cannot be removed from the module.

CAUTION
Potential service interruption
Unseat only the DS512 controller module that you busied in step 13, and not the corresponding DS512 controller module in the other domain. The in-service LED on the module busied in step 13 is off, and the out-of-service LED is on (red).

If you remove the remaining in-service dS512 controller module, you will isolate the SDM from the computing module (CM).

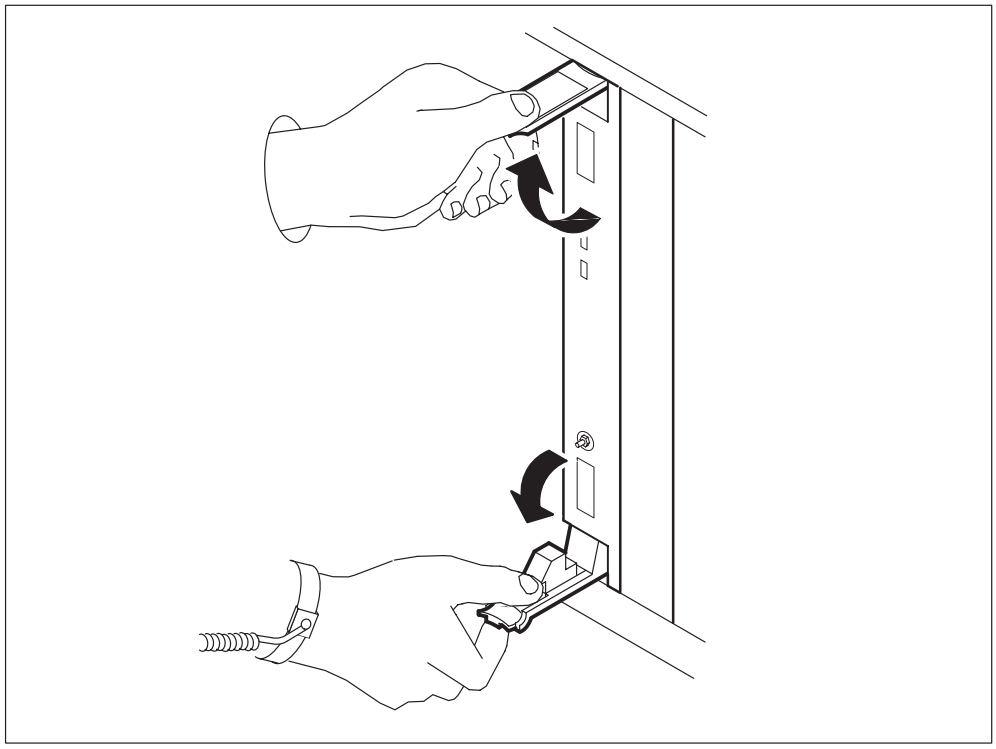
NTRX50GH
DS512 personality module (continued)

18 Depress the tips of the locking levers on the face of the DS512 controller module.



NTRX50GH
DS512 personality module (continued)

19 Open the locking levers on the face of the DS512 controller module by moving the levers outwards.



At the back of the SDM

20 Loosen the two thumbscrews located at the top and the bottom of the DS512 personality module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

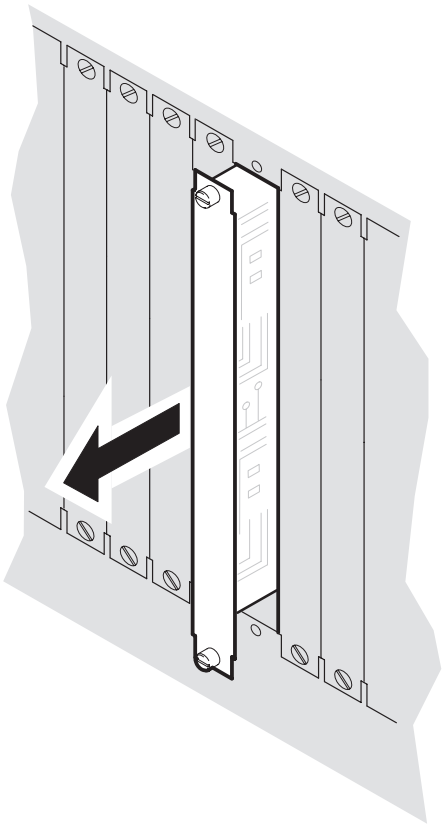
NTRX50GH
DS512 personality module (continued)

21

CAUTION
Disconnecting transmit and receive cables
Do not mix the transmit and receive cables for each domain. If you have not already done so, label these cables to ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

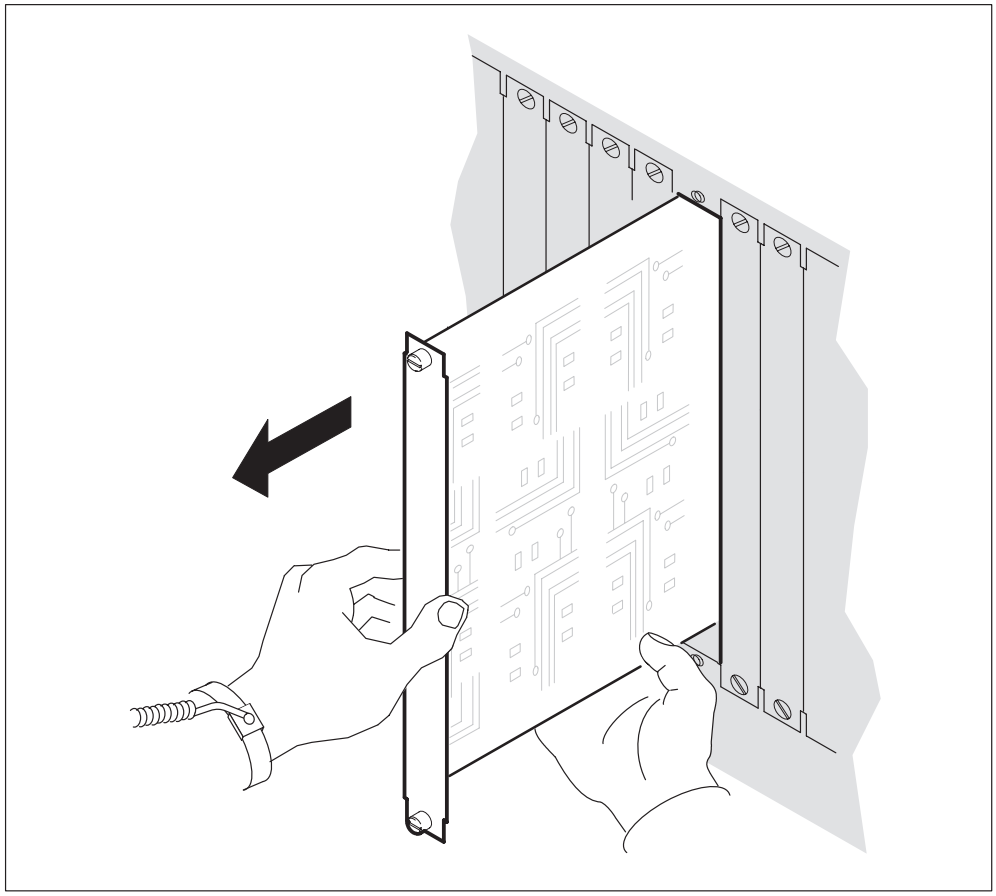
Disconnect the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the left.

22 While grasping the thumbscrews, gently pull the DS512 personality module towards you until it protrudes about 2 in. (5.1 cm) from the SDM shelf.



NTRX50GH
DS512 personality module (continued)

23 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the DS512 personality module toward you until it clears the shelf.

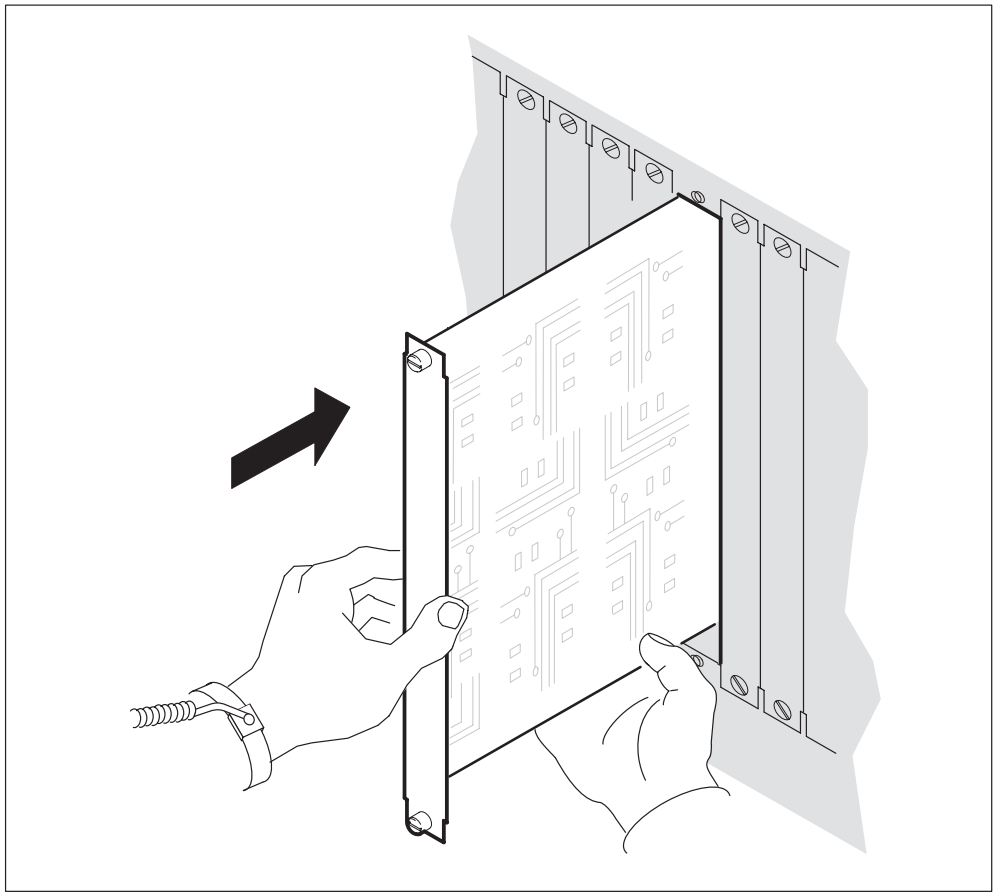


24 Place the DS512 personality module you have removed in an ESD protective container.

25 Insert the replacement DS512 personality module into the SDM shelf.

NTRX50GH
DS512 personality module (continued)

26 Gently slide the DS512 personality module into the shelf until it is fully inserted.



27 Tighten the thumbscrews at the top and the bottom of the DS512 personality module.

28

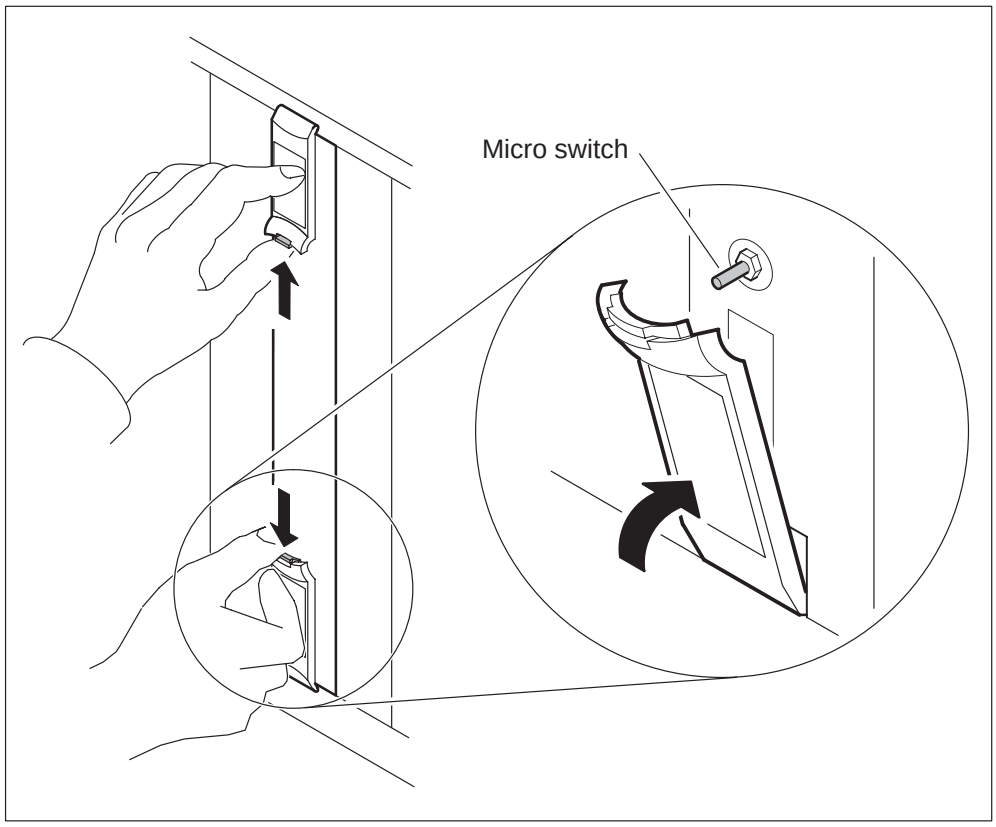
CAUTION
Reconnecting transmit and receive cables
Do not mix the transmit and receive cables for each domain. Ensure that you reconnect the cables to the correct slots. Link 0 transmit and link 0 receive connect to MS0. Link 1 transmit and link 1 receive connect to MS1.

Reconnect the four DS512 fiber cables on the DS512 personality module by pressing the fiber cable in, and turning it a 1/4 turn to the right.

NTRX50GH
DS512 personality module (continued)

At the front of the SDM

29 Close the locking levers to secure the DS512 controller module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



30 Tighten the thumbscrews on the DS512 controller module.

At the local or remote VT100 console

31 At the hardware menu level of the RMI, return the DS512 controller module to service by typing

>RTS *n* 512

and pressing the Enter key.

where

n is the SDM domain number (0 or 1) of the DS512 controller module you replaced. (See step 13.)

Example response:

```
Hardware RTS : Domain 0 Device 512 – Command initiated.
Please wait...
```

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

Example response:

```
Hardware RTS : Domain 0 Device 512 – Command submitted.
```

Note: At the hardware menu level of the RMI, the state of the DS512 controller module changes to a dot (.), indicating the module has returned to service. The in-service LED on the DS512 controller module is on (green).

At the MAP display

32 At the MS port module level of the MAP (accessed in step 7), return to service the DS512 link between MS plane 0 and the DS512 personality module you replaced by typing

>RTS 0 LINK *link number*
and pressing the Enter key.

where

link number is the MS link number that you busied in step 8

If	MS link number is
the DS512 personality module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 personality module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to RTS MS: 0 shelf: 0 chain:19 link:  0 submitted.
Request to RTS MS: 0 shelf: 0 chain:19 link: 0 passed.
```

Note: The state for the DS512 link changes to a dot (.) if the SDM DS512 link is in-service. Otherwise, the state for DS512 link changes to a “P”.

NTRX50GH
DS512 personality module (end)

33 At the MS port module level of the MAP (accessed in step 7), return to service the DS512 link between MS plane 1 and the DS512 personality module you replaced by typing

>RTS 1 LINK *linknumber*
and pressing the Enter key.

where

link number is the MS link number that you busied in step 9

If	MS link number is
the DS512 personality module to be replaced is in SDM domain 0 (slot 1)	0
the DS512 personality module to be replaced is in SDM domain 1 (slot 12)	1

Example response:

```
Request to RTS MS: 1 shelf: 0 chain:19 link:  1 submitted.
Request to RTS MS: 1 shelf: 0 chain:19 link: 1 passed.
```

Note: The state for the DS512 link changes to a dot (.) if the SDM DS512 link is in-service. Otherwise, the state for DS512 link changes to a “P”.

34 You have completed this procedure.

SDM system administration procedures

Introduction to SDM system administration procedures

This chapter contains SDM system administration procedures. Each procedure contains the following:

- explanatory and context-setting information
- summary flowchart
- step-action instructions

Explanatory and context-setting information

The first page of each procedure contains the following headings:

- Application (why you would perform the procedure)
- Action (how to use the flowchart and step-action instructions)

Summary flowchart

The flowchart is only a summary of the main actions, decision points, and possible paths you may take. Do not use the summary flowchart to perform the procedure. Instead, use it to preview what you will be doing and to prepare for it.

Step-action instructions

The step-action instructions tell you how to perform the procedure. Normally you will perform the steps in order, but you may be directed to return to a previous step and repeat a sequence. The successful completion of a step may depend on previous steps; therefore, always perform the steps in the order specified.

While following the step-action instructions, you may be sent to other procedures of this book to perform a set of instructions, or to another NTP for a related procedure. If this happens, you will be told when to return to the original instructions, and to which point in those instructions you should go.

Return key and Enter key

The carriage return key is identified in different ways (such as Enter, Return or Carriage Return) on various types of terminals. It is always used to enter commands and parameters into the system.

The procedures contained in this book and in other NTPs instruct you to press the Enter key after each step. If your terminal has a Return key, press the Return key instead. Do not press the Enter key located beside the numeric key pad.

Changing a user password

Application

Use this procedure to change a user password or to set up a temporary password for a new user. For more information on password administration, see page 3-9.

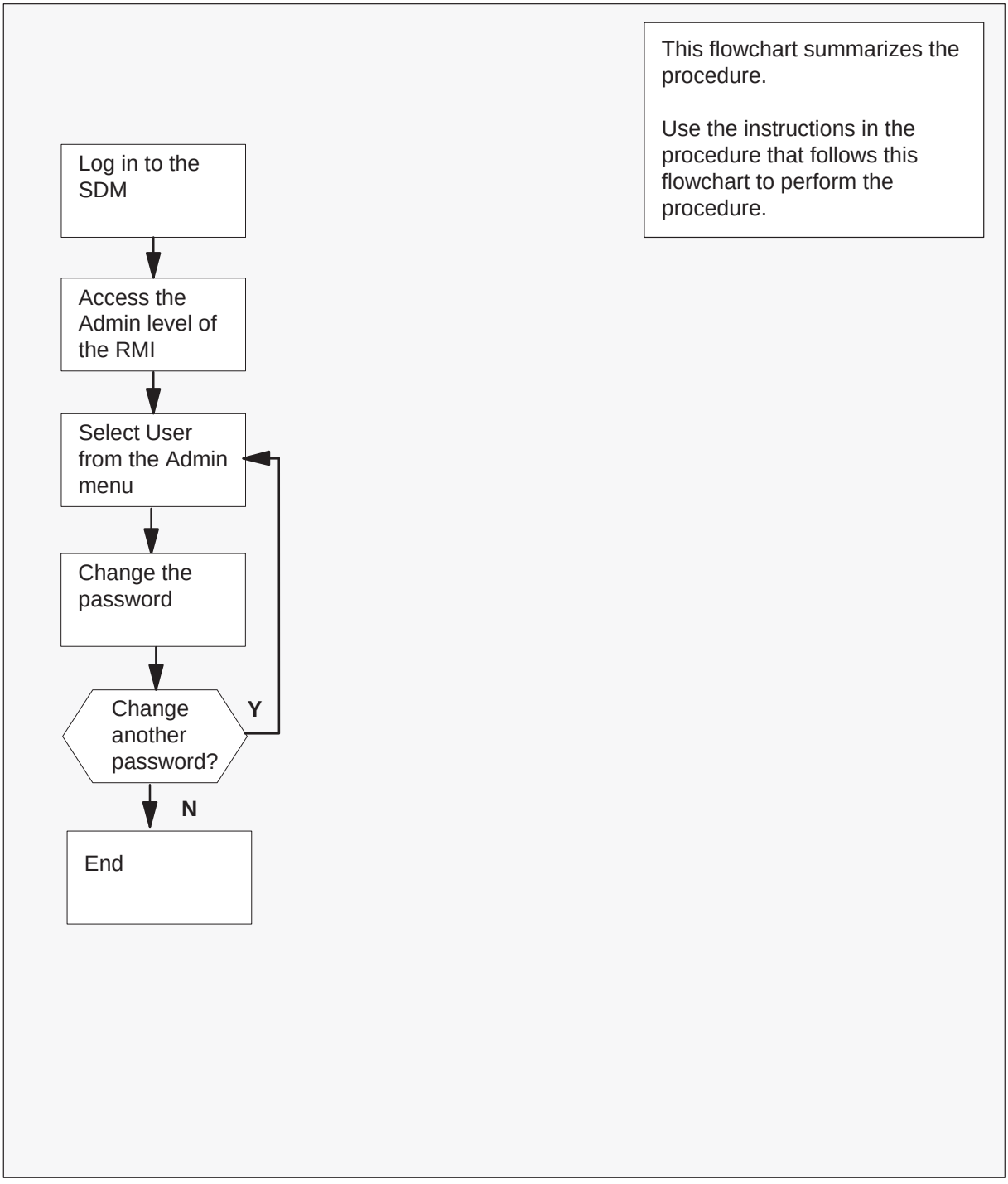
Note: Maintenance users and root users can change their own passwords if they know their current passwords. The root user can change the password of any other user on the system at any time without knowing the current password of the account.

Action

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

Changing a user password (continued)

Summary of Changing a user password



Changing a user password (continued)

Changing a user password

At the local or remote VT100 terminal

1 If you are not already logged in to the SDM, log in as either the root user or a maint user.

2 Proceed according to whether you are logged in as a root or maint user.

If you are a	Do
maint user	step 3
root user	step 11

3 Change your password by typing

>change
Example response:

```
Changing password for “maint”
maint’s Old password:
```

Changing a user password (continued)

4 Enter your old password by typing

>password
and pressing the Enter key.

where

password — is your current password

Example response:

```
Changing password for “maint”
maint’s Old password:
maint’s New password:
```

5 Enter the new password by typing

>password
and pressing the Enter key.

where

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

Example response:

```
Changing password for “maint”
maint’s Old password
maint’s New password:
Enter the new password again:
```

6 If you get an error message, go to step 16.

Changing a user password (continued)

7 Retype the password and press the Enter key.

Example response:

```
Changing password for “maint”
maint’s Old password:
maint’s New password:
```

The system returns you to the User menu. Go to step 15.

8 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

9 Select the administration menu level of the RMI by typing

>3
and pressing the Enter key.

10 Select User by typing

>3
and pressing the Enter key. The User menu is displayed.

11 Change a user password by typing

>change *userID*
and pressing the Enter key.

where

userID	is the userID of the user for whom you are changing the password

Changing a user password (continued)

Note: If no userID is specified, the system will change the password of the current user.

Example response:

```
Changing password for “root”
root’s New password:
```

12 Enter the new password by typing

>password
and pressing the Enter key.

where

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

Example response:

```
Changing password for “root”
root’s New password:
Enter the new password again:
```

13 Retype the password and press the Enter key. The system returns you to the User menu.

Changing a user password (end)

Example response:

```
Changing password for “root”
root’s New password:
Enter the new password again:
 ...
Please press ’Enter’ when ready...
```

Note: If the root user changes a maint user’s password, the change is temporary. The maint user will be asked to change the password again at the next login.

The system returns you to the User menu.

14 Determine if you want to change another password.

If you	Do
want to change another password	step 11
do not want to change another password	step 15

15 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key. Go to Step 17.

16 Contact your next level of support.

17 You have completed this procedure.

Adding or removing a maintenance user

Application

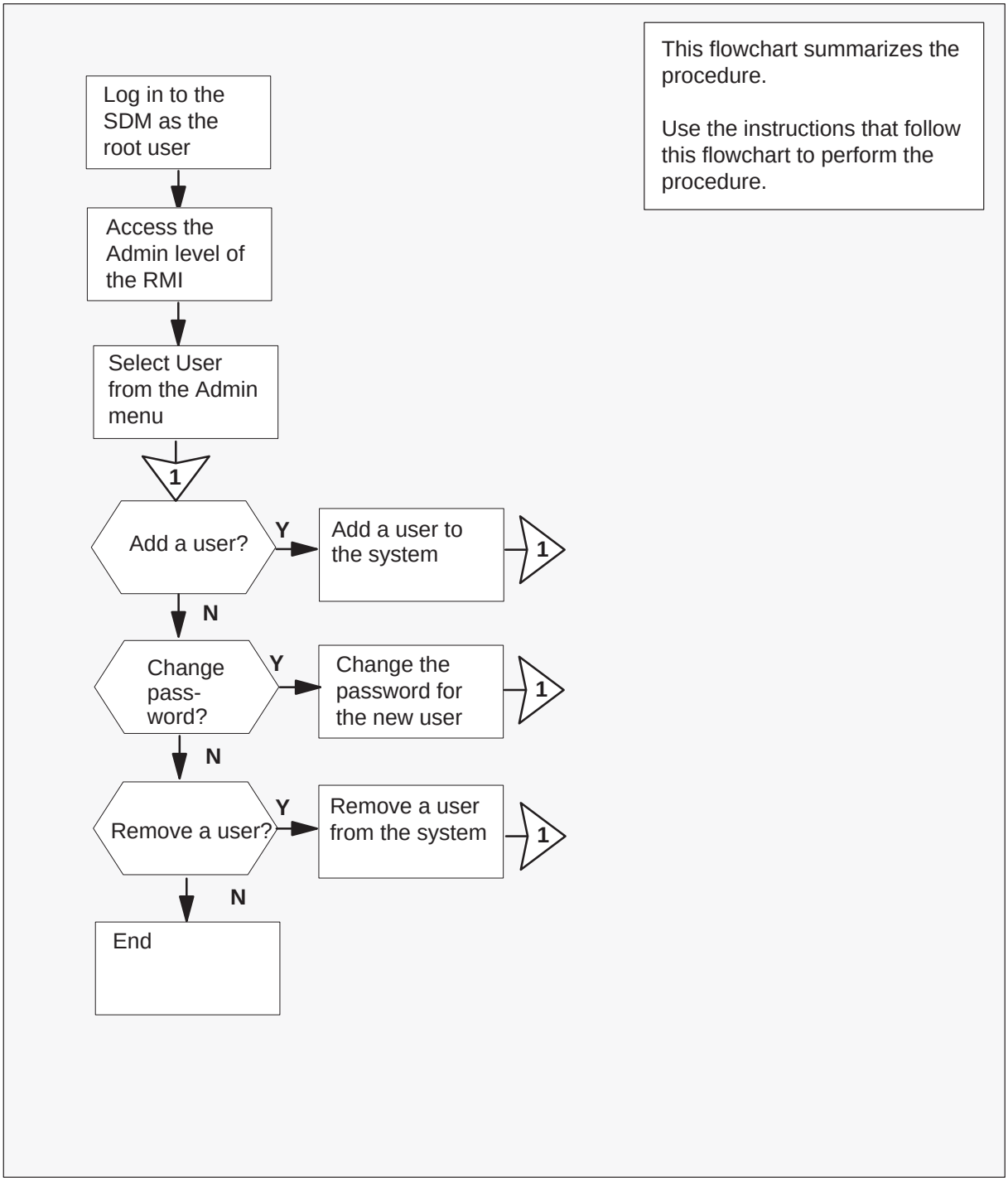
Use this procedure to add or remove a maintenance class user. This procedure must be performed by the root user.

Action

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

Adding or removing a maintenance user (continued)

Summary of Adding or removing a maintenance user



Adding or removing a maintenance user (continued)

Adding or removing a maintenance user

At the local or remote VT100 console

1 Log in to the SDM as the root user.

2 Access the top menu level of the Remote Maintenance Interface (RMI) by typing

 # sdmmtc

and pressing the Enter key. The top menu level of the RMI is displayed.

3 Select the administration (Admin) menu level of the RMI by typing

>3

and pressing the Enter key.

4 Select User by typing

>3

and pressing the Enter key. The User menu is displayed.

Example response:

```
                        SDM Remote Maintenance Interface
              SDM      CON     LAN      APPL      SYS      HW            CM : FCC1
               I        S       .        I         I        .            SDM: SDM1

User
 0 Quit          SDM USERS
 2
 3               Administrative users:
 4               root
 5
 6               Maintenance users:
 7               Jane
 8               John
 9
10
11
12
13
14
15
16
17 Help
18 Refresh

   root
Time  19:48  >
```

Adding or removing a maintenance user (continued)

5 Determine whether you want to add, remove, or change the password of a user.

If you want to	Do
add a user	step 6
change a user password	step 8
remove a user	step 12

6 Add a maintenance user by typing

add: *userID*

where

userID is the userID of the new user

and pressing the Enter key.

Example response:

```
                          SDM Remote Maintenance Interface
              SDM      CON     LAN     APPL     SYS     HW            CM : FCC1
               I        S       .       I        I       .            SDM: SDM1

User
 0 Quit          SDM USERS
 2
 3               Administrative users:
 4               root
 5
 6               Maintenance users:
 7               Jane
 8               John
 9
10
11
12
13
14
15
16
17 Help
18 Refresh

   root
Time  19:48  >add smith
```

Adding or removing a maintenance user (continued)

The User menu immediately displays the new userID. (In the example below, the userID Smith was added.

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

Example response:

```
                          SDM Remote Maintenance Interface
              SDM      CON     LAN      APPL      SYS      HW            CM : FCC1
               I        S       .        I         I        .            SDM: SDM1

User
 0 Quit          SDM USERS
 2
 3               Administrative users:
 4               root
 5
 6               Maintenance users:
 7               Jane
 8               John
 9               Smith
10
11
12               To activate the account for 'smith',
13               use the CHANGE command to set the password.
14
15
16
17 Help
18 Refresh

   root
Time  19:48  >
```

7 Determine whether you want to activate the user or add another user.

If you	Do
want to activate the user	step 8
want to add another user	step 6
do not want to add another user	step 17

Adding or removing a maintenance user (continued)

8 Set or change a password for the user by typing

change *userID*
and pressing the Enter key.

where

userID — is the userID of the user for whom you are changing the password

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

Example response:

```
Changing password for “smith”
smith’s New password:
```

9 Enter the new password by typing

password
and pressing the Enter key.

where

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

Example response:

```
Changing password for “Smith”
Smith’s New password:
Enter the new password again:
```

Adding or removing a maintenance user (continued)

10 Retype the password and press enter. The system returns you to the User menu.

```
Changing password for “Smith”
Smith’s New password:
Enter the new password again:
```

The system returns you to the User menu.

11 Determine if you want to change another userID password.

If you	Do
want to change another password	step 8
do not want to change another password	step 17

12 Remove a user by typing

delete *userID*
and pressing the Enter key.

where

userID is the userID of the user you are deleting

The system immediately deletes the userID and redisplays the User menu. (In the example following, the userID Smith was added.)

Response:

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

13 Decide if you really want to delete the user.

If you	Do
want to delete the user	step 14
do not want to delete the user	step 15

Adding or removing a maintenance user (end)

14 Confirm that you want to delete the user by typing

>Y
and pressing the Enter key.

Go to step 16.

15 Confirm that you do not want to delete the user by typing

>N
and pressing the Enter key.

16 Determine if you want to remove another user from the system.

If you	Do
want to remove another user	step 12
do not want to remove another user	step 17

17 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

18 You have completed this procedure.

Setting the time zone, date and time

Application

ATTENTION

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

ATTENTION

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

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

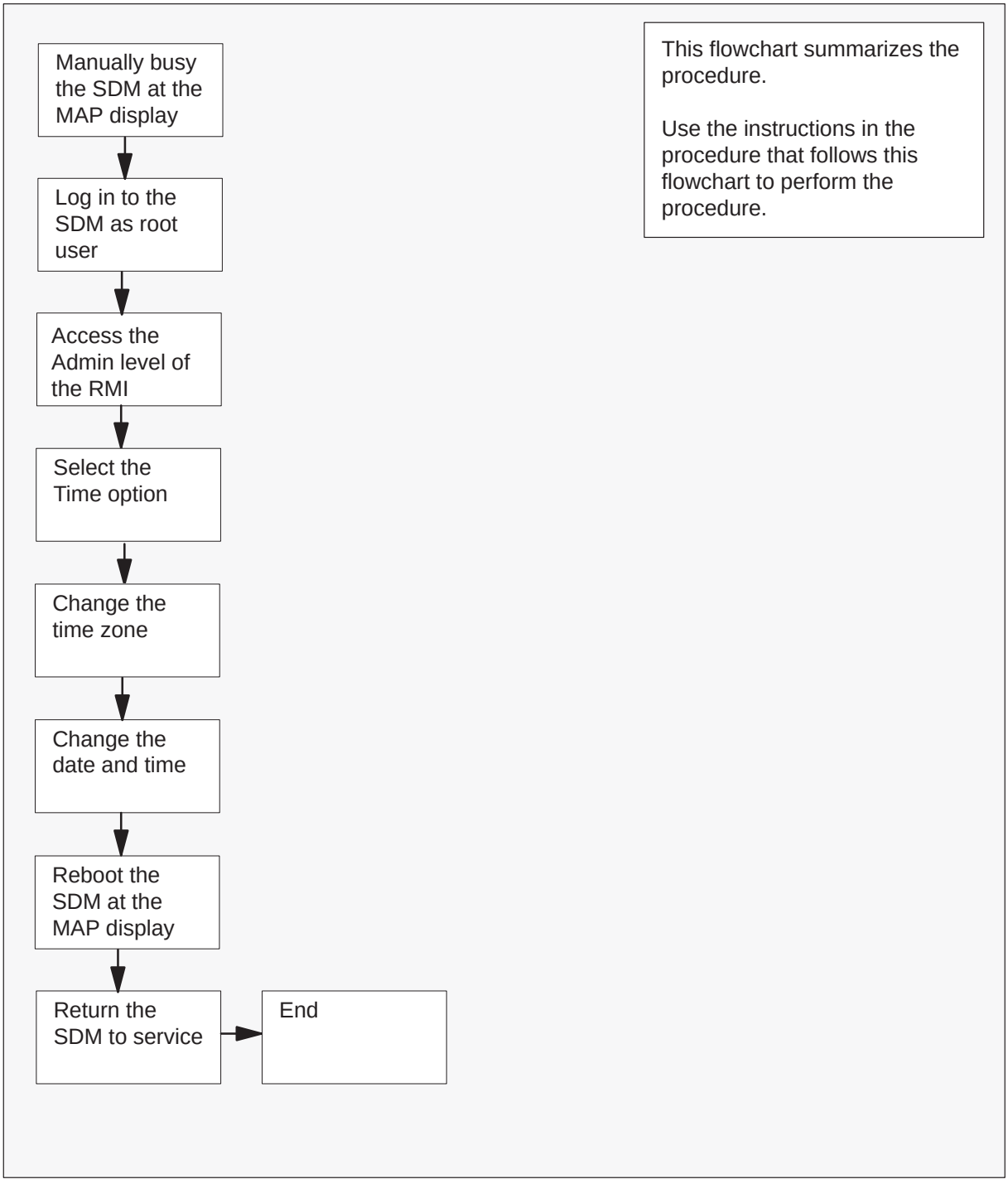
The SDM must be rebooted after changing the time zone, date and time.

Action

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

Setting the time zone, date and time (continued)

Summary of Setting the time zone, date and time



Setting the time zone, date and time (continued)

Setting the time zone, date and time

At the MAP display

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

>MAPCI; MTC;APPL;SDM
and pressing the Enter key.

2 Determine the SDM node state.

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

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

Go to step 2.

4

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

Manually busy the SDM by typing

>BSY
and pressing the Enter key.

Response:

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

Setting the time zone, date and time (continued)

5 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

Response:

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

At the local or remote VT100 terminal

6 Log in to the SDM as the root user.

7 Access the top menu level of the RMI by typing

 # sdmmtc
and pressing the Enter key.

8 Select the administration (Admin) menu level of the RMI by typing

>3
and pressing the Enter key.

9 Select Time by typing

>2
and pressing the Enter key. The SDM Remote Maintenenace Interface is displayed. Press the Enter key again. The Use Daylight Savings Time screen is displayed.

Response:

```
                        Use DAYLIGHT SAVINGS TIME?

Move cursor to desired item and press Enter.

  # Does this time zone go on
  # DAYLIGHT SAVINGS TIME?
  #
  1 yes
  2 no

F1=Help             F2=Refresh            F3=Cancel
F8=Image            F10=Exit              Enter=Do
/=Find              n=Find Next
```

10 Use the arrow key to select “yes” (option 1) to the question, “Does this time zone go on daylight savings time?” if at some time in the year daylight savings time will be applied to this time zone. Otherwise, select “no” (option 2). Press the Enter key when you have selected the appropriate response.

Setting the time zone, date and time (continued)

11 The CUT (Coordinated Universal Time) Time Zone screen is displayed. Use the up and down arrows to choose the appropriate time zone, and then press the Enter key.

Note: All time zones do not fit on a single screen display. Use the up and down arrow keys to view the rest of the time zones.

Response:

```
                CUT (Coordinated Universal Time) Time Zone

Move cursor to desired item and press Enter.

 [TOP]
   (CUTOGDT)              Coordinated Universal Time         (CUT)
   (GMTOBST)              United Kingdom                     (CUT)
   (AZOREST1AZOREDT)      Azores; Cape Verde               (CUT -1)
   (FALKST2FALKDT0        Falkland Islands                 (CUT -2)
   (GRNLNDST3GRNLNDDT)    Greenland; East Brazil           (CUT -3)
   (AST4ADT)              Central Brazil                   (CUT -4)
   (EST5EDT)              Eastern U.S.; Colombia           (CUT -5)
   (CST6CT)               Central U.S.; Honduras           (CUT -6)
   (MST7MDT)              Mountain U.S.                    (CUT -7)
   (PST8PDT)              Pacific U.S.; Yukon              (CUT -8)
[MORE...19]

 F1=Help                   F2=Refresh                    F3=Cancel
 F8=Image                  F10=Exit                      Enter=Do
 /=Find                    n=Find Next
```

Setting the time zone, date and time (continued)

12 The Change / Show Date, Time, & Time Zone screen is displayed. Use the up and down arrows to move the cursor to a date or time entry you want to change. Repeat until you modify all the entries you want to change. Press the Enter key.

Example response:

```
               Change / Show Date, Time, & Time Zone

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
  Old time zone                                          EST5EDT
  Time zone                                             [CUT0GDT]
  Does this time zone go on daylight savings time?       yes

* YEAR (00-99)                                         [97]              #
* MONTH (01-12)                                        [02]              #
* DAY (01-31)                                          [26]              #

* HOUR (00-23)                                         [21]              #
* MINUTES (00-59)                                      [18]              #
* SECONDS (00-59)                                      [00]              #



F1=Help        F2=Refresh          F3=Cancel           F4=List
F5=Reset       F6=Command          F7=Edit             F8=Image
F9=Shell       F10=Exit            Enter=Do
```

Special attention is required when you use the screen in the preceding example response. The default offset for daylight savings time change is set according to the rule in North America. According to this rule, the move from standard time to daylight savings time occurs on the first Sunday of April. That is, clock time is moved forward one hour. The move from daylight savings time to standard time occurs on the last Sunday of October. That is, clock time is moved backward one hour.

If you are outside of North America, you need to manually set the time zone. In the time zone window, select a time zone and enter the date and time values. Manually add the offset variable.

For example, change the selected time zone “NFT-1DFT” for Norway and France to “NFT-1DFT,M3.5.0,M10.4.0/2:00”.

Note 1: The offset variable “M3.5.0,M10.4.0/2:00” added to the time zone means the following:

- time changes forward at 2 a.m. on Sunday of the fifth week of March.
- time changes backward at 2 a.m. on Sunday of the fourth week of October.

Note 2: The time indicated in Note 1 is only an example. Check with appropriate personnel for the hour that daylight savings time occurs.

Setting the time zone, date and time (continued)

13 The Command Status screen is displayed. The command status is shown as "running" while the changes are being processed. The command status changes to "OK" when processing is complete. The date, time and time zone are displayed.

Example response:

```
                              COMMAND STATUS

Command: OK         stdout: yes         stderr: no

Before command completion, additional instructions may appear below.

Wed Feb 26 21:18:00 CUT 1997

Any changes made to the time zone will take effect at your next login
session.









 F1=Help                  F2=Refresh                  F3=Cancel
 F8=Image                 F10=Exit                    Enter=Do
 /=Find                   n=Find Next
```

14 Exit the command status screen by pressing the F3 key.

At the SDM level of the MAP display

15 Reboot the SDM by typing

>REBOOTSDM
and pressing the Enter key.

Response:

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

Do you wish to proceed?

Please confirm ("YES", "Y", "NO", or "NO"):
```

Setting the time zone, date and time (end)

16 Confirm that you want to proceed by typing

>Y
and pressing the Enter key.

Response:

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

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

17 Return the SDM to service by typing

>RTS
and pressing the Enter key.

Response:

```
SDM InSv                    Links_00S:  .

SDM RTS initiated.
SDM RTS completed.
```

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

18 You have completed this procedure.

Creating SDM backup tapes
System image backup (S-tape)

Application

ATTENTION

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

ATTENTION

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

ATTENTION

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

ATTENTION

The files under the /data file system are excluded from all SDM backup (both system image and incremental backup). The files under the /data file system are temporary files that do not require backing up.

Use this procedure to create a system image backup tape (S-tape). The system image includes the following:

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

Creating SDM backup tapes
System image backup (S-tape) (continued)

Nortel (Northern Telecom) recommends that you perform a system image backup after the following:

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

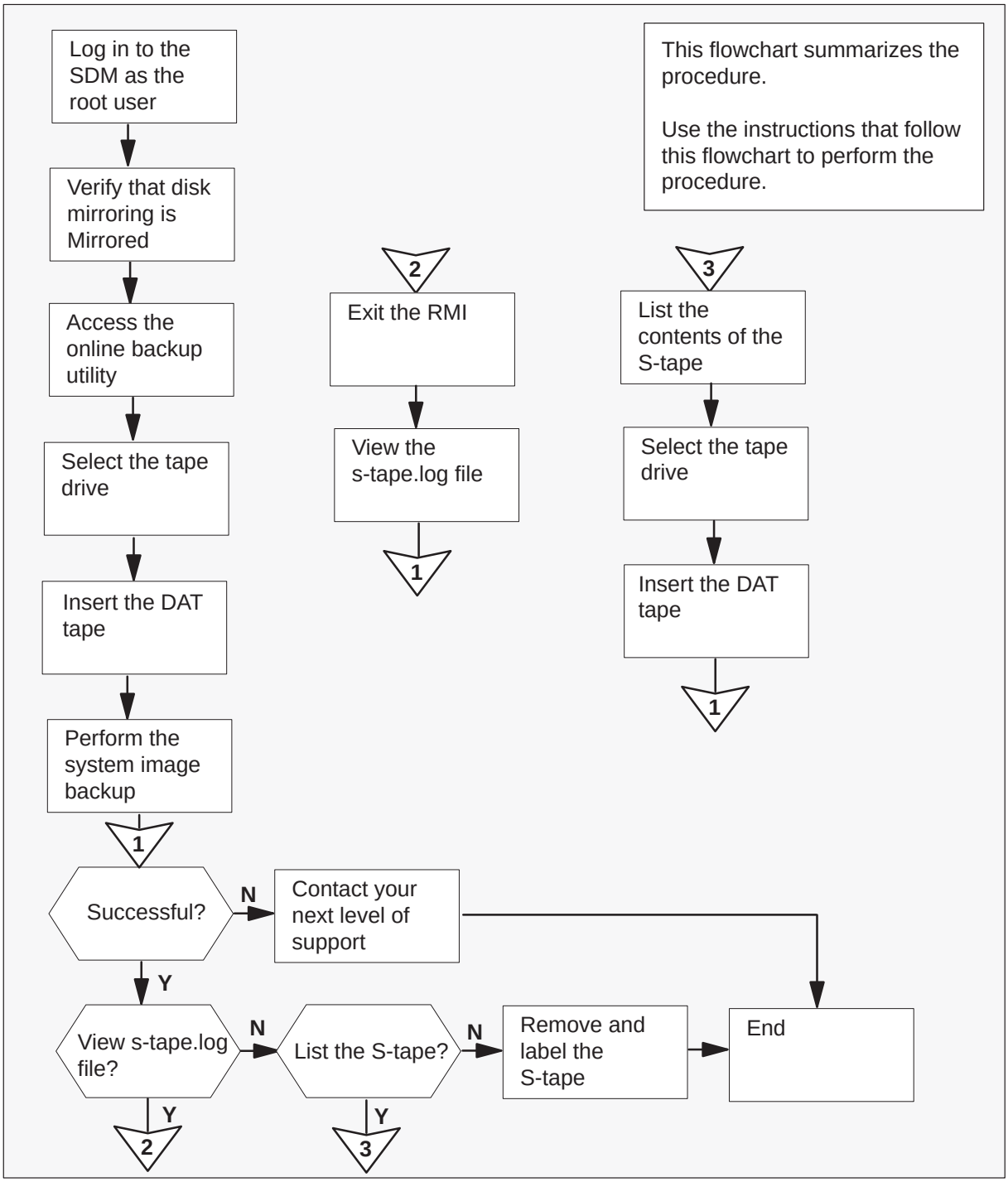
A system image backup takes a minimum of 10 min to complete, depending on the size of your file systems.

Action

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

Creating SDM backup tapes
System image backup (S-tape) (continued)

Summary of System image backup



Creating SDM backup tapes
System image backup (S-tape) (continued)

System image backup

At the local or remote VT100 console

1 Log in to the SDM as the root user.

2 Access the RMI by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                          Mirrored
  Volume              Size(MB)              (% full/ threshold)
 1 /                     20                        25/ 80
 2 /usr                  192                       85/ 90
 3 /var                  40                        17/ 80
 4 /tmp                  20                        11/ 90
 5 /home                 300                       27/ 70
 6 /sdm                  192                       65/ 90
(unallocated)            972

Disk mirroring (datavg):                          Mirrored
   Volume              Size(MB)               (% full/ threshold)
 7 /data                 112                       4/ 80
 (unallocated)           8000
```

5 Determine at the storage menu level if disk mirroring for all volume groups is Mirrored.

If disk mirroring is	Do
Mirrored	step 7
anything else	step 6

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

Creating SDM backup tapes
System image backup (S-tape) (continued)

7 Access the administration (Admin) menu level of the RMI by typing

>ADMIN
and pressing the Enter key.

8 Access the Backup and Restore Main Menu by typing

>5
and pressing the Enter key.

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

Example response:

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

9 From the Backup and Restore Main Menu, select “System Image Backup and Restore” by typing

>2
and pressing the Enter key.

Note: If disk mirroring for all volume groups is not Mirrored, an error message is displayed. You are prompted to return to the System Image Backup and Restore Main Menu.

10 From the System Image Backup and Restore Menu, select “Create a System Image on Tape (S-tape)” by typing

>2
and pressing the Enter key.

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

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

Creating SDM backup tapes
System image backup (S-tape) (continued)

12 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

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

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key.

If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

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

Example response:

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

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

Creating SDM backup tapes
System image backup (S-tape) (continued)

At the SDM

14

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

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

At the local or remote console

15 When you are certain you are using the correct tape, type

>y
and press the Enter key.

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

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

Example response:

```
Rewinding the tape...

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


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

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

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

If there is	Do
enough disk space	step 19
not enough disk space	step 17

Creating SDM backup tapes
System image backup (S-tape) (continued)

17 Erase enough files from the temporary directory to create the required amount of disk space specified in the error message by typing

>rm –rf /tmp/*

and press the Enter key.

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

18 Execute the system image backup again.

19 The system image backup begins.

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

Example response:

```
Rewinding the tape...

    Starting the system image backup on bnode73.

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

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

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

20 Read the system message.

If the backup	Do
is successfully completed	step 21
fails	step 46

Creating SDM backup tapes
System image backup (S-tape) (continued)

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

Example response:

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

Please remove the backup tape from the tape drive.
Label the tape as shown below and store it in a safe place.

       System Image Tape (S-tape)
       The Machine Node Id: bnode73
       Date: Wed Oct 16 08:37:37 EDT 1997

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

22 Determine if you wish to eject the S-tape. Type “y” to eject the tape, and “n” if you do not wish to eject the tape.

Note: If you wish to list the contents of the tape, do not eject the tape. Go to step 35.

If you eject the tape, the screen displays “Tape ejected.” below the information displayed in step 21. You are then prompted to return to the System Image Backup and Restore Main Menu.

Response:

```
Tape ejected.

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

Nortel recommends that you place the write-protect tab of the S-tape in the open position, to prevent accidental erasing.

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

>y

and press the Enter key.

Creating SDM backup tapes
System image backup (S-tape) (continued)

24 Determine if the backup is successful. The system informs you if the system image backup is successful, as shown in the response in step 21. You may also wish to view the s-tape.log file or list the files on the S-tape.

If	Do
you wish to view the s-tape.log file	step 25
you wish to list the S-tape	step 34
the backup is successful	step 43
the backup fails	step 46

25 Exit the System Image Backup and Restore Main Menu by typing

>0
and pressing the Enter key.

26 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

27 Access the s-tape.log file by typing

 # cd /tmp
at the prompt and pressing the Enter key.

28 Scroll through the file by typing

 # more s–tape.log
and pressing the Enter key. This screen informs you that the system image backup was completed successfully.

Example response:

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

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

The S-tape backup started on Wed Oct 16 09:24:07 EDT 1997
completed successfully on Wed Oct 16 09:36:03 EDT 1997
```

Creating SDM backup tapes
System image backup (S-tape) (continued)

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

If you	Do
wish to list the S-tape	step 30
do not wish to list the S-tape	step 47

30 Return to the login directory by typing

 # cd
and pressing the Enter key.

31 Access the RMI by typing

 # sdmmtc
and pressing the Enter key.

32 Access the administration (Admin) menu level of the RMI by typing

>ADMIN
and pressing the Enter key.

33 Access the Backup and Restore Main Menu by typing

>5
and pressing the Enter key.

34 From the Backup and Restore Main Menu, select “System Image Backup and Restore” by typing

>2
and pressing the Enter key.

35 From the System Image Backup and Restore Menu, select “List Contents of the System Image Tape (S-tape)” by typing

>3
and pressing the Enter key.

Creating SDM backup tapes
System image backup (S-tape) (continued)

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

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

37 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

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

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key.

If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the System Image Backup and Restore Menu.

38 After you select the tape drive, you are prompted to insert the S-tape into the tape drive you selected in step 37.

Example response:

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

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

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

Creating SDM backup tapes
System image backup (S-tape) (end)

At the SDM

39 Insert the S-tape into the tape drive you selected.

At the local or remote VT100 terminal

40 When you are ready to continue this procedure, type

>y
and press the Enter key.

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

Response:

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

42 Return to the System Image Backup and Restore Menu, by typing

>y
and pressing the Enter key.

At the SDM

43 If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive. Label the tape according to your office procedures, and store it in a safe location. If you ejected an SBA tape or I-tape, reinsert the appropriate tape.

At the local or remote VT100 terminal

44 Exit the System Image Backup and Restore Menu, by typing

>0
and pressing the Enter key.

45 Exit the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

Note: If you wish to exit the RMI, type QUIT ALL and press the Enter key.

Go to step 47.

46 Contact the personnel responsible for the next level of support.

47 You have completed this procedure.

Creating SDM backup tapes
Manual incremental backup (I-tape)

Application

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

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

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

ATTENTION
The files under the /data file system are excluded from all SDM backup (both the system image back up and the incremental back up) because the /data files are temporary files that do not require back up.

Use this procedure to manually back up SDM software files that have been changed or created since the most recent system image backup tape (S-tape) was created.

If a file is open when the incremental backup begins, the most recent saved version of the file is backed up, which may result in inconsistency between the open file when it is saved, and the backed-up version. To prevent or minimize this inconsistency, incremental backups should be performed in a low-usage period.

Incremental backups can be run manually or scheduled to run automatically. For additional information on scheduling and performing software backups,

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

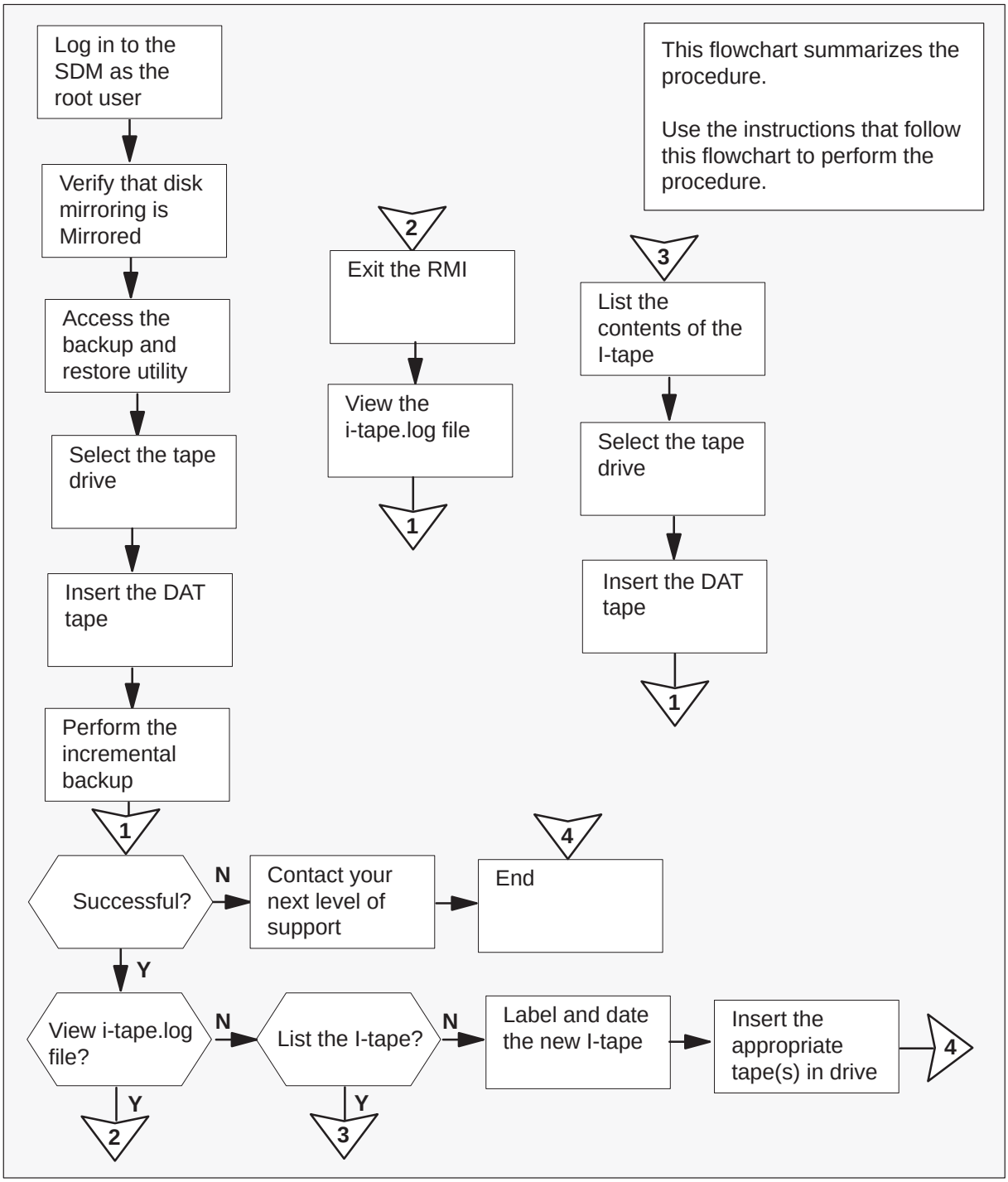
refer to the “SDM system administration overview” chapter of this document, and the procedure ”Creating SDM backup tapes–Automated incremental backups” on page 6-50 in this chapter.

Action

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

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

Summary of Manual incremental backup



Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

Manual incremental backup

At the local or remote console

1 Log in to the SDM as the root user.

2 Access the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                          Mirrored
  Volume              Size(MB)                (% full/ threshold)
 1 /                     20                          25/ 80
 2 /usr                  192                         85/ 90
 3 /var                  40                          17/ 80
 4 /tmp                  20                          11/ 90
 5 /home                 300                         27/ 70
 6 /sdm                  192                         65/ 90
(unallocated)            972

Disk mirroring (datavg):                            Mirrored
   Volume              Size(MB)                  (% full/ threshold)
 7 /data                 112                         4/ 80
 (unallocated)           8000
```

5 Determine at the storage menu level if disk mirroring for all volume groups is Mirrored.

If disk mirroring is	Do
Mirrored	step 7
Integrating or Not Mirrored	step 6

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

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

7 Access the administration (Admin) menu level of the RMI by typing

>ADMIN

and pressing the Enter key.

8 Access the Backup and Restore Main Menu by typing

>5

and pressing the Enter key.

Note: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

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

9 From the Backup and Restore Main Menu, select “Incremental Backup and Restore” by typing

>3

and pressing the Enter key.

Note: If you disk mirroring for all volume groups is not Mirrored, an error message is displayed. You are also prompted to return to the Incremental Backup and Restore Menu.

10 From the Incremental Backup and Restore Menu, select “Create an Incremental Backup Tape Now (I-tape)” by typing

>3

and pressing the Enter key.

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

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

12 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the Incremental Backup and Restore Menu if you do not wish to use DAT1.

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

Example response:

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

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

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

At the SDM

14

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

Ensure that you are using the correct digital audio tape (DAT) to be used for this incremental backup.

At the local or remote console

15 If you are certain you are using the correct tape, type

>y
and press the Enter key.

16 All files and directories that have changed or been added since the last full SDM system image backup tape (S-tape) was made are backed up.

Example response:

```
Rewinding the tape in tape drive DAT0...

Incremental backup is in progress.
A log file /tmp/i-tape.log is recording all entries.
```

Note: An error message is displayed if the incremental backup is unsuccessful. If this occurs, go to step 19.

17 When the incremental backup is successfully completed, the following message appears:

Response:

```
The incremental backup is successfully completed.
A log file /tmp/i-tape.log is created.

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

18 When you are ready to return to the Incremental Backup and Restore Menu, type

>y
and press the Enter key.

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

19 Determine if the incremental backup is successful. The system informs you that the incremental backup is successful, as shown in the response in step 17. You may also wish to view the i-tape.log file or list the files on the I-tape.

If	Do
the backup is successful	step 40
the backup failed	step 41
you wish to view the i-tape.log file	step 20
you wish to list the I-tape	step 30

20 Return to the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

21 Exit the Backup and Restore Main Menu by typing

>0
and pressing the Enter key.

22 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

23 Access the i-tape.log file by typing

 # cd /tmp
at the prompt and pressing the Enter key.

Scroll through the file by typing

 # more i–tape.log
and pressing the Enter key. The system informs you that the incremental backup was successfully completed.

Example response:

```
Incremental Backup Started – Mon Mar 24 16:54:06 EST 1997
using the tape drive in /dev/rmt0.

Incremental Backup is Successfully Completed - Mon Mar 24 17:06 EST 1997
```

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

24 Determine if you wish to list the I-tape.

If you	Do
wish to list the I-tape	step 25
do not wish to list the I-tape	step 42

25 Return to the login directory by typing

 # cd
and pressing the Enter key.

26 Access the RMI by typing

 # sdmmtc
and pressing the Enter key.

27 Access the administration (Admin) menu level of the RMI by typing

>ADMIN
and pressing the Enter key.

28 Access the Backup and Restore Main Menu by typing

>5
and pressing the Enter key.

29 From the Backup and Restore Main Menu select ”Incremental Backup and Restore” by typing

>3
and pressing the Enter key.

30 From the Incremental Backup and Restore Menu, select “List Contents of an Incremental Backup Tape (I-tape)” by typing

>4
and pressing the Enter key.

31 After you select option 4, you are prompted to select the tape drive.

Response:

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

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

Creating SDM backup tapes
Manual incremental backup (I-tape) (continued)

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

32 Select the tape drive you wish to use, by typing

>n
and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the Incremental Backup and Restore Menu.

33 After you select the tape drive, you are prompted to insert the I-tape into the tape drive you selected in step 32.

Example response:

```
Please insert your Incremental Backup tape (I-tape) into
the tape drive DAT0 and allow a few minutes to complete the listing.

A log file will be saved in /tmp/i–tape.toc.

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

At the SDM

34 Insert the I-tape into the tape drive you selected.

At the local or remote VT100 console

35 If you are ready to continue this procedure, type

>y
and press the Enter key.

Creating SDM backup tapes
Manual incremental backup (I-tape) (end)

36 The contents of the I-tape are displayed. When the system has finished listing the contents of the I-tape, it prompts you to return to the Incremental Backup and Restore Menu.

Response:

```
Listing of the incremental backup tape is complete.
A log file is in /tmp/i-tape.toc.

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

37 If you are ready to return to the Incremental Backup and Restore Menu, type

>y
and press the Enter key.

38 Return to the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

39 Exit the Backup and Restore Main Menu by typing

>0
and pressing the Enter key.

Note: If you wish to exit the RMI, type QUIT ALL and press the Enter key.

At the SDM

40 Remove the tape and label it according to your office procedures. Clearly identify the tape as an I-tape, and include the date it was created. If you are using the same tape repeatedly for incremental backups, reinsert the tape into the tape drive. If you are alternating I-tapes on a rotational basis, insert the appropriate I-tape to be used for the next incremental backup into the tape drive. If you removed the SBA tape, reinsert the SBA tape into the appropriate tape drive.

Go to step 42.

41 Contact the personnel responsible for the next level of support.

42 You have completed this procedure.

Creating SDM backup tapes
Automated incremental backups

Application

ATTENTION

This procedure must be performed by a trained AIX system administrator who has root user privileges to access the SDM.

ATTENTION

All volume groups on the SDM must be fully mirrored (Mirrored) before an automated incremental backup can take place. If the automated incremental backup is scheduled when all volume groups are not Mirrored, the automated incremental backup will fail, and a PM SDM minor alarm will occur.

ATTENTION

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

Use this procedure to perform the following tasks:

- create an automated incremental backup schedule
- clear the automated incremental backup schedule
- view the automated incremental backup schedule

An incremental backup creates incremental backup tapes (I-tapes) that consist of all SDM software files that have been changed or created since the most recent system image backup tape (S-tape) was created. Automated incremental backups can be scheduled to occur daily, weekly, monthly or on a specific date. The procedure to schedule, clear or view the automated incremental backup can be performed while the SDM is in service.

The automated incremental backup status can have the status of disabled, enabled, completed or failed. Disabled indicates that the automated backup is not enabled. Enabled indicates that the automated backup has been enabled but not executed yet. Completed means that the last automated incremental backup has been successfuly completed. Failed indicates that

the last automated incremental backup failed. Refer to the custlog/sdmstatlog or the /tmp/i-tape.log for failure reasons.

If a file is open when the incremental backup begins, the most recent saved version of the file is backed up, which may result in inconsistency between the open file when it is saved, and the backed-up version. To prevent or minimize this inconsistency, automated incremental backups should be scheduled to take place in a low-usage period.

The Automated Incremental Backup Menu allows you to create an incremental backup schedule, view the current incremental backup schedule, or clear the current incremental backup schedule.

When an automated incremental backup schedule is cleared, the previous schedule is deleted. If this schedule is to be used at a later date, make note of the schedule for future reference.

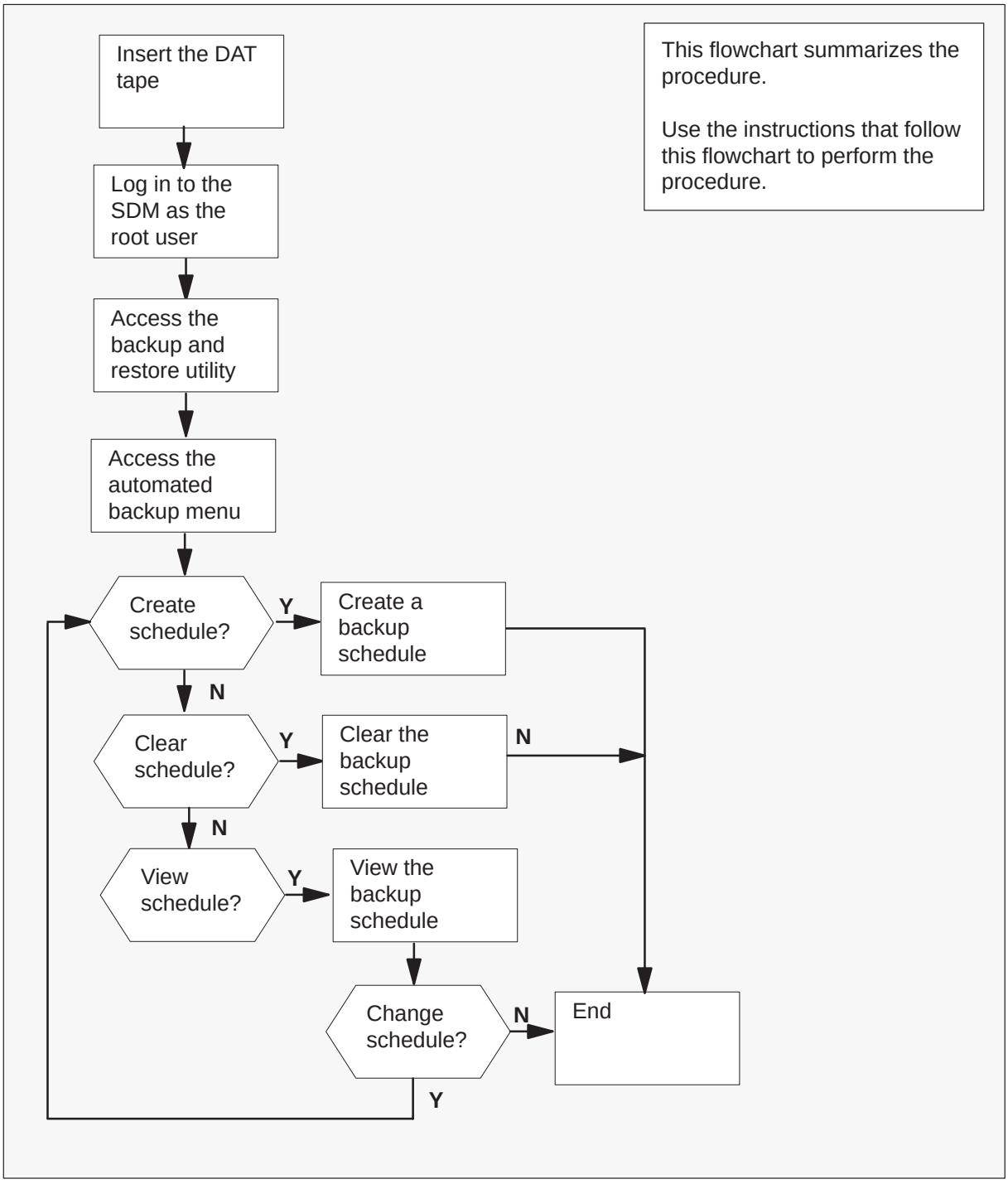
Incremental backups can be performed manually if required. Refer to the procedure ”Creating SDM backup tapes–Manual incremental backup (I-tape)” on page 6-39 in this section. For additional information on performing software backups, refer to page 3-11 in the System Administration Overview section of this document.

Action

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

Creating SDM backup tapes
Automated incremental backups (continued)

Summary of Automated incremental backups



Creating SDM backup tapes
Automated incremental backups (continued)

Automated incremental backups

At the local or remote console

1 Insert the digital audio tape (DAT) to be used for the automated incremental backup into one of the SDM tape drives, if required.

Note 1: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

Note 2: See the page 3-16 in the “SDM system administration overview” chapter of this document for guidelines on tape usage and rotation for incremental backups.

2 Log in to the SDM as the root user.

3 Access the Backup and Restore Main Menu by typing

 # sdmbkup
and pressing the Enter key.

Note: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

```
Currently there is a backup running on bnode75.
Please execute yours later.
Exiting . . .
```

4 From the Backup and Restore Main Menu, select “Incremental Backup and Restore” by typing

>3
and pressing the Enter key.

5 From the Incremental Backup and Restore Menu, select “Automated Incremental Backup Menu” by typing

>2
and pressing the Enter key. The Automated Incremental Backup Menu is displayed.

Creating SDM backup tapes
Automated incremental backups (continued)

6 Determine if you wish to schedule an incremental backup, clear the incremental backup, or view the incremental backup schedule.

If you wish to	Do
schedule an incremental backup	step 7
clear the incremental backup schedule	step 16
view the incremental backup schedule	step18

7 From the Automated Incremental Backup Menu, select “Create Automated Incremental Backup Schedule” by typing

>2

and pressing the Enter key. You are prompted to select the tape drive you wish to use.

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

8 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Creating SDM backup tapes
Automated incremental backups (continued)

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

9

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

You are then prompted to insert a tape in the drive you have selected, if the tape drive does not already contain a tape. If you have inserted a tape, go to step 11.

Example response:

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

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

At the SDM

10 Ensure that you are using the correct DAT tape for the automated incremental backup.

Creating SDM backup tapes
Automated incremental backups (continued)

At the local or remote console

11 If you are certain you are using the correct tape, type

>y

and press the Enter key. The Set Date and Time for SDM Incremental Backup screen is displayed.

Response:

```
*******************************************
Set Date and Time for SDM Incremental Backup
*******************************************

The valid input values are:

    min    hr        day     month         day of wk
   0-59   0-23,*    1-31,*   1-12,*    0-6,*, with 0=Sunday

For example:

    min    hr     day    month     day of wk
     0      2      *       *           1

This example denotes that the incremental backup is scheduled
for every Monday at 2 a.m.

Please enter your preferred schedule by filling in all 5 fields
separated by a space or a tab:

         min      hr      day      month      day of wk
```

12 The following examples show the respective values you may use to schedule an automated incremental backup daily, weekly, monthly and on a specific date.

	min	hr	day	month	day of wk
Daily	0	2	*	*	*
Weekly	0	2	*	*	6
Monthly	0	2	15	*	*
Specific date/time	0	2	10	12	*

Note: Select all by typing " * " instead of the appropriate number. (See exceptions below for min and hr.)

The following pairs of values cannot be used for minutes and hour.

min	hr
*	0-23
*	*

Note: You are prompted at the top of the Set Date and Time for SDM Incremental Backup screen, to re-enter the values for minutes and hour when incorrect values are entered.

Creating SDM backup tapes
Automated incremental backups (continued)

Example response

```
Your input was invalid.
Please re-enter your backup schedule.
```

13 Enter the desired schedule according to the acceptable ranges displayed at the Set Date and Time for SDM Incremental Backup menu. The numeric ranges correspond to minute, hour, day/month, month/year, and day/week. Use the Tab key to move to each field.

14 Schedule the incremental backup. When you have successfully entered the backup schedule, the schedule is displayed. You are also prompted to return to the Automated Incremental Backup Menu.

Example response:

```
The Automated Incremental Backup is scheduled as follows:


       Tape Drive   :    DAT0

       Day of Week  :    Mondays
       Month        :    –
       Day          :    –

       Hour         :    2
       Minutes      :    0

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

15 Return to the Automated Incremental Backup Menu by typing

>y
and press the Enter key.

Go to step 24.

Creating SDM backup tapes
Automated incremental backups (continued)

16

CAUTION
Clearing the automated incremental backup
Clearing the automated incremental backup deletes the previous automated incremental backup schedule. If you wish to use the same schedule at a later date, make a note of the schedule before clearing it.

Select "Clear Automated Incremental Backup Schedule" by typing

>4

and pressing the Enter key.

Response:

```
The Automated Incremental Backup schedule has been cleared.

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

Note: If you attempt to clear the automated incremental backup when you have not set up a schedule, you will receive an error message telling you that a schedule was never set up. You are prompted to return to the Automated Incremental Backup Menu.

Response:

```
The Automated Incremental Backup schedule was never scheduled.

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

17 Return to the Automated Incremental Backup Menu by typing

>y

and press the Enter key.

Go to step 24.

Creating SDM backup tapes
Automated incremental backups (continued)

18 Select “View Automated Incremental Backup Schedule” by typing

>3

and pressing the Enter key. The current schedule is displayed.

In the example shown, the automated incremental backup occurs daily at 2 a.m. (See example of scheduling an incremental backup in step 12.)

Example response:

```
The Automated Incremental Backup is scheduled as follows:


        Tape Drive :     DAT0

        Week       :     Daily
        Month      :     –
        Day        :     –
        Hour       :     2
        Minutes    :     0

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

Note: If you attempt to view the automated incremental backup schedule when none has been created, an error message is displayed. You are prompted to return to the Automated Incremental Backup Menu.

Response:

```
The Automated Incremental Backup is not scheduled.

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

19 Return to the Automated Incremental Backup Menu by typing

>y

and pressing the Enter key.

20 Determine whether you wish to change the current automated incremental backup schedule.

If you wish to	Do
use the current automated incremental backup schedule	step 21
change the schedule for automated incremental backups	step 7

Creating SDM backup tapes
Automated incremental backups (end)

21 Exit the Automated Incremental Backup Menu by typing

>0

and pressing the Enter key. The Incremental Backup and Restore Menu is displayed.

22 Exit the Incremental Backup and Restore Menu by typing

>0

and pressing the Enter key. The Backup and Restore Main Menu is displayed.

23 Exit the Backup and Restore Menu by typing

>0

and pressing the Enter key.

i
24 You have completed this procedure.

Restoring the SDM
Full restore from S-tape and I-tape

Application

ATTENTION

This procedure must be performed by a trained AIX system administrator who has root user privileges to access the SDM.

ATTENTION

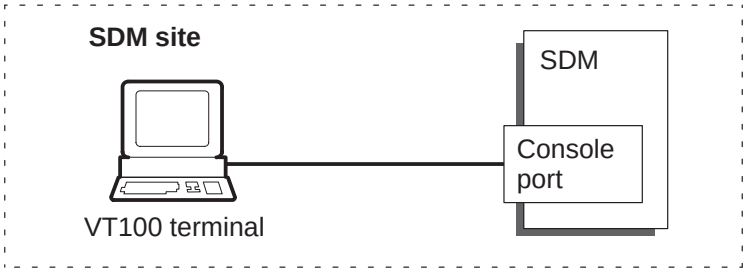
All volume groups on the SDM must be fully mirrored (Mirrored) before performing this procedure. If you attempt to perform this procedure when disk mirroring is not Mirrored, an error message is displayed on the screen.

ATTENTION

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

Use this procedure to perform a full restore of the SDM software load from the system image backup tape (S-tape) and the most recent incremental backup tape (I-tape). A full software restore is required when the SDM is out of service because the software load has become corrupted.

This procedure must be performed by the root user from a local VT100 console as shown in following figure.



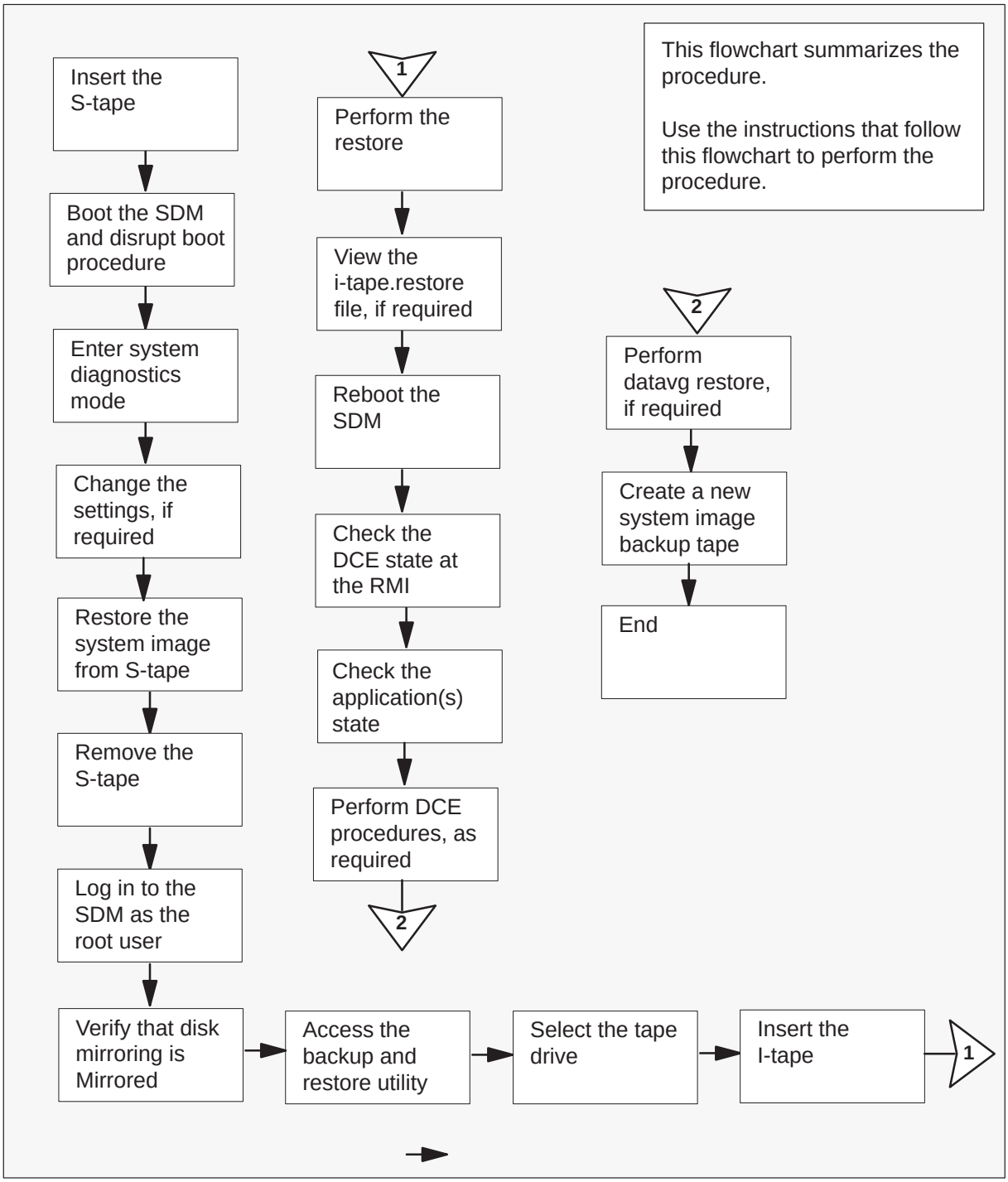
Restoring the SDM
Full restore from S-tape and I-tape (continued)

Action

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

Restoring the SDM
Full restore from S-tape and I-tape (continued)

Summary of Full restore from S-tape and I-tape



Restoring the SDM
Full restore from S-tape and I-tape (continued)

Full restore from S-tape and I-tape

At the SDM

1 Ensure that one of the SDM tape drives (slot 2 or 13 in the main chassis) contains the system image backup tape (S-tape).

Note: Nortel recommends that you use tape drive DAT0 (option for performing a full restore from an S-tape) if your system also includes SBA.

At the MSP

2 Boot the SDM by turning the power off, then on, using the MSP breaker that supplies power to the SDM.

At the local VT100 console

3 When the system displays “COLD start...”, press the Break key or the Esc key twice to interrupt the boot process. The system takes about 4 min to initialize.

4 Proceed, depending on the prompt that is displayed on the screen.

If the prompt is	Do
FX-Bug	step 7
FX-Bug and you are in a menu	step 5
FX-Diag	step 6

5 From the selection menu, select “Go to System Debugger”, by typing

>3
and pressing the Enter key.

Go to step 7.

6 Switch the directory to FX-Bug, by typing

>sd
and pressing the Enter key.

Restoring the SDM
Full restore from S-tape and I-tape (continued)

7 View the input/output devices on the SDM to verify the address of the tape drive from the FX-Bug prompt. Type

Fx-Bug>ioi

and press the Enter key.

Example response:

```
CLUN  DLUN  CNTRL-TYPE  DADDR  DTYPE  RM  Inquiry–Data
  1     0   IO          0      $00    N   SEAGATE ST11200N ST 31200 0660
  3     0   IO          0      $00    N   SEAGATE ST12400N ST32430 0660
  3    50   IO          5      $01    Y   ARCHIVE Python 28388-XXX 5.45
  6     0   IO          0      $00    N   SEAGATE ST11200N ST31230 0660
  8     0   IO          0      $00    N   SEAGATE ST12400N ST32430 0660
  8    50   IO          5      $01    Y   ARCHIVE Python 28388-XXX 5.45
```

Note: In the example response, the tape drive is ARCHIVE.

Wait for the FX-Bug prompt, and then type

Fx-Bug>pboot <address for Archive Python>

and press the Enter key.

In the example, the following are valid choices:

- pboot 3 50 if the tape drive is located in slot 2
- pboot 8 50 if the tape drive is located in slot 13

8 Wait about 4 min after the pboot command is entered. You are then asked to define the console setting and the language setting. To define the console setting, select option 1 and press the Enter key.

Note: When you define the console setting, the “1” is not echoed on the screen.

Type1 to select the language setting, and press the Enter key. The Welcome to Base Operating System Installation and Maintenance menu is then displayed.

Restoring the SDM
Full restore from S-tape and I-tape (continued)

9 Select “Change/Show Installation Settings and Install” by typing

>2

and pressing the Enter key. The System Backup Installation and Settings menu is displayed.

Example response:

```
              System Backup Installation and Settings

Either type 0 and press Enter to install with the current settings, or
type the number of the setting you want to change and press Enter.

    Setting:                              Current Choice(s):
1   Disk(s) where you want to install     hdisk0...
         Use Maps                          No
2   Shrink File System                    No


>>> 0 Install with the settings listed above.
```

Note: “...” shown under Current Choice(s) indicates that more than one disk is currently in use.

10 The default disk for the installation is hdisk0, located in slot 2 of the main chassis. If your SDM contains one disk drive in each domain of the main chassis, accept the default setting. Only change the default settings if you want to install the backup image on the alternate 4Gbyte hard disk.

To	Do
change the current settings	step 11
use the current settings	step 14

11 To change the disks where you want to install the backup image, type

>1

and press the Enter key.

Restoring the SDM
Full restore from S-tape and I-tape (continued)

The Change Disk(s) Where You Want to Install menu is displayed.

Example response:

```
           Change Disk(s) Where You Want to Install

Type one or more numbers for the disk(s) to be used for installation and
press Enter.  To cancel a choice, type the corresponding number and Press
Enter.  At least one bootable disk must be selected.  The current choice
is indicated by >>>.

      Name     Location Code  Size(MB)   VG Status    Bootable   Maps
    1 hdisk1   c1-f4-00-0,0       2039   rootvg           Yes     No
>>> 2 hdisk0   c1-f2-00-0,0       1006   not in any v     Yes     No
>>> 3 hdisk2   c1-f13-00-0,0      1006   not in any v     Yes     No
    4 hdisk3   c1-f15-00-0,0      2039   rootvg           Yes     No
```

This menu displays the list of all available disks on which you can install the system backup image. The currently selected disks are indicated by >>>.

Note: The system backup backup must be installed on one disk in each domain to achieve fault-tolerant operation. Valid choices in the example in step 11 are hdisk0 and hdisk2, or hdisk1 and hdisk3. Disks in domain 0 are installed in slots 1 to 5. Disks in domain 1 are installed in slots 12 to 16 in the main chassis.

12 To select a disk or disks, enter the number of the disk, and press the Enter key. To deselect a selected disk, enter its number again and press the Enter key.

13 When you have finished entering the settings, the System Backup Installation and Settings menu is displayed. Type

>0

and press the Enter key.

Go to step 10.

14 To accept the current settings type

>0

and press the Enter key.

15 The restore process begins, and lasts about 25 min. During the restore process, the screen displays the approximate percentage of tasks completed, and the elapsed time.

Note: As part of the restore, the system reboots automatically and displays the login prompt.

At the SDM

Note: If there is only an I-tape and no I-tape has been made, go to step 39.

16 Remove the S-tape from the tape drive when the reboot is completed and store it in a secure location.

Restoring the SDM
Full restore from S-tape and I-tape (continued)

At the local or remote terminal

17 Log in to the SDM as the root user. Press the Enter key when you see the "TERM=(vt100)" prompt.

18 Access the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

19 Access the system (Sys) menu level by typing

>SYS
and pressing the Enter key.

20 Access the storage menu level by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                          Mirrored
  Volume              Size(MB)              (% full/ threshold)
 1 /                     20                        25/ 80
 2 /usr                  192                       85/ 90
 3 /var                  40                        17/ 80
 4 /tmp                  20                        11/ 90
 5 /home                 300                       27/ 70
 6 /sdm                  192                       65/ 90
(unallocated)            972

Disk mirroring (datavg):                          Mirrored
   Volume              Size(MB)              (% full/ threshold)
 7 /data                 112                       4/ 80
 (unallocated)           8000
```

21 Determine at the storage menu level if disk mirroring for all volume groups is in service (Mirrored).

If disk mirroring is	Do
Mirrored	step 23
Integrating or Not Mirrored	step 22

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

Restoring the SDM
Full restore from S-tape and I-tape (continued)

23 Access the administration (Admin) menu level of the RMI by typing

>ADMIN

and pressing the Enter key.

24 Access the Backup and Restore Main Menu by typing

>5

and pressing the Enter key.

Note: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

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

25 From the Backup and Restore Main Menu, select “Incremental Backup and Restore” by typing

>3

and pressing the Enter key.

26 From the Incremental Backup and Restore Menu, select “Restore All Files from an I-tape” by typing

>5

and pressing the Enter key.

27 After you select option 5, you are prompted to select the tape drive.

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

28 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

Restoring the SDM
Full restore from S-tape and I-tape (continued)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the Incremental Backup and Restore Menu if you do not wish to use DAT1.

29 After you select the tape drive, the system prompts you to enter the I-tape into the appropriate tape drive.

Example response:

```
Please insert your Incremental Backup tape (I-tape)
into the tape drive DAT0.

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

30 When you have inserted the tape and are ready to continue this procedure, type

>y

and press the Enter key. The file restore begins immediately.

Response:

```
Rewinding the tape...

Restoring all files and directories from the incremental
backup tape (I-tape).

A log file /tmp/i-tape.restore is being created.
Restoring is in progress.
```

Note: An error message is displayed if the restore is unsuccessful. If this occurs, go to step 52.

Restoring the SDM
Full restore from S-tape and I-tape (continued)

31 The system informs you when the restore is complete. You are then prompted to return to the Incremental Backup and Restore Menu.

Response:

```
All files were restored from the incremental backup tape.
A log file is in /tmp/i–tape.restore.


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

32 When you are ready to return to the Incremental Backup and Restore Menu, type

>y
and press the Enter key.

33 Return to the Backup and Restore Main Menu by typing

>0
and pressing the Enter key.

34 Exit the backup and restore utility by typing

>0
and pressing the Enter key.

35 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

36 The UNIX prompt is displayed after you exit the RMI. The system informs you when the restore is complete (see response in step 31). You may also wish to view the i-tape.restore file.

To	Do
view the i-tape.restore file	step 37
continue this procedure	step 38

Restoring the SDM
Full restore from S-tape and I-tape (continued)

37 Access the I-tape.restore file by typing

 # cd /tmp
at the prompt and pressing the Enter key.

Scroll through the file by typing

 # more i-tape.restore
and pressing the Enter key.

Press the spacebar to scroll through the listing. When the listing is finished, the screen displays when the restore from the I-tape was performed. Press the spacebar again to restore the UNIX prompt.

38 The system restore is complete. Reboot the SDM by typing

 # rebootsdm
and pressing the Enter key.

The reboot display takes about 1 min to appear. The reboot takes about 5 min to complete.

39 Log in to the SDM as the root user. Press the Enter key when you see the "TERM=(vt100)" prompt.

40 Access the RMI by typing

 # sdmmtc
and pressing the Enter key. The top menu level of the RMI is displayed.

41 Access the LAN menu level of the RMI by typing

>LAN
and pressing the Enter key.

Check the state of DCE.

Example response:

```
DCE State: SysB
```

42 Access the application (APPL) menu level of the RMI to check the state of any DCE-based applications. Type

>APPL
and press the Enter key.

Example response:

```
# Package Description       Version       State
1 Table Access Service      8.0.19.0      InSv
2 Operation Measurements    8.0.19.0      InSv
3 Log Delivery Service      8.0.19.0      InSv
4 Enhanced Terminal Access  8.0.19.0      Fail
5 Exception Reporting       8.0.19.0      Fail
```

Restoring the SDM
Full restore from S-tape and I-tape (continued)

43 DCE and DCE-based applications may fail if the keytab files restored from tape contain obsolete keys. If the DCE state is displayed as SysB at the LAN menu level of the RMI (step 41), and the logs displayed indicate an error with the security client service in DCE, restore the service by performing the following procedures described in the “SDM system administration procedures” chapter of this document:

- ”Distributed Computing Environment-Removing an SDM from a DCE cell” on page 6-110
- ”Distributed Computing Environment-Configuring an SDM in a DCE cell” on page 6-97

If some DCE-based applications are faulty (Fail state, see step 42), restore them by executing the procedure to add the application server to the DCE cell. This procedure is documented in the NTP for each specific application.

44 Proceed depending on if your system includes the data volume group (datavg).

If your system	Do
has datavg	step 45
does not have datavg	step 51

Note: Datavg is shown at the storage menu level of the RMI.

45 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

46 Identify the ID of the small computer systems interface (SCSI) to the hard disk number, by typing

 # lsdev -Cc disk
and pressing the Enter key.

47 Identify the disks that are part of the root volume group (rootvg) and datavg, by typing

 # lspv
and pressing the Enter key.

48 For each volume group, run the hard disk number by typing

 # importvg -y datavg hdisk#
and pressing the Enter key.

Restoring the SDM
Full restore from S-tape and I-tape (end)

Note: The hdisk# is any disk that does not belong to rootvg, but used to belong to datavg.

49 For each volume group other than rootvg, type

 # varyonvg volume group
and press the Enter key.

where

volume group is rootvg or datavg

50 Synchronize the object data manager (ODM) and mount all file systems on reboot, by typing

 # shutdown -Fr
and pressing the Enter key.

51 You must create a new system image backup tape. Refer to the procedure ”Creating SDM backup tapes– System image backup tape (S-tape)” on page 6-26 in this document.

52 You have completed this procedure.

Restoring the SDM
Partial restore from the system image tape (S-tape)

Application

ATTENTION

This procedure must be performed by a trained AIX system administrator who has root user privileges to access the SDM.

CAUTION

Possible loss of data

Use this procedure at the discretion of the system administrator. Perform a partial restore only if you are familiar with the files, and know exactly which files are to be restored. If you restore the wrong files, you may inadvertently corrupt SDM software.

ATTENTION

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

ATTENTION

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

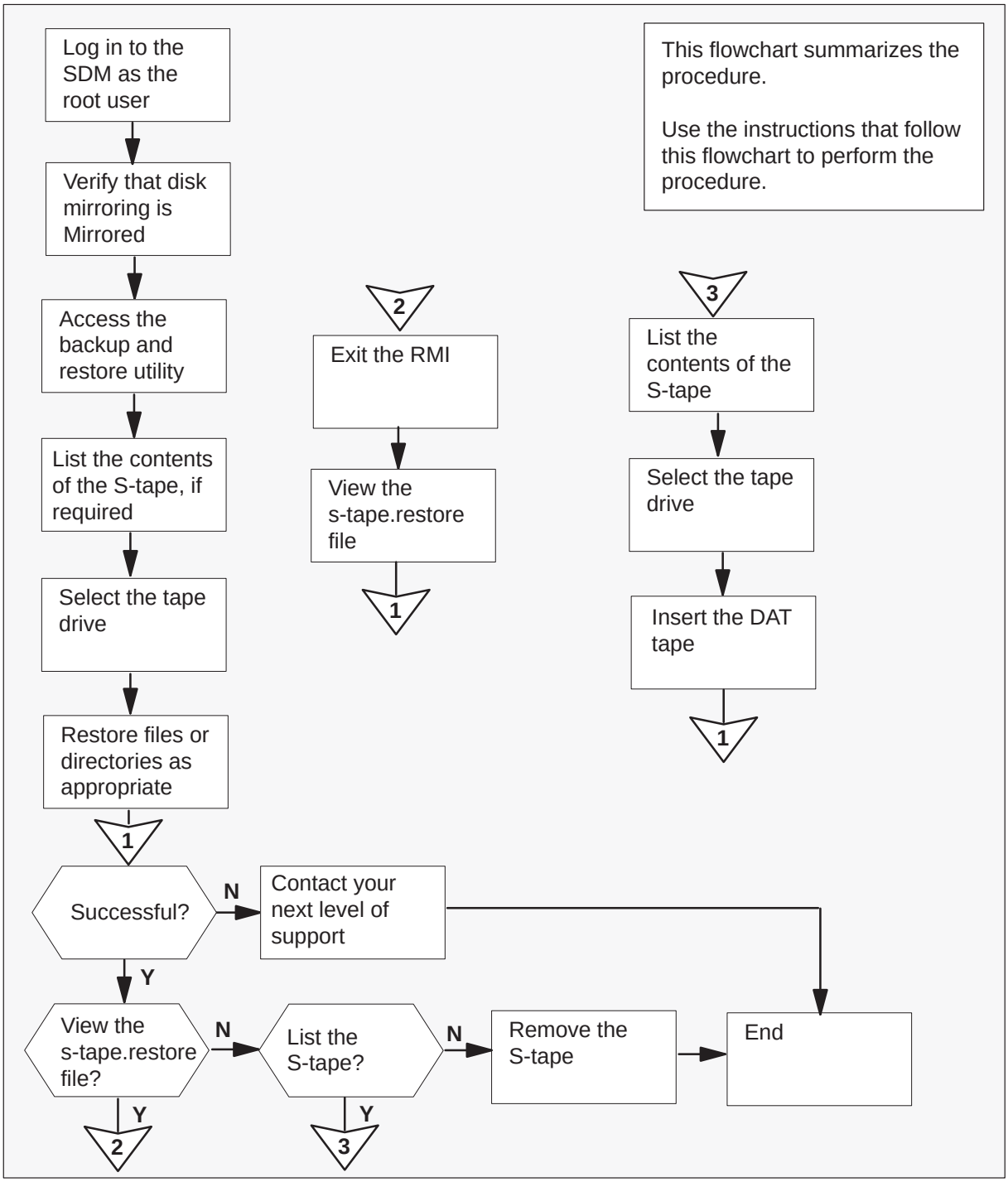
Use this procedure to restore individual files or sets of files from the system image backup tape (S-tape). This procedure can be performed by the root user from a local or remote terminal.

Action

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

Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

Summary of Partial restore from the system image tape (S-tape)



Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

Partial restore from the system image tape (S-tape)

At the local or remote console

1 Log in to the SDM as the root user.

2 Access the RMI by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                          Mirrored
  Volume              Size(MB)                (% full/ threshold)
 1 /                     20                          25/ 80
 2 /usr                  192                         85/ 90
 3 /var                  40                          17/ 80
 4 /tmp                  20                          11/ 90
 5 /home                 300                         27/ 70
 6 /sdm                  192                         65/ 90
(unallocated)            972

Disk mirroring (datavg):                            Mirrored
   Volume              Size(MB)                  (% full/ threshold)
 7 /data                 112                         4/ 80
 (unallocated)           8000
```

5 Determine at the storage menu level if disk mirroring for all volume groups is Mirrored.

If disk mirroring is	Do
Mirrored	step 7
anything else	step 6

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

Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

7 Access the administration (Admin) menu level of the RMI by typing

>ADMIN
and pressing the Enter key.

8 Access the Backup and Restore Main Menu by typing

>5
and pressing the Enter key.

Note: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

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

9 From the Backup and Restore Main Menu, select “System Image Backup and Restore Menu” by typing

>2
and pressing the Enter key.

Note: If disk mirroring for all volume groups is not Mirrored, an error message is displayed. You are prompted to return to the System Image Backup and Restore Menu.

10 Determine if you need to list the contents of the S-tape to determine the full path name of the directory or file you wish to restore.

If you	Do
wish to list the S-tape	step 11
do not wish to list the S-tape	step 20

11 From the System Image Backup and Restore Menu, select “List Contents of the System Image Tape (S-tape)” by typing

>3
and pressing the Enter key.

Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

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

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

13 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

14 After you select the tape drive, the system prompts you to insert the S-tape into the appropriate tape drive.

Example response:

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

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

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

Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

At the SDM

15 Insert the S-tape into the tape drive you selected.

At the local or remote VT100 console

16 When you are ready to continue this procedure, type

>y
and press the Enter key.

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

Response:

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

18 Return to the System Image Backup and Restore Menu by typing

>y
and pressing the Enter key.

19 The next step of this procedure depends on why you are listing the contents of the S-tape.

If you are verifying	Do
that the file has been restored	step 28
the file name or directory that you wish to restore	step 20

20 From the System Image Backup and Restore Menu, select “Restore Files from the System Image Tape (S-tape)” by typing

>4
and pressing the Enter key.

21 After you select option 4, you are prompted to select the tape drive.

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

22 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

23 After you select the tape drive, you are prompted to insert the S-tape into the appropriate tape drive. A warning is displayed advising that this procedure must only be completed by qualified SDM system administrators. The warning also advises that files and directories must be entered exactly as they appear in the file listing. Insert the S-tape in the appropriate tape drive.

Response:

```
Are you ready to enter the name of the file or directory? ( y | n )
```

24 Continue this procedure, by typing

>y

and pressing the Enter key.

Response:

```
Enter the name of the directory or file that you wish to
restore as ./<your-full-path>/<your-file-or-directory>.

Note: Tape processing may take a few minutes to complete.
      A log file /tmp/s-tape.restore will be created.

==>
```

25 Enter the full path name of the directory or file that you wish to restore, exactly as shown in the file listing, including “./” at the beginning. A log file /tmp/s-tape.restore is created when the restore is completed.

Restoring the SDM
Partial restore from the system image tape (S-tape) (continued)

Note: An error message is displayed if the restore is unsuccessful. If this occurs, go to step 28.

26 During the restore process, the screen will not display any additional information. When the file restore is complete, the file you have restored is displayed. The system then prompts you to return to the System Image Backup and Restore Menu.

Response:

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

Note: If the restore has failed, an error message is displayed before the prompt, advising you to list the contents of the tape, and perform the procedure again.

27 To return to the System Image Backup and Restore Menu, type

>y
and press the Enter key.

28 Determine if the restore was successful. The system displays the file that you have restored, as described in step 26. You may also wish to view the s-tape.restore file or list the files on the S-tape.

If	Do
the restore is successful	step 34
the restore failed	step 37
you wish to view the s-tape.restore file	step 29
you wish to list the S-tape	step 11

29 Return to the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

30 Exit the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

31 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

Restoring the SDM
Partial restore from the system image tape (S-tape) (end)

32 Access the s-tape.restore file by typing

 # cd /tmp
at the prompt and pressing the Enter key.

Scroll through the file by typing

 # more s-tape.restore
and pressing the Enter key. Continue pressing the Enter key until the files you have restored, and the date of the restore are displayed.

33 Proceed as follows.

If the restore	Do
is successful	step 36
failed	step 37

34 Return to the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

35 Exit the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

Note: If you wish to exit the RMI, type QUIT ALL and press the Enter key.

At the SDM

36 Remove the S-tape and store it in a secure place. If you are using the automated incremental backup utility, insert the appropriate incremental backup tape (I-tape) into the tape drive.

Go to step 38.

37 Contact the personnel responsible for the next level of support.

38 You have completed this procedure.

Restoring the SDM
Partial restore from an incremental backup tape (I-tape)

Application

ATTENTION

This procedure must be performed by a trained AIX system administrator who has root user privileges to access the SDM.

CAUTION

Possible loss of data

Use this procedure at the discretion of the system administrator. Perform a partial restore only if you are familiar with the files, and know exactly which files are to be restored. If you restore the wrong files, you may inadvertently corrupt software.

ATTENTION

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

ATTENTION

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

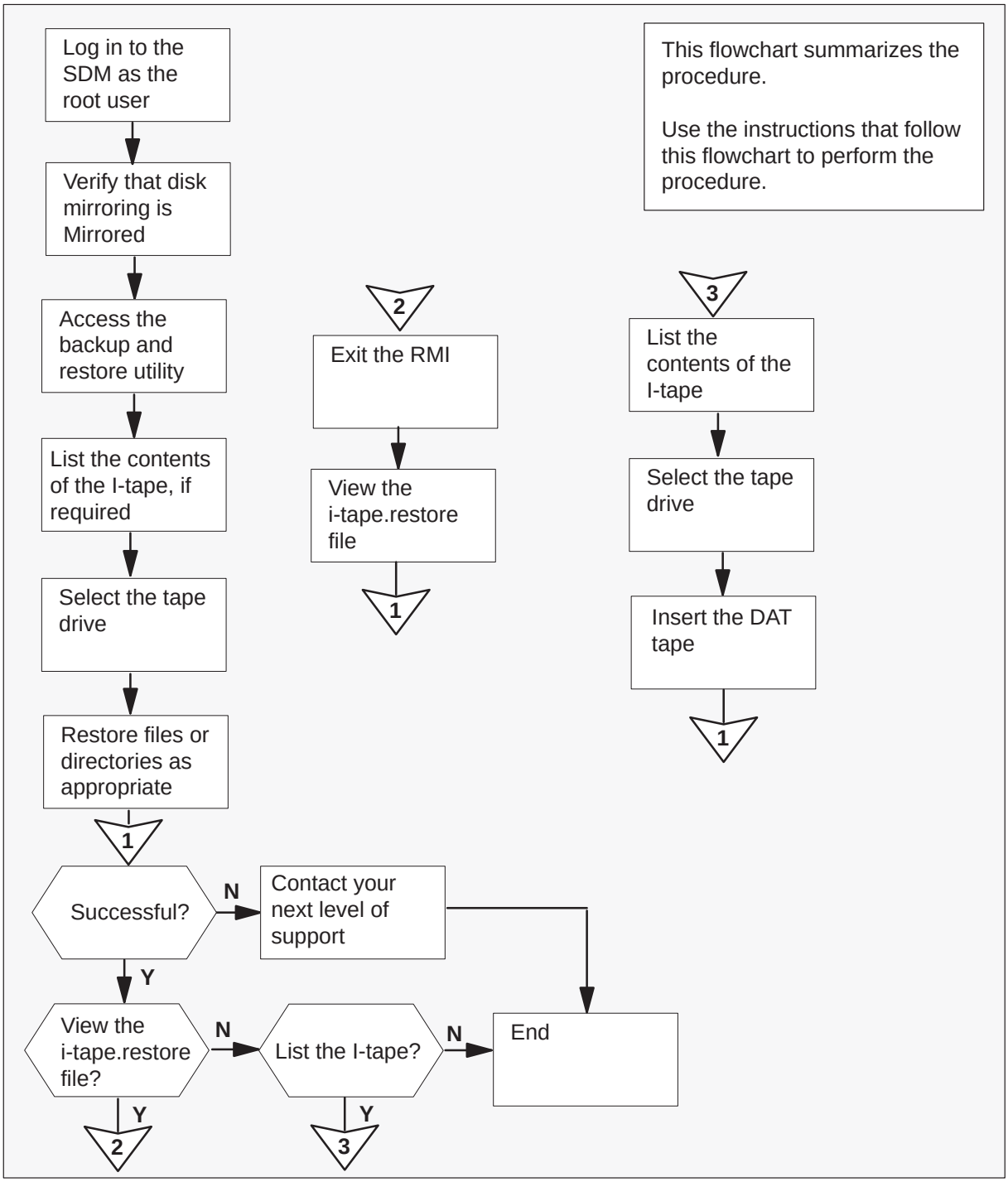
Use this procedure to restore individual files or sets of files from the incremental backup tape (I-tape). This procedure can be performed by the root user from a local or remote terminal.

Action

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

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

Summary of Partial restore from an incremental backup tape (I-tape)



Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

Partial restore from an incremental backup tape (I-tape)

At the local or remote console

1 Log in to the SDM as the root user.

2 Access the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

3 Access the system (Sys) menu level by typing

>SYS
and pressing the Enter key.

4 Access the storage menu level by typing

>5
and pressing the Enter key.

Example response:

```
Disk mirroring (rootvg):                          Mirrored
  Volume              Size(MB)              (% full/ threshold)
 1 /                     20                        25/ 80
 2 /usr                  192                       85/ 90
 3 /var                  40                        17/ 80
 4 /tmp                  20                        11/ 90
 5 /home                 300                       27/ 70
 6 /sdm                  192                       65/ 90
(unallocated)            972

Disk mirroring (datavg):                          Mirrored
   Volume              Size(MB)              (% full/ threshold)
 7 /data                 112                       4/ 80
 (unallocated)           8000
```

5 Determine at the storage menu level if disk mirroring for all volume groups is Mirrored.

If disk mirroring is	Do
Mirrored	step 7
anything else	step 6

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

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

7 Access the administration (Admin) menu level of the RMI by typing

>ADMIN
and pressing the Enter key.

8 Access the Backup and Restore Main Menu by typing

>5
and pressing the Enter key.

Note: If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

Example response:

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

9 From the Backup and Restore Main Menu, select “Incremental Backup and Restore” by typing

>3
and pressing the Enter key.

10 Determine if you need to list the contents of the I-tape to determine the full path name of the directory or file you wish to restore.

If you	Do
wish to list the I-tape	step 11
do not wish to list the I-tape	step 19

11 From the Incremental Backup and Restore Menu, select “List Contents of an Incremental Backup Tape (I-tape), by typing

>4
and pressing the Enter key.

12 After you select option 4, you are prompted to select the tape drive.

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

13 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the Incremental Backup and Restore Menu if you do not wish to use DAT1.

At the SDM

14 After you select the tape drive, you are prompted to insert the I-tape into the tape drive you have selected.

Example response:

```
Please insert your Incremental Backup tape (I-tape) into
the tape drive DAT0 and allow a few minutes to complete the listing.

A log file will be saved in /tmp/i–tape.toc.

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

At the local or remote VT100 console

15 When you are ready to continue this procedure, type

>y

and press the Enter key.

Note: An error message is displayed if the restore is unsuccessful. If this occurs, go to step 26.

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

16 The contents of the I-tape are listed on the screen. When the listing is complete, the system prompts you to return to the Incremental Backup and Restore Menu.

Response:

```
Listing contents of the incremental backup tape is complete.
A log file is in /tmp/i-tape.toc.

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

17 When you are ready to return to the Incremental Backup and Restore Menu, type

>y
and press the Enter key.

18 The next step of this procedure depends on why you are listing the contents of the I-tape.

If you are verifying	Do
that the file has been restored	step 26
the file name or directory that you wish to restore	step 19

19 From the Incremental Backup and Restore Menu, select “Restore Selective Files from an I-tape by typing

>6
and pressing the Enter key.

20 After you select option 6, you are prompted to select the tape drive.

Response:

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

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

Note: Nortel recommends that you use tape drive DAT0 (option 1) if your system also includes SBA.

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

21 Select the tape drive you wish to use, by typing

>n

and pressing the Enter key.

where

n is the tape drive you wish to use (1 or 2)

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

Response:

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

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

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

If you wish to continue using DAT1, type “y” and press the Enter key. If you do not wish to use DAT1, type “n” and press the Enter key. The system prompts you to return to the Incremental Backup and Restore Menu if you do not wish to use DAT1.

22 After you select the tape drive, you are prompted to insert the I-tape into the appropriate tape drive, if the tape is not already inserted. A warning is displayed advising that this procedure must only be performed by qualified SDM system administrators. This warning also advised that files and directories to be restored must be entered exactly as they appear in the file listing. You are then prompted to enter the name of the directory or file that you wish to restore.

Response:

```
Enter the name of the directory or file that you wish to restore:
==>
```

23 Enter the full path name of the directory or file that you wish to restore exactly as shown in the listing, including “./” at the beginning. For example, “/etc/inittab”. The system displays the names of the files as they are restored.

Example response:

```
Restoring /tmp/data from the incremental backup tape.
A log file /tmp/i-tape.restore is being created.

Restoring is in progress.
5350 blocks
/tmp/data
```

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (continued)

24 When the files have been restored, the following message is displayed:

Response:

```
Restore is complete.
A log file is in /tmp/i-tape.restore.

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

25 To return to the Incremental Backup and Restore Menu, type

>y
and press the Enter key.

26 Determine if the restore is complete. The system informs you when the restore is complete, as shown in the response in step 24. You may also wish to view the i-tape.restore file or list the files on the I-tape.

If	Do
the restore is successful	step 32
the restore failed because the files could not be found	step 34
the restore failed for any other reason	step 35
you wish to view the i-tape.restore file	step 27
you wish to list the I-tape	step 11

27 Return to the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

28 Exit the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

29 Exit the RMI by typing

>QUIT ALL
and pressing the Enter key.

Restoring the SDM
Partial restore from an incremental backup tape (I-tape) (end)

30 Access the i-tape.restore file by typing

 # cd /tmp
at the prompt and press the Enter key.

Scroll through the file by typing

 # more i-tape.restore
and pressing the Enter key. Continue pressing the Enter key until the files you have restored, and the date of the restore are displayed.

31 Proceed as follows

If the restore	Do
is successful	step 34
failed	step 35

32 Return to the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

33 Exit the Backup and Restore Main Menu, by typing

>0
and pressing the Enter key.

Note: If you wish to exit the RMI, type QUIT ALL and press the Enter key.

Go to step 36.

At the SDM

34 The specified files are not on the I-tape. Verify the contents of the I-tape to ensure the file you want to restore is on the I-tape.

If you have exited the backup utility, type “sdmmtc”, then go to step 7. If you have not exited the backup utility, go to step 11.

35 Contact the personnel responsible for the next level of support.

36 You have completed this procedure.

Installing the logreceiver tool

Application

ATTENTION

This procedure must be performed by a trained AIX system administrator who has root user privileges to access the SDM, execute access to FTP on the SDM, and write permissions to the directory where the logreceiver tool will be installed.

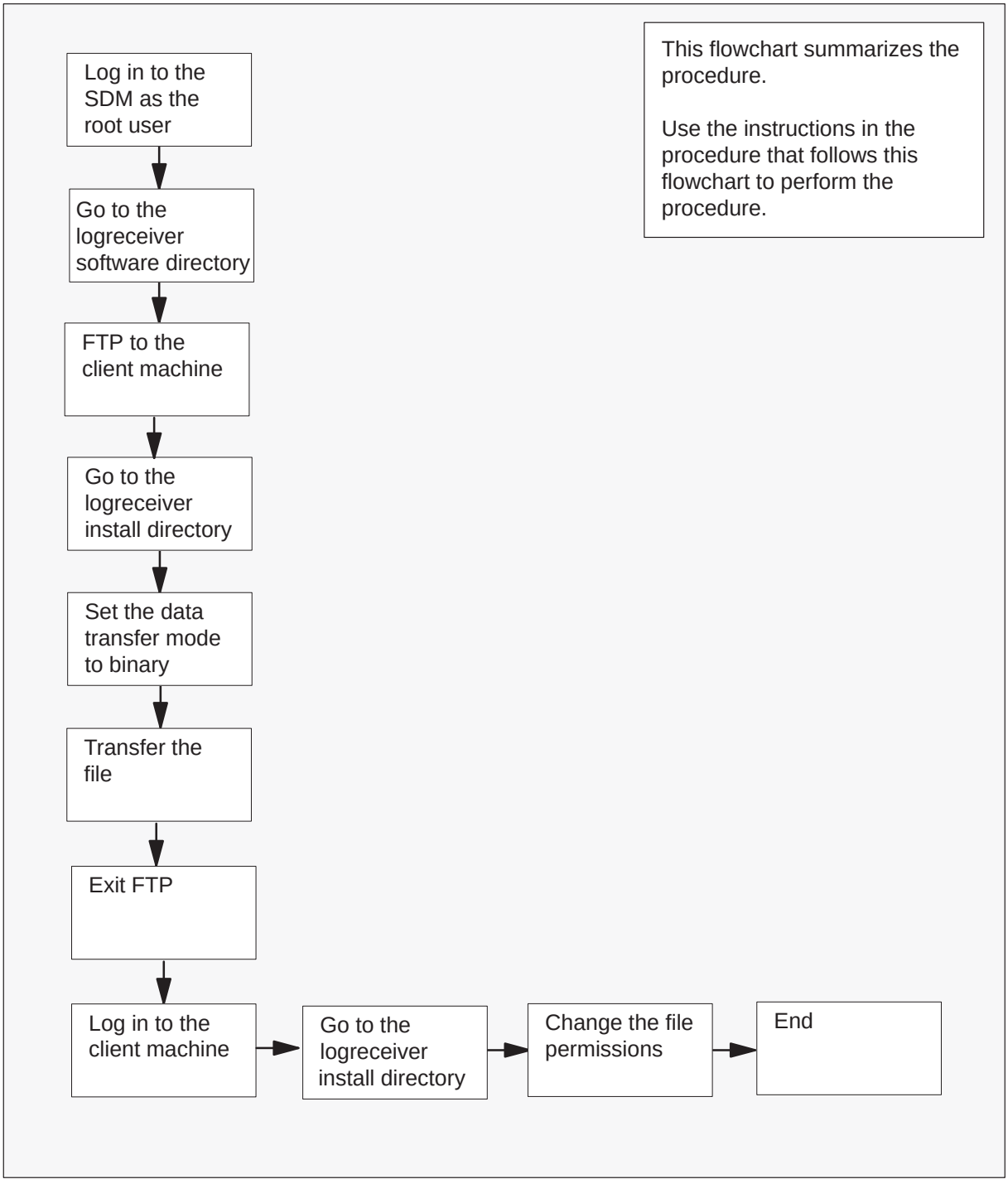
Use this procedure to install the logreceiver tool on a workstation. The procedure accesses the logreceiver software stored on an SDM to which the workstation can connect, and installs it in a specified directory location on the workstation.

Action

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

Installing the logreceiver tool (continued)

Summary of Installing the logreceiver tool



Installing the logreceiver tool (continued)

Installing the logreceiver tool

At the local or remote VT100 terminal

1 Log in as the root user to the SDM where the logreceiver tool is stored.

2 Go to the SDM directory that contains the logreceiver tool by typing

 # cd /sdm/logs/osf
and pressing the Enter key.

3 FTP to the client machine where the logreceiver tool is to be installed, by typing

 # ftp *client*
and pressing the Enter key.

where

client is the IP address of the client workstation where you are installing the logreceiver tool

4 When prompted for “Name:”, type

> root
and press the Enter key.

5 When prompted for “Password:”, type

> password
and press the Enter key.

where

password is the root password for the client machine

6 Go to the client machine directory where you wish to install the logreceiver tool by typing

ftp>cd install_dir
and pressing the Enter key.

where

install_dir is the client machine directory where the logreceiver tool is to be installed. The logreceiver tool can be installed in a directory of the client’s choice or it could be installed in the /sdm/bin directory.

7 Set the data transfer mode to binary by typing

ftp>bin
and pressing the Enter key.

Installing the logreceiver tool (end)

8 Determine if the client machine is a SUN or HP (Hewlett Packard) workstation.

If the client machine is a	Do
an HP workstation	step 9
a SUN workstation	step 10

9 Send the software from the SDM to the client machine (HP workstation) by typing

ftp>put logreceiver.hp logreceiver
and pressing the Enter key.

Go to step 11.

10 Send the software from the SDM to the client machine (SUN workstation) by typing

ftp>put logreceiver.sun logreceiver
and pressing the Enter key.

11 Exit FTP by typing

ftp>quit
and pressing the Enter key.

12 Log in to the workstation.

13 Go to the directory where the logreceiver is installed by typing

 # cd install_dir
and pressing the Enter key.

where

install_dir — is the directory where the logreceiver tool was installed (see step 6)

14 Alter the permission so that logreceiver can be executed from within that directory, by typing

 # chmod a+rx logreceiver
and pressing the Enter key.

15 You have completed this procedure.

Distributed Computing Environment Configuring an SDM in a DCE cell

Application

ATTENTION

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

ATTENTION

If you use the default cell_admin "master administrator" account (full configuration only), the administrative user's password is sent in clear text across the network when you use Enhanced Terminal Access (ETA) or telnet to access the SDM remotely. Nortel recommends that you execute the command from a terminal that is attached to the SDM console port, to ensure password security.

When an SDM is installed, it must be configured in the DCE cell to function properly. This procedure assumes that a DCE cell is already in operation.

To perform this procedure you must know the password to use the cell_admin DCE account (or principal) that is automatically created with the DCE cell. The cell_admin DCE account has the required privileges to make changes to the DCE cell.

Alternatively, the cell_admin principal can also create a subadministrator account with limited privileges for the sole purpose of adding SDMs to the DCE cell. If you choose to create a subadministrator account, the following privileges are required:

- quotas to create principals
- read and insert permissions on the / .:/hosts cell directory service (CDS) directory

Before performing this procedure, determine if you are going to configure the SDM in the DCE cell using full configuration (one step) or local configuration (two steps). Nortel recommends that you use full configuration to perform this procedure because it is simpler, less prone to errors, and it is controlled by the SDM commissioning tool.

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

To configure the SDM in a DCE cell using the full configuration procedure, you must be able to

- log on as the root user to the SDM that is being configured
- provide a DCE administrator account principal name (cell_admin or an equivalent principal), and its password, and all other required parameters when running the “sdmconfig” program

If, for security reasons, the user configuring the SDM into the DCE cell cannot obtain both the root password of the SDM, and the cell_admin password, use local DCE configuration. To use local configuration, you must be able to

- log in as the DCE administrator to a machine (another SDM, a Motorola PowerStack or an IBM RS-6000 workstation) other than the SDM being configured. This machine is an active node in the DCE cell, and it must be running the AIX version of DCE. It is not necessary to log in as the root user.
  - — If you are performing this step on an SDM that is already configured in the DCE cell, the “mkdce” command is not accessible to the maintenance (maint) user. You must, therefore, log in as the root user to that SDM. If you cannot log in as root, have the root user add a special user on that SDM that the DCE administrator can use to perform the local configuration procedure. Refer to the procedure ”Adding or removing a maintenance user” on page 6-10 in this document. Ensure that this special user’s initial program field is set to /bin/csh or some other UNIX shell other than /sdmtools/bin/cm_screener.
- run the “mkdce -o admin” command providing a DCE administrator account principal name and password, and the hostname and IP address of the SDM being preconfigured. The “mkdce” program is only available on machines that run the AIX version of DCE.
- log in as root to the SDM being configured, and run the “sdmconfig” program and provide all the required parameters for local SDM DCE configuration

Note: You cannot commission DCE until you have commissioned the LAN. If you attempt to commission DCE before commissioning the LAN, an error message will be displayed. For information on LAN commissioning, refer to the procedure ”Commissioning SDM-LAN connectivity” on page 4-89 in the “SDM maintenance procedures” chapter of this document.

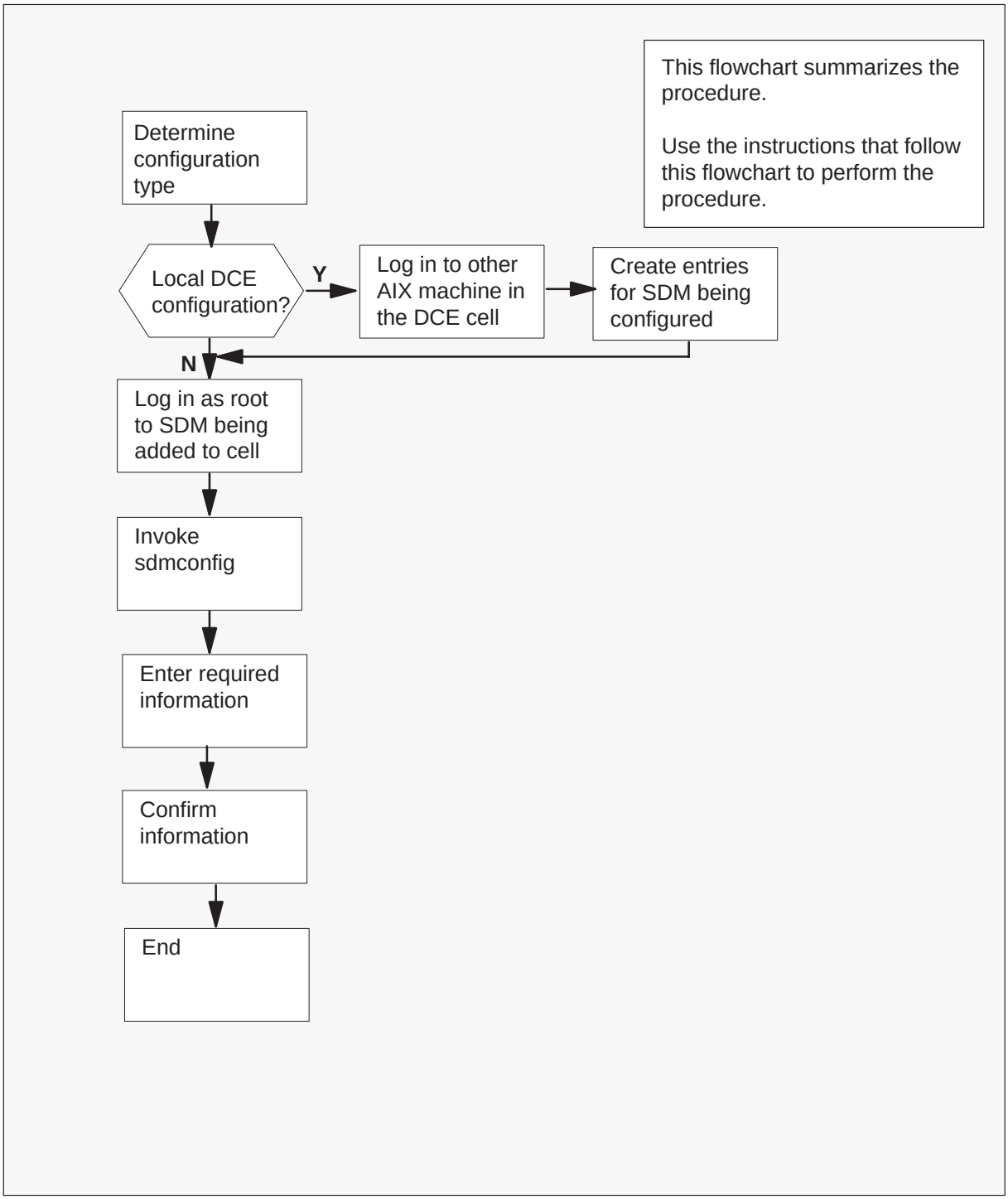
Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

Action

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

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

Summary of Configuring an SDM in a DCE cell



Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

Configuring an SDM in a DCE cell

At the SDM

1 Determine which method you wish to use to configure the SDM in a DCE cell.

If you are using	Do
full DCE configuration	step 5
local DCE configuration	step 2

2 Log in as any user that can execute UNIX commands to a machine other than the SDM being configured. This machine must be an active node in the DCE cell, and must be running the AIX version of DCE.

3 Create entries for the SDM being configured in the DCE servers by typing

>mkdce -o admin -a DCE_admin_principal_name -h target_SDM_hostname -i IP_address_of_the_target_SDM -p profile_name all_cl

and pressing the Enter key

where

DCE_admin_principal_name	is the DCE administrator's principal name
target_SDM_hostname	is the hostname of the SDM that you are configuring in the DCE cell
IP_address_of_the_taget_SDM	is the IP address of the SDM that you are configuring in the DCE cell
profile_name	is the name of the DCE LAN profile for the SDM. To use the default profile (lan_profile), omit this parameter, and the "-p" before it.

Example response:

```
Configuring Security Client (sec_cl) for dce_host bnode76
on
machine 47.105.144.30 ...
Password must be changed!
Complete admin configuration of Security Client (sec_cl)
for
  dce_host bnode76 on machine 47.105.144.30

Configuring CDS Clerk (cds_cl) for dce_host bnode76 on
  machine 47.105.144.30 ...
```

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

```
          Modifying acls on hosts/bnode76
          Modifying acls on hosts/bnode76/self
          Modifying acls on hosts/bnode76/cds-clerk
          Modifying acls on hosts/bnode76/profile
          Modifying acls on / .:/lan-profile

Completed admin configuration of CDS Clerk (cds_cl) for
  dce_host bnode76 on machine 47.105.144.30

Cell administrator's portion of client configuration has
completed
  successfully.  Root administrator for
47.105.144.30 should now complete the client configuration
on that
machine.

#
```

4 At the prompt, enter the password for the DCE account cell_admin by typing

>password
and pressing the Enter key.

where

password is the password for the DCE account cell_admin

5 Log in as the root user to the SDM that you are adding to the DCE cell.

6 Invoke the SDM commissioning tool by typing

 # sdmconfig
and pressing the Enter key.

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

7 The DCE configuration screen is displayed.

Response:

```
                        SDM COMMISSIONING

DCE

You will be asked to select:
–Local DCE configuration, or
–Full DCE configuration

After your selection, you will be prompted for the
following information:
- the DCE cell name
- the DCE hostname of the SDM
- the IP address and hostname of the master Security
Server
- the IP address and hostname of the CDS Server
- the LAN profile for the SDM (FULL configuration only)
- the DCE Principal Name (FULL configuration only)
- the DCE Principal (or equivalent) password (FULL
configuration only)

Do you wish to proceed with DCE commissioning? [YES]
```

Note 1: DCE hostname is the name set to the UNIX hostname for the SDM. If you enter a different name, the DCE application server initialization may fail.

Note 2: LAN profile is the name of the DCE LAN profile that supports the portion of the cell (LAN) that this SDM is in. The LAN profile is mainly used for defining the local Distributed Time Service (DTS) servers that provide time synchronization for “electronically close” DCE nodes. For a small DCE cell, you can select the default LAN profile (lan-profile); then all the nodes in the cell will use the same set of DTS local servers.

8 Ensure that you know the required information shown in step 7. To proceed with DCE commissioning, press the Enter key. You are then prompted to select Local or Full DCE commissioning.

Response:

```
                        SDM COMMISSIONING

DCE

Please select either (L)ocal or (F)ull DCE commissioning:
```

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

9 Proceed according to the method you are using to configure the SDM in a DCE cell.

If you are using	Do
full DCE configuration	step 10
local DCE configuration	step 16

10 Select full DCE configuration by typing

>F
and pressing the Enter key.

11 For full DCE configuration, you are prompted to enter the following information in the order shown. Press the Enter key to get prompted for the next information request.

- the DCE principal name
- the DCE cell name
- the IP address of the master Security Server
- the hostname of the master Security Server
- the IP address of the cell directory service (CDS) server
- the LAN profile for the SDM

Example response:

```
                    SDM COMMISSIONING

FULL DCE CONFIGURATION

Please enter the DCE principal name: [cell_admin]
```

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

12 Enter the required information, as prompted. When you have entered all required information, the values are displayed on the screen. You are prompted to confirm whether the values are correct.

Example response:

```
                    SDM COMMISSIONING

FULL DCE CONFIGURATION

The following values have been entered:

DCE Administrator Principal Name:   cell_admin
DCE Cell Name:                  sdmdev.bnr.ca
Security Server IP Address:     47.105.144.9
Security Server Hostname:       bnode61
CDS Server IP Address:          47.105.144.9
CDS Server Hostname:            bnode61
LAN Profile name:               lan-red_105-profile

Are these values correct? [YES}
```

13 If the values are correct, press the Enter key. Full DCE configuration begins immediately.

Note: If you type “N” for no, you are prompted to re-enter the information in step 11. Enter the required information when prompted.

14 You will then be prompted to enter the DCE administrator’s password at the beginning of this process. When you enter the password, full configuration continues. Each item is displayed on the screen when it has been successfully configured.

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

Note: In the following example response, after the system displays the message, “Testing DCE stability....,” the system may display DCE configuration messages until the DCE is stable.

Example response:

```
                    SDM COMMISSIONING

FULL DCE CONFIGURATION

Starting DCE commissioning...

Please enter the DCE administrator’s password:
Configuring RPC Endpoint Mapper (rpc)...
Suspending the DCE Monitor process during commissioning...
RPC Endpoint Mapper (rpc) configured successfully

Configuring Security Client (sec_cl)...
Password must be changed!
Security Client (sec_cl) configured successfully

Configuring CDS Clerk (cds_cl)...
Password must be changed!
Waiting (up to 2 minutes) for cdsadv to find a CDS server.
Found a CDS server.

        Modifying acls on hosts/bnode64
        Modifying acls on hosts/bnode64/self
        Modifying acls on hosts/bnode64/cds-clerk
        Modifying acls on hosts/bnode64/profile
        Modifying acls on /.:/lan-red_105-profile

CDS Clerk (cds_cl) configured successfully

Configuring DTS Clerk (dts_cl)...
DTS Clerk (dts_cl) configured successfully

Current state of DCE configuration:
cds_cl      COMPLETE        CDS Clerk
dts_cl      COMPLETE        DTS Clerk
rpc             COMPLETE        RPC Endpoint Mapper
sec_cl      COMPLETE        Security Client

DCE has been installed.
Testing DCE stability....

DCE is stable.

Un-suspending DCE Monitor process...
```

Distributed Computing Environment
Configuring an SDM in a DCE cell (continued)

15 A message is displayed to inform you that DCE has been successfully commissioned on the SDM. You are then prompted to press the Enter key to continue.

Response:

```
DCE Commissioning PASSED

HIT ENTER TO CONTINUE
```

Go to step 23.

16 Select local DCE configuration by typing

>L
and pressing the Enter key.

17 For local DCE configuration, you are prompted to enter the following information in the order shown. Press the Enter key to get prompted for the next information request.

- the DCE cell name
- the DCE hostname of the SDM
- the IP address of the master security server
- the hostname of the master security server
- the IP address of the cell directory service (CDS) server

Response:

```
                    SDM COMMISSIONING

LOCAL DCE CONFIGURATION

Please enter the DCE cell name:
```

Distributed Computing Environment Configuring an SDM in a DCE cell (continued)

18 When all the information is entered, the values are displayed on the screen. You are then prompted to confirm that the values are correct.

Response:

```
                    SDM COMMISSIONING

LOCAL DCE CONFIGURATION

The following values have been entered:

DCE Cell Name:                  sdmdev.bnr.ca
Security Server IP Address:     47.105.144.9
Security Server Hostname:       bnode61
CDS Server IP Address:          47.105.144.9
CDS Server Hostname:            bnode61

Are these values correct? [YES}
```

19 If the values are correct, press the Enter key. Local configuration begins immediately.

Note: If you type “N” for no, you are prompted to re-enter the information in step 17. Enter the required information when prompted.

20 You will be prompted to enter the DCE administrator’s password at the beginning of this process. When you enter the password, local configuration continues. Each item is displayed on the screen when it has been successfully configured.

Example response:

```
                    SDM COMMISSIONING

LOCAL DCE CONFIGURATION

Commissioning DCE - Suspending the DCE Monitor process
during commissioning...

Un-suspending DCE Monitor process...
```

21 A message is displayed on the screen to inform you that DCE has been successfully commissioned on the SDM.

Response:

```
DCE Commissioning PASSED

HIT ENTER TO CONTINUE
```

Distributed Computing Environment Configuring an SDM in a DCE cell (end)

22 Press the Enter key. If DCE is the last item to be commissioned on the SDM, you will see the following message:

Response:

```
                SDM COMMISSIONING

SDM Commissioning complete!

#
```

If there are other items to be commissioned, the appropriate screen is displayed.

23 You have completed this procedure.

Distributed Computing Environment Removing an SDM from a DCE cell

Application

ATTENTION

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

ATTENTION

If you use the default cell_admin "master administrator" account (full removal only), the administrative user's password is sent in clear text across the network when you use Enhanced Terminal Access (ETA) or telnet to access the SDM remotely. Nortel recommends that you execute the command from a terminal that is attached to the SDM console port, to ensure password security.

If an SDM is being taken out of service permanently, it must be removed from the DCE cell. It may also be necessary to remove the SDM from the DCE cell if there is a DCE error condition that cannot be fixed by other means.

To perform this procedure, you must know the password to use the cell_admin DCE account (or principal) that is automatically created with the DCE cell. The cell_admin DCE account has the required privileges to make changes to a DCE cell.

Alternatively, the cell_admin principal can also create a subadministrator account with limited privileges for the sole purpose of maintaining SDMs in the DCE cell. If you choose to create a subadministrator account, the following privileges are required:

- quotas to create principals
- read and insert permissions on the / .:/hosts cell directory service (CDS) directory

Before performing this procedure, determine if you are going to remove the SDM from the DCE cell using full removal (one step) or local removal (two steps). Nortel recommends that you use full removal to perform this procedure because it is simpler, and less prone to errors.

Distributed Computing Environment
Removing an SDM from a DCE cell (continued)

To remove the SDM from a DCE cell using the full removal procedure, you must be able to

- log on as the root user to the SDM that is being removed
- provide a DCE administrator account principal name (cell_admin or an equivalent principal), and its password, and all other required parameters when running the “rmdce” program

If, for security reasons, the user removing the SDM from the DCE cell cannot obtain both the root password of the SDM, and the cell_admin password, use local DCE removal. To use local removal, you must be able to

- log in as the root user to the SDM that is being removed
- run the “rmdce -o local” command
- log in as the DCE administrator to a machine (another SDM, a Motorola PowerStack or an IBM RS-6000 workstation) other than the SDM being removed. This machine is an active node in the DCE cell, and it must be running the AIX version of DCE. It is not necessary to log in as the root user.

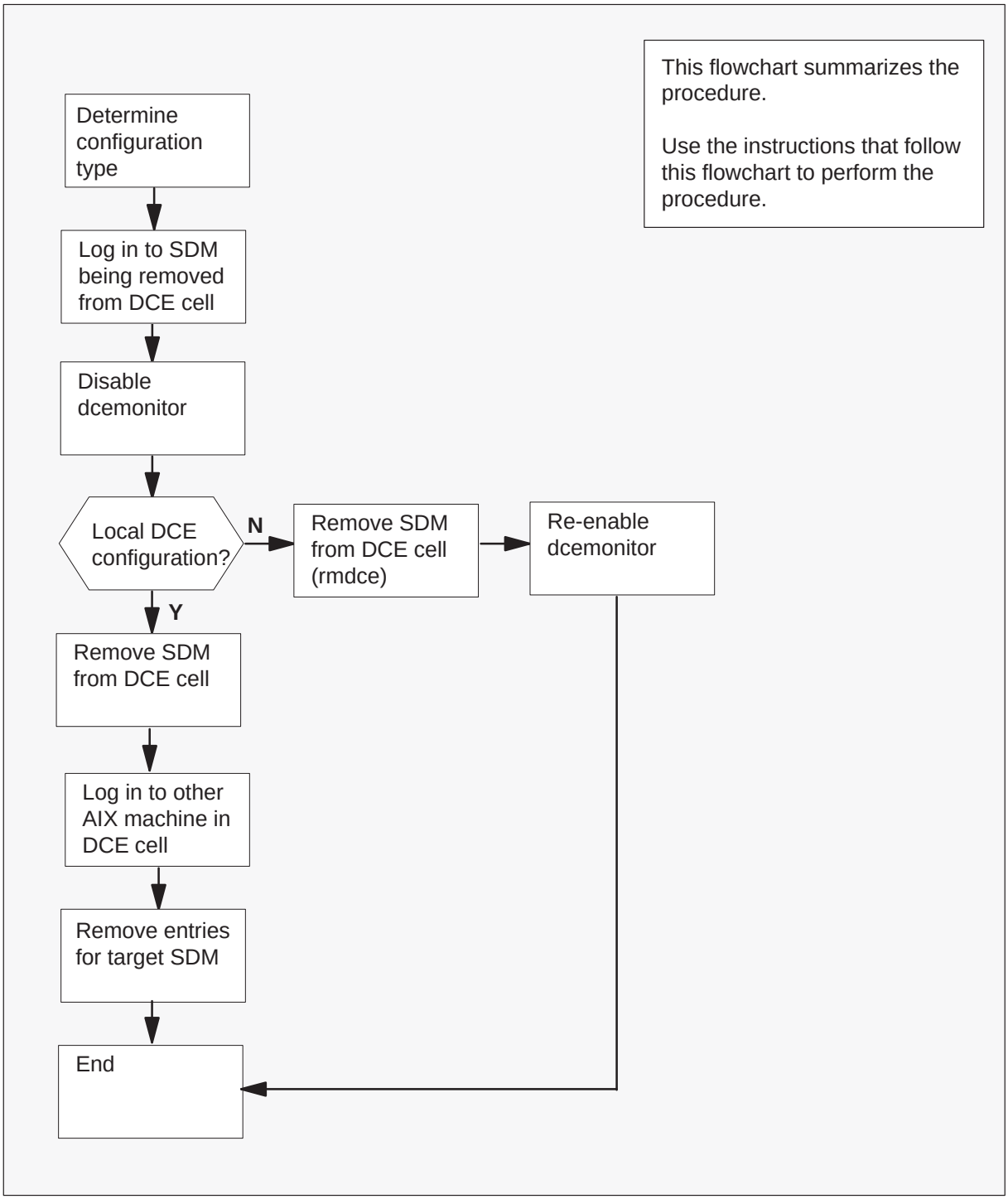
  — If you are performing this step on an SDM that is already configured in the DCE cell, the “rmdce” command is not accessible to the maintenance (maint) user. You must, therefore, log in as the root user to that SDM. If you cannot log in as root, have the root user add a special user on that SDM that the DCE administrator can use to perform the local removal procedure. Refer to the procedure ”Adding or removing a maintenance user” on page 6-10 in this document. Ensure that this special user’s initial program field is set to /bin/csh or some other UNIX shell other than /sdmtools/bin/cm_screener.
- run the “rmdce -o admin” command providing a DCE administrator account principal name and password, and the hostname and IP address of the SDM being pre-configured. The “rmdce” program is only available on machines that run the AIX version of DCE.

Action

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

Distributed Computing Environment
Removing an SDM from a DCE cell (continued)

Summary of Removing an SDM from a DCE cell



Distributed Computing Environment
Removing an SDM from a DCE cell (continued)

Removing an SDM from a DCE cell

At the SDM

1 Determine which method you wish to use to remove the SDM from the DCE cell.

If you are using	Do
full DCE removal	step 2
local DCE removal	step 8

2 Log in as the root user to the SDM that is being removed from the DCE cell.

3 Disable the DCE monitor program to prevent it from interfering with this procedure. Refer to the procedure ”Distributed Computing Environment – Disabling and enabling dcemonitor” on page 6-136 in the “SDM system administration procedures” chapter of this document. When you have disabled dcemonitor, continue this procedure.

4 Remove the SDM from the DCE cell by typing

 # rmdce -a administrator_principal all_cl
and pressing the Enter key.

where

administrator_principal is the DCE administrator’s principal name

Distributed Computing Environment
Removing an SDM from a DCE cell (continued)

5 At the prompt, enter the password for the DCE account cell_admin by typing

 # password
and pressing the Enter key.

where

password is the password for the DCE account cell_admin

Response:

```
Unconfiguring DTS Clerk (dts_cl)...
DTS Clerk (dts_cl) unconfigured successfully

Unconfiguring CDS Clerk (cds_cl)...
CDS Clerk (cds_cl) unconfigured successfully

Unconfiguring Security Client (sec_cl)...
Security Client (sec_cl) unconfigured successfully

Unconfiguring RPC Endpoint Mapper (rpc)...
RPC Endpoint Mapper (rpc) unconfigured successfully

Current state of DCE configuration:
No components are configured
#
```

6 When you see the message “No components are configured”, the SDM has been removed from the DCE cell.

7 Enable the DCE monitor program that was disabled in step 3. Refer to the procedure ”Distributed Computing Environment – Disabling and enabling dcemonitor” on page 6-136 in the “SDM system administration procedures” chapter of this document. When you have enabled dcemonitor, go to step 16.

8 Log in as the root user to the SDM that is being removed from the DCE cell.

9 Disable the DCE monitor program to prevent it from interfering with this procedure. Refer to the procedure ”Distributed Computing Environment – Disabling and enabling dcemonitor” on page 6-136 in the “SDM system administration procedures” chapter of this document. When you have disabled dcemonitor, continue this procedure.

Distributed Computing Environment
Removing an SDM from a DCE cell (continued)

10 Remove the local DCE components from the SDM by typing

 # rmdce -o local all_cl
and pressing the Enter key.

Response:

```
Unconfiguring DTS Clerk (dts_cl)...
DTS Clerk (dts_cl) unconfigured successfully on the
  local machine

Unconfiguring CDS Clerk (cds_cl)...
CDS Clerk (cds_cl) unconfigured successfully on the
  local machine

Unconfiguring Security Client (sec_cl)...
Security Client (sec_cl) unconfigured successfully on the
  local machine

Unconfiguring RPC Endpoint Mapper (rpc)...
RPC Endpoint Mapper (rpc) unconfigured successfully on the
  local machine

Current state of DCE configuration:
No components are configured
#
```

11 When you see the message “No components are configured”, the SDM has been removed from the DCE cell.

12 Enable the DCE monitor program that was disabled in step 9. Refer to the procedure ”Distributed Computing Environment – Disabling and enabling dcemonitor” on page 6-136 in the “SDM system administration procedures” chapter of this document. When you have enabled dcemonitor, continue this procedure.

13 Log in to any machine (another SDM, a Motorola PowerStack or an IBM RS-6000 workstation) other than the SDM being removed. This machine is an active node in the DCE cell, and it is running the AIX version of DCE. It is not necessary to log in as the root user.

Distributed Computing Environment Removing an SDM from a DCE cell (end)

14 Remove the entries for the SDM you are removing from the DCE servers by typing

 # rmdce -o admin -h machine name -a cell_admin all_cl
and pressing the Enter key

where

machine name is the name of the SDM you are removing

15 At the prompt, enter the password for the DCE account cell_admin by typing

>password
and pressing the Enter key.

where

password is the password for the DCE account cell_admin

Note: If the DCE host has a distributed file system (DFS) client (dfs_cl) configured, the DFS client cannot be used until the host has been reconfigured as a DCE client.

Example response:

```
Password must be changed!
Unconfiguring DTS Clerk (dts_cl) for
  DCE host bnode64 ...
DTS Clerk (dts_cl) unconfigured successfully for
  DCE host bnode64

Unconfiguring CDS Clerk (cds_cl) for
  DCE host bnode64 ...
CDS Clerk (cds_cl) unconfigured successfully for
  DCE host bnode64

Unconfiguring Security Client (sec_cl) for
  DCE host bnode64 ...
Security Client (sec_cl) unconfigured successfully for
  DCE host bnode64
```

16 You have completed this procedure.

Distributed Computing Environment Creating a DCE user

Application

ATTENTION

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

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

Invoking the create_dce_user command creates a new DCE user and makes the user a member of a specified group. Use groups for access control purposes to categorize users with similar job functions. You only need a DCE account to run an SDM GUI program. There may be some exceptions for specific SDM applications. For any exceptions, refer to the documentation *OSF DCE Command Reference*, provided with the application.

CAUTION

Risk of failure of SDM SFT and ETA applications

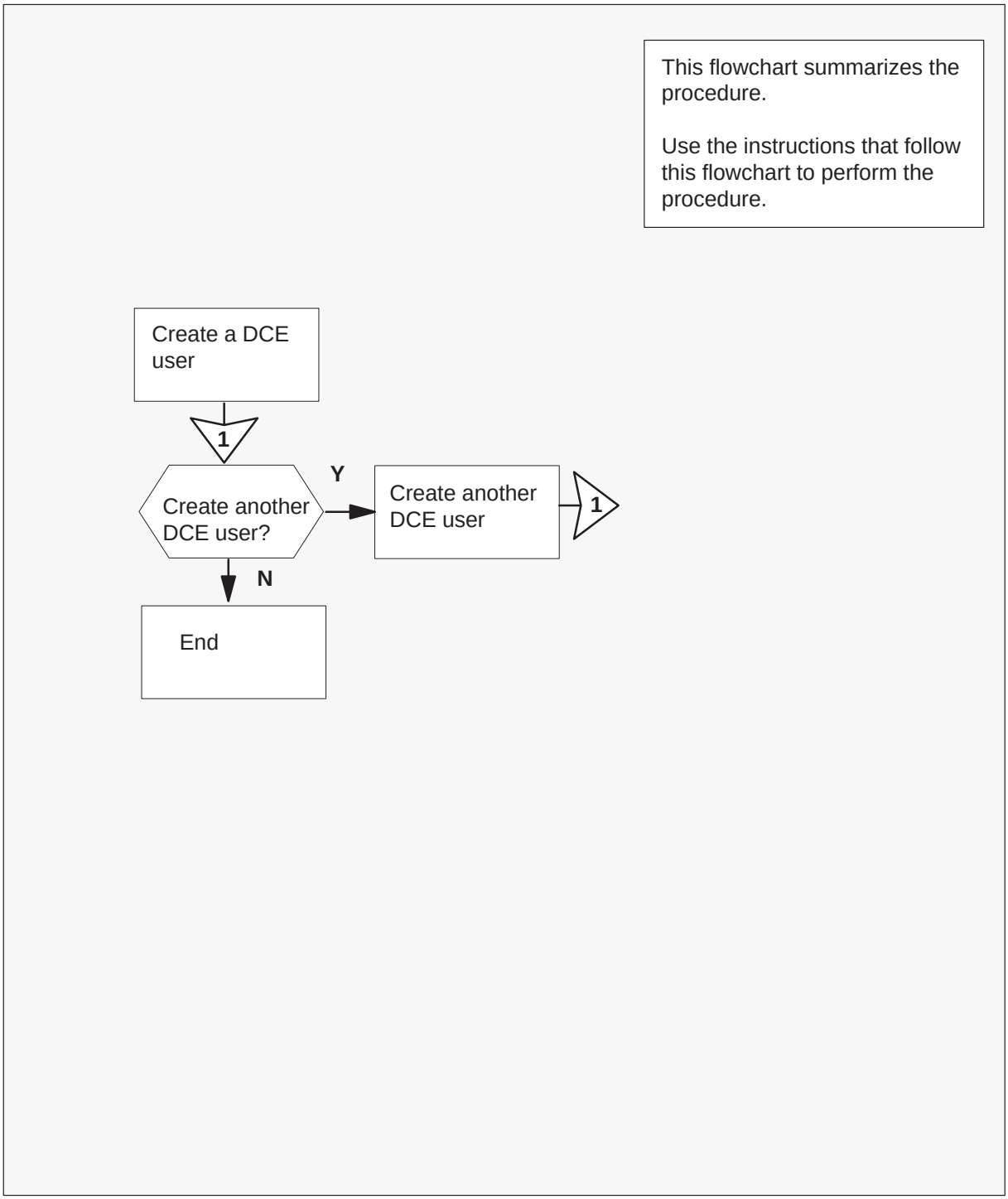
Do not use this procedure unless you have installed SDM software version SDMNM009 *x* MNCL 9.3 (1 of 1), or later, on your client workstation. (*x* is "V" for a software verification load or "R" for a software release load.)

Action

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

Distributed Computing Environment
Creating a DCE user (continued)

Summary of Creating a DCE user



Distributed Computing Environment
Creating a DCE user (continued)

Creating a DCE user

At the SDM client workstation

1 Create a DCE user by typing

>/sdm/bin/create_dce_user

2 Enter the user ID at the prompt by typing

>DCE administrator user ID[cell_admin]: *UserID*
and pressing the Enter key.

where

UserID is the user ID of the DCE administrator
Note: **cell_admin** is the default value. If you do not specify a user Id, the system enters the default value.

3 Enter the DCE administrator password at the prompt by typing

>DCE administrator password:*password*
and pressing the Enter key.

where

password is the password for the administrator account that you are using
Note: The password is not echoed on the screen.

4 Enter the name of the DCE user by typing

>New DCE user ID:*userID*
and pressing the Enter key.

where

userID is the user ID of the new DCE user
Response:

```
Enter the full name of the person associated with this
user ID:
```

5 Enter the full name of the person associated with the user ID by typing

>*fullname*
and pressing the Enter key.

where

fullname is the full name of the person associated with the user ID

6 Enter the user group by typing

>User group [sdm–users]:*sdm–maint*
and pressing the Enter key.

Distributed Computing Environment
Creating a DCE user (end)

where

sdm–maint is the user group of the DCE user

Example response:

```
The "sdm–maint" group doesn't exist! it will be created.
```

Note: **sdm–users** is the default value. If no user group is specified, the system enters the default value.

7 Enter the user password by typing

>User password:*password*
and pressing the Enter key.

where

password is the password for the DCE user ID

Note: The password is not echoed on the screen.

8 Re-enter the user password by typing

>Re–enter user password:*password*
and pressing the Enter key.

Example response:

```
The new DCE user ID "joe" has been created.
```

9 Determine if you want to create another DCE user.

If you	Do
want to create another user	step 1
do not want to create another user	step 11

10 Contact the personnel responsible for the next level of support.

11 You have completed this procedure.

Distributed Computing Environment Updating DCE principal names

Application

ATTENTION

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

Determine if a system administrator has already defined the DCE principal names using the create_dce_user command from a software load before SDMNM009 *x* MNCL 9.3. If that has happened, you must update the DCE principal names in each cell. Use this procedure to update all DCE principal names in each DCE cell.

CAUTION

Risk of failure of SDM SFT and ETA applications

Use this procedure only if at least one of the nodes in the DCE cell has been upgraded to SDM software version SDMNM009 *x* MNCL 9.3 (1 of 1), or later. (*x* is "V" for a software verification load or "R" for a software release load.)

The update_access_perm command updates all DCE principal names for users in a cell. This command allows all users in a DCE cell to use all SDMN0009 software without access restrictions.

Note: You need only run the update_access_perm command once to upgrade all DCE principal names in a DCE cell. Thereafter, if an administrator creates a non-compliant principal name by using a create_dce_user script that is earlier than SDMNM009.3, you can correct the error by using this procedure again.

Distributed Computing Environment
Updating DCE principal names (continued)

DCE principal names with definition errors

Problems occur with DCE principal names when all of the following conditions are present within a single DCE cell:

- one or more SDMs are running an SDMN0008 load
- one or more SDMs are running the SDMNM009.1 load
- SDMN0008 DCE principals have been defined
- the SDMNM009.3 MNCL has not been installed and deployed on an SDM and a client workstation
- Enhanced Terminal Access or Secure File Transfer are being used

DCE principal names and ETA

Enhanced Terminal Access (ETA) fails if you use a principal name that was defined with the SDMN0009 create_dce_user command to connect ETA to an SDM running an SDMN0008 load. For a principal name defined with the SDMN0008 create_dce_user command, no problem occurs with either the SDMN0008 or SDMN0009 versions of ETA.

Between the installation of the first SDMNM009.1 load on an SDM and the installation of the SDMNM009.3 MNCL, do the following:

- Use SDMN0008 DCE principal names when using ETA to communicate with an SDMN0008-equipped SDM. Do not use an SDMN0009-defined DCE principal name.

DCE principal names and SFT

Secure File Transfer (SFT) fails if a principal name was defined with the SDMN0008 create_dce_user command. No such problem occurs when using an SDMN0009 principal name.

Between the installation of the first SDMNM009.1 load on an SDM and the installation of the SDMNM009.3 MNCL, do the following:

- Use SDMN0009-defined DCE principal names to run SFT. Do not use an SDMN0008-defined DCE principal name.

Distributed Computing Environment
Updating DCE principal names (continued)

Action

The following points summarize the procedure for updating DCE principal names:

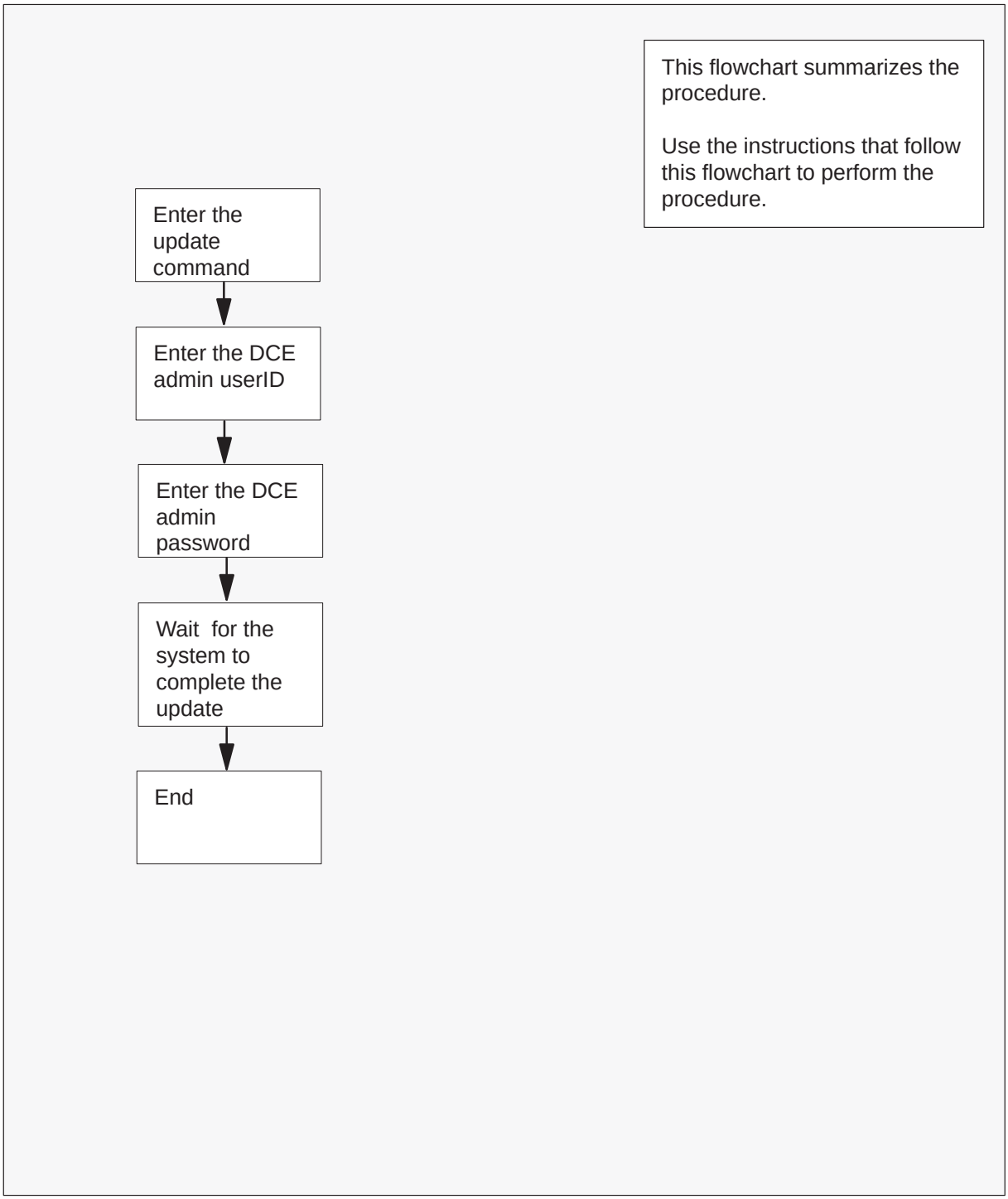
- After you install SDMNM009.3 software on an SDM and the client software on a client workstation, update DCE principal names using the update_access_perm command. After you run the script on at least one workstation in a cell, the system updates all SDMN0008 and SDMN0009 principal names in the cell.
- As client workstations are updated with SDMNM009.3, you can use the create_dce_user command on the updated nodes to define new DCE principal names.
- The create_dce_user command replaces the add_dce_user command that was available before SDMNM008.1 MNCL. After you use the update_access_perm command to update the DCE principal names, do not use either of the add_dce_user or create_dce_user commands on nodes running loads prior to SDMNM009.3.

Note: For information about the installation and use of the SDMNM009.3 MNCL, see the SDMNM009 *SuperNode Data Manager FT Platform & Applications Maintenance Release Notes*.

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

Distributed Computing Environment
Updating DCE principal names (continued)

Summary of Updating DCE principal names



Distributed Computing Environment Updating DCE principal names (end)

Updating DCE principal names

At the SDM client workstation

1 Enter the command to update all DCE principal names in the cell by typing

>/sdm/bin/update_access_perm
and pressing the Enter key.

2 Enter the userID at the prompt by typing

>DCE administrator user ID[cell_admin]: *UserID*
and pressing the Enter key.

where

UserID — is the userID of the DCE administrator

Note: **cell_admin** is the default value. If you do not specify a userID, the system enters the default value.

3 Enter the DCE administrator password at the prompt by typing

>DCE administrator password:*password*
and pressing the Enter key.

where

password — is the password for the administrator account that you are using

Note: The password is not echoed on the screen.

4 Wait for the system to update the DCE principal names.

The system displays the following response to indicate that the process is complete:

```
DCE principal access permission upgrade is completed.
```

Note: If the system does not respond or displays an error message, contact the personnel responsible for the next level of support.

5 You have completed this procedure.

Distributed Computing Environment Changing a DCE user password

Application

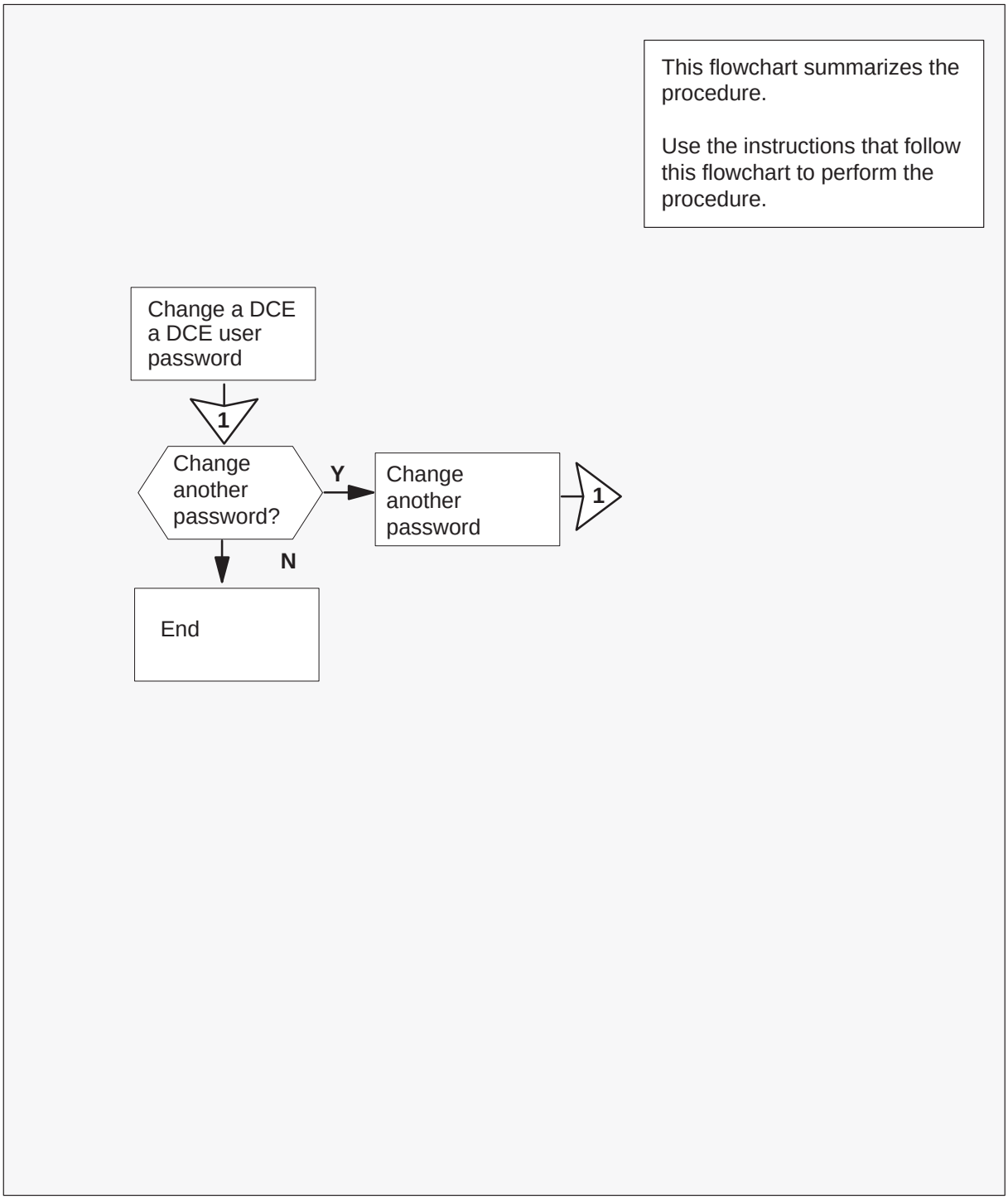
Use this procedure to change a DCE user password.

Action

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

Distributed Computing Environment
Changing a DCE user password (continued)

Summary of Changing a DCE user password



Distributed Computing Environment
Changing a DCE user password (continued)

Changing a DCE user password

At the SDM client workstation

1 Change a DCE user password by typing

>/sdm/bin/change_dce_password

Response:

```
DCE user ID:
```

2 Enter the user ID of the user for whom you are changing the password by typing

>userID
and pressing the Enter key.

where

userID	is the user ID of the user for whom you are changing the password

Response:

```
Old password:
```

3 Enter the old password by typing

>password
and pressing the Enter key.

where

password	is the old password of the user for whom you are changing the password

Note: The password is not echoed on the screen.

Response:

```
New password:
```

4 Enter the new password by typing

>password
and pressing the Enter key.

where

password	is the new password of the user

Response:

```
Re-enter password:
```

Distributed Computing Environment Changing a DCE user password (end)

Note: The password is not echoed on the screen.

5 Re-enter the user password by typing

>password
and pressing the Enter key.

Example response:

```
The password for ”joe” has been changed.
```

6 Determine if you want to change another DCE user password.

If you	Do
want to change another password	step 1
do not want to change another password	step 7

7 You have completed this procedure.

Distributed Computing Environment Deleting a DCE user

Application

ATTENTION

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

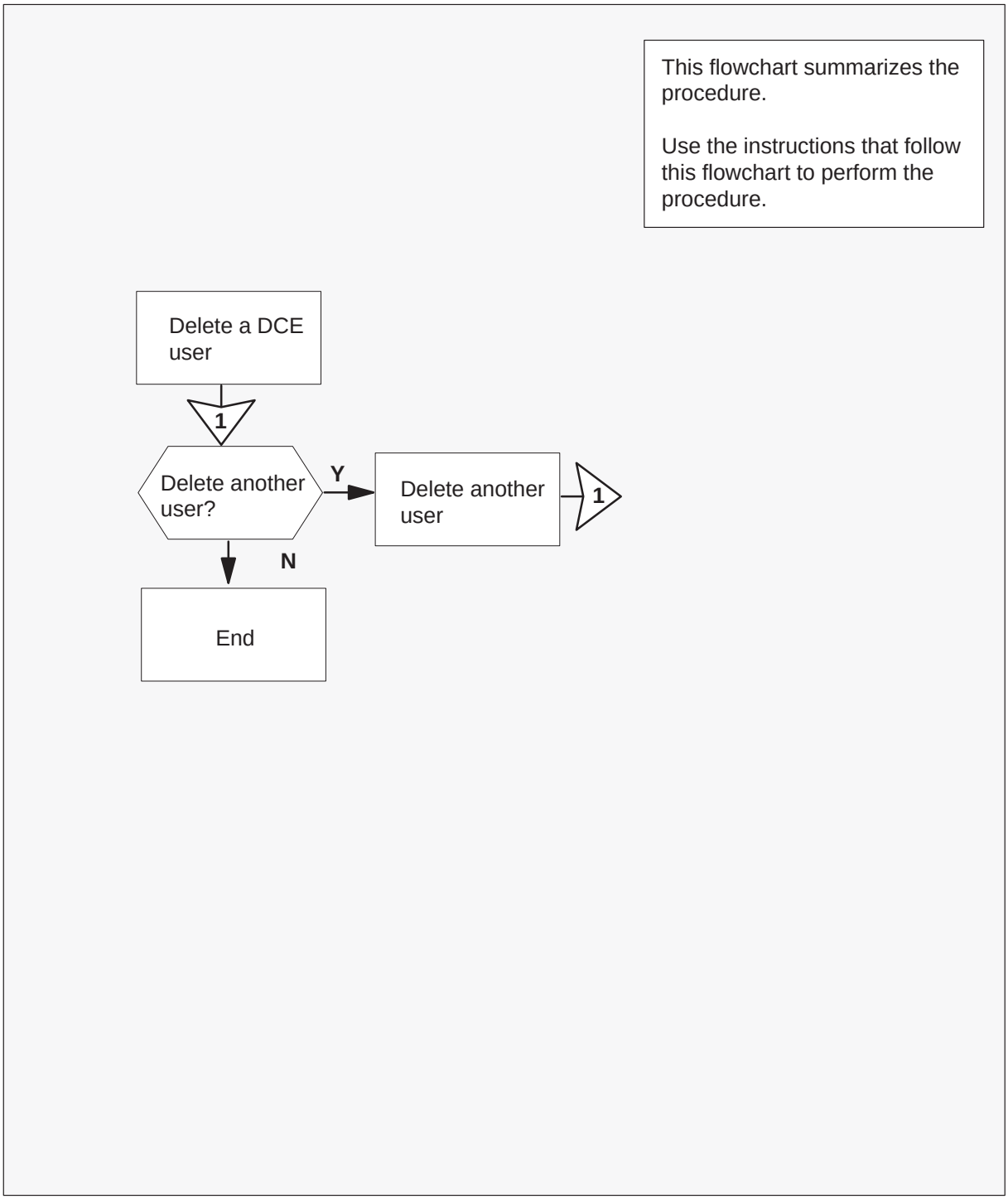
Use this procedure to delete a DCE user.

Action

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

Distributed Computing Environment
Deleting a DCE user (continued)

Summary of Deleting a DCE user



Distributed Computing Environment
Deleting a DCE user (end)

Deleting a DCE user

At the SDM client workstation

1 Delete a DCE user by typing

>/sdm/bin/delete_dce_user

Response:

```
DCE administrator user ID [cell_admin]:
```

2 Enter the user ID at the prompt by typing

>userID
and pressing the Enter key.

where

userID is the user ID of the DCE administrator

Note: **cell_admin** is the default value. If you do not specify a user Id, the system enters the default value.

Response:

```
DCE user ID to be deleted:
```

3 Enter the DCE user ID to be deleted by typing

>userID
and pressing the Enter key.

where

userID is the user ID of the user to be deleted

Example response:

```
The DCE user ID ”joe” has been deleted.
```

4 Determine if you want to delete another DCE user.

If you	Do
want to delete another password	step 1
do not want to delete another password	step 5

5 You have completed this procedure.

Distributed Computing Environment Viewing the dcemonitor status file

Application

ATTENTION

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

The SDM detects common DCE failure conditions, reports them to the SDM node control facility, and automatically takes the appropriate recovery action to clear the problem. The status of DCE, reported by dcemonitor, is displayed under the LAN connectivity menu level of the SDM remote maintenance interface (RMI).

This automatic DCE maintenance is performed by the dcemonitor script. The dcemonitor sript is a Tool Command Language (TCL) script that is continuously executed by a DCE control program (dcecp) running in the SDM platform. Dcemonitor dumps its current status, problems found, and the recovery action in a file that is regularly rewritten. By viewing the contents of the status file, you can determine what caused the DCE state change.

This procedure assists you when dcemonitor cannot fix the problem, and manual intervention is necessary. Problems requiring manual intervention include:

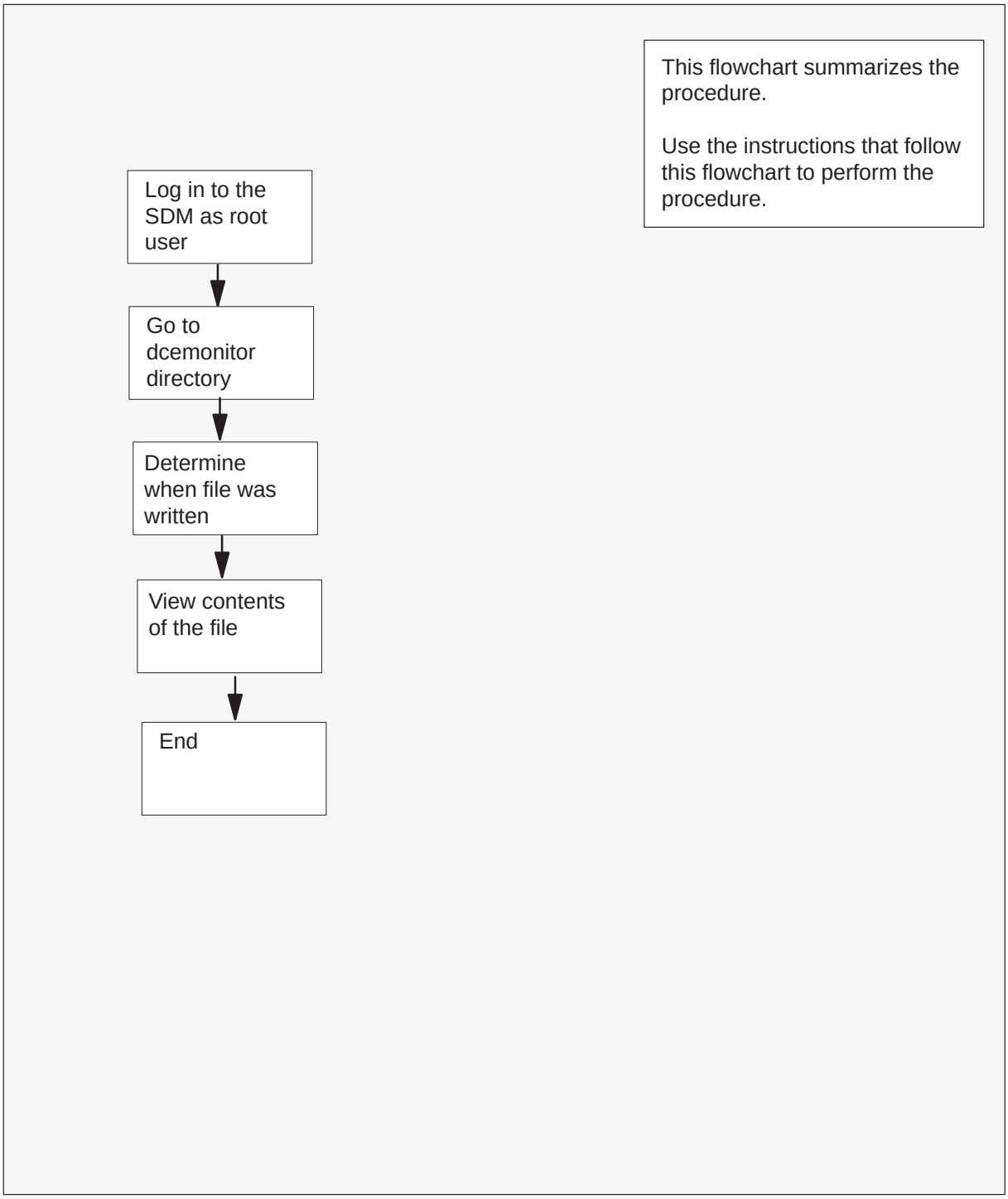
- the server identifies a mismatch resulting from a change to the switch Common Language Location Identifier (CLLI)
- the SDM hostname is changed
- the SDM has been restored from a backup tape

Action

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

Distributed Computing Environment
Viewing the dcemonitor status file (continued)

Summary of Viewing the dcemonitor status file



Distributed Computing Environment
Viewing the dcemonitor status file (end)

Viewing the dcemonitor status file

At the local VT100 console or remote workstation

1 Log in to the SDM as the root user

2 Go to the dcemonitor data directory by typing

 # cd /data/mtce/dce
and pressing the Enter key.

3 Determine when the file was last written by typing

 # ls -l dce_mon_status
and pressing the Enter key.

4 View the contents of the status file by typing

 # cat dce_mon_status
and pressing the Enter key.

5 You have completed this procedure.

Distributed Computing Environment Disabling and enabling dcemonitor

Application

ATTENTION

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

When dcemonitor cannot solve a service-affecting DCE problem, it attempts to solve the problem by killing the DCE daemons using /etc/dce.clean, and restarting them using /etc/rc.dce. If this does not solve the problem, dcemonitor waits 3 min, and repeats these operations indefinitely.

The "DCE Monitor present action:" line in the dce_mon_status file will be "restart" if dcemonitor is doing recovery by restarts. If dcemonitor constantly kills DCE daemons, the DCE environment on the SDM becomes unstable. This can seriously impair your ability to fix the problem.

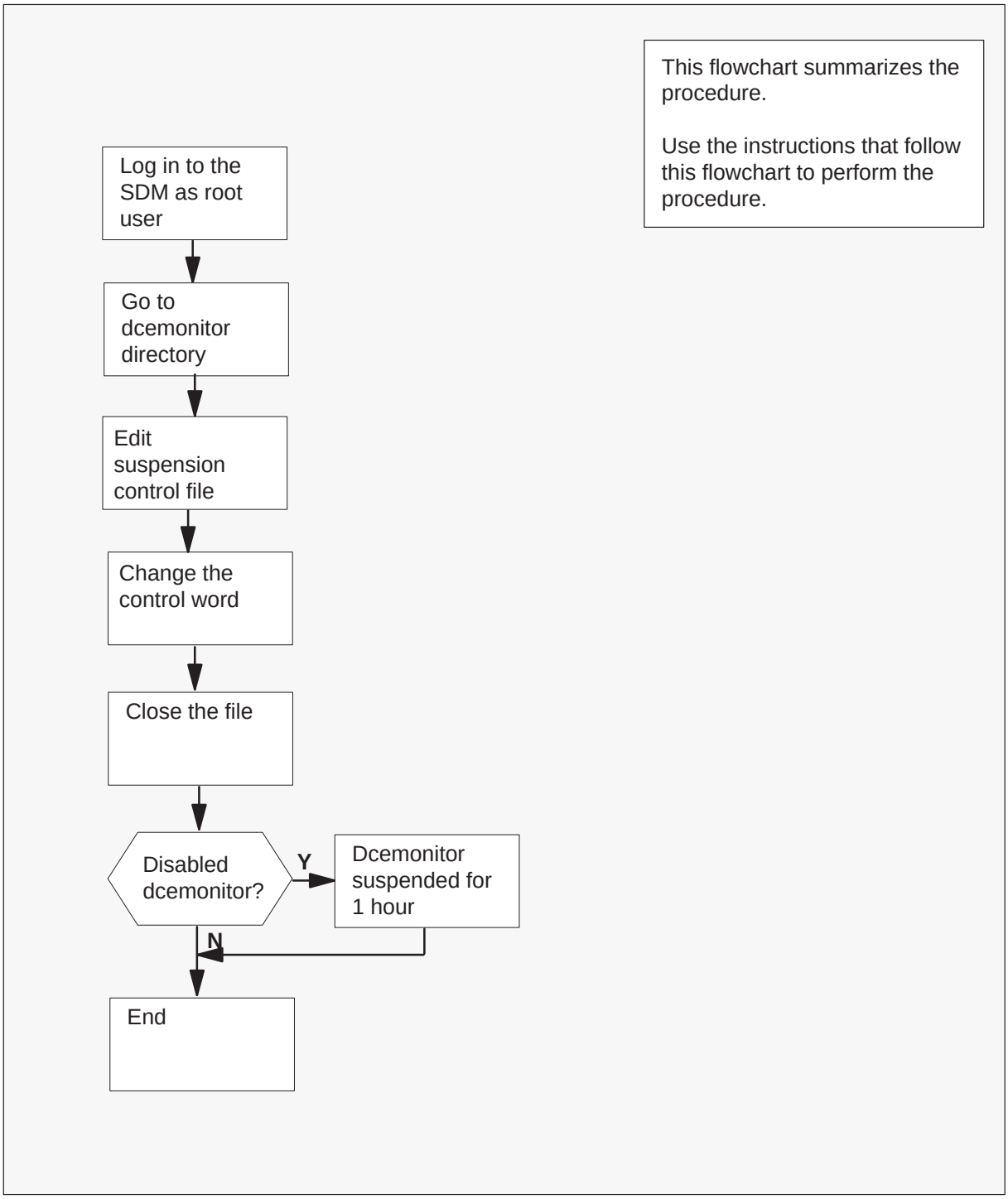
This procedure prevents dcemonitor from restarting and killing DCE daemons by suspending these operations for 1 hour. After 1 hour, dcemonitor resumes these activities.

Action

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

Distributed Computing Environment
Disabling and enabling dcemonitor (continued)

Summary of Disabling and enabling dcemonitor



Distributed Computing Environment
Disabling and enabling dcemonitor (continued)

Disabling and enabling dcemonitor

At the local VT100 console or remote workstation

1 Log in to the SDM as the root user

2 Go to the dcemonitor data directory by typing

 # cd /data/mtce/dce
and pressing the Enter key.

3 Edit the dcemonitor suspension control file by typing

 # vi dce_mon_suspend
and pressing the Enter key. This file contains one word.

4 Determine whether you wish to disable or enable dcemonitor

If you wish to	Do
disable dcemonitor	step 7
enable dcemonitor	step 5

5 Modify the control word by typing

>cw
The word suspend is replaced by “suspen$”.

6 Enable dcemonitor by typing the activation control word

>active

The $ from “suspen$” (step 5) remains.

Go to step 9.

7 Modify the control word by typing

>cw

The word active is replaced by “activ$”.

8 Disable dcemonitor by typing the suspension control word

>suspend

Distributed Computing Environment
Disabling and enabling dcemonitor (end)

9 Close the file by pressing the Esc key and typing

>: wq
and pressing the Enter key.

Dcemonitor stops killing and restarting DCE daemons for one hour.

Note: After an hour dcemonitor continues to restart and kill DCE daemons. The “active$” and “$” disappear when you press the Esc key.

10 You have completed this procedure.

Distributed Computing Environment Restricting ports to an SDM-defined range

Application

ATTENTION

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

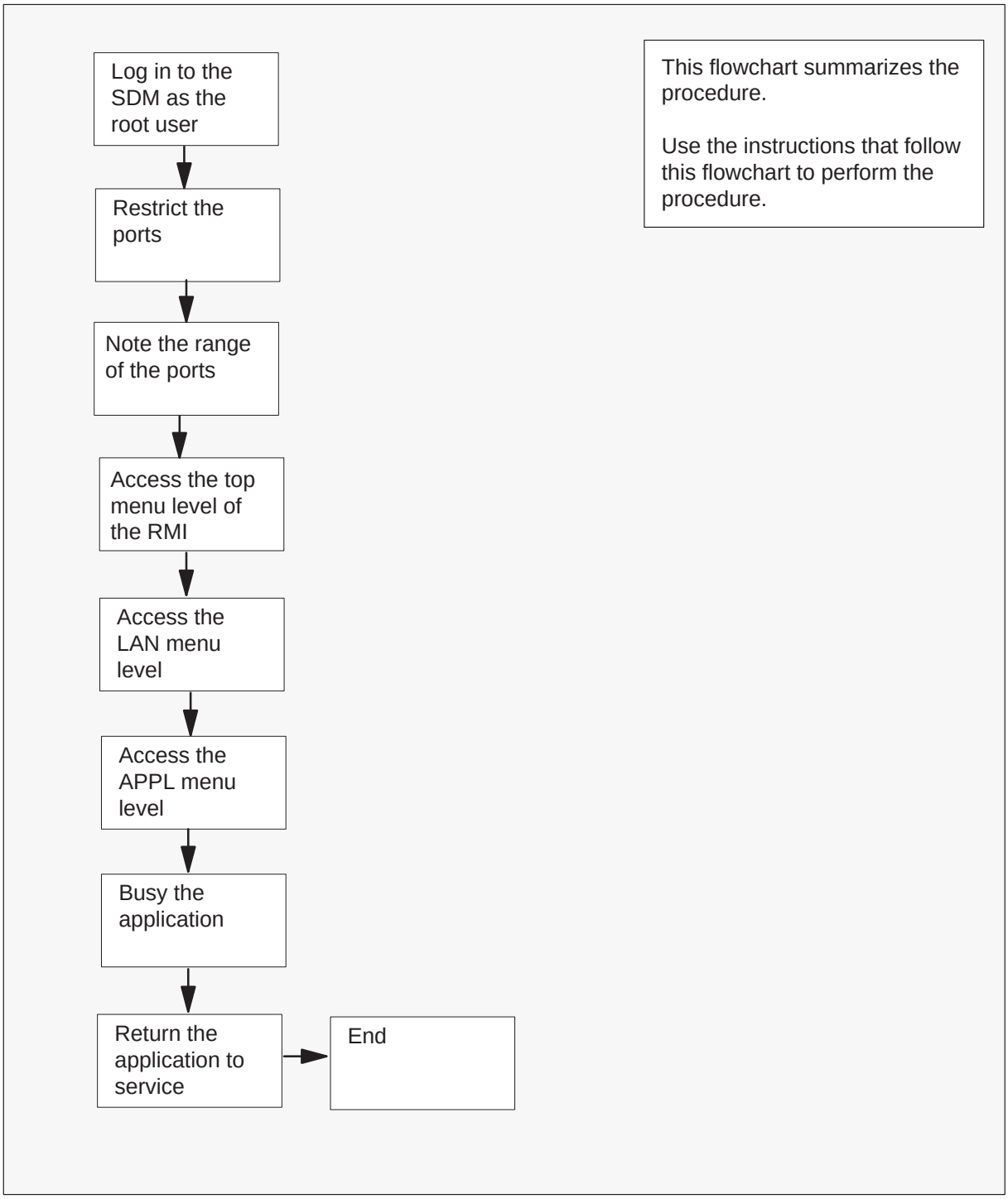
Use the following procedure to restrict the ports to a range that is predefined by the SDM software, and a range that will coexist with other SDM applications. You must have root user privileges to perform this procedure.

Action

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

Distributed Computing Environment
Restricting ports to an SDM-defined range (continued)

Summary of Restricting ports to an SDM-defined range



Distributed Computing Environment Restricting ports to an SDM-defined range (continued)

Restricting ports to an SDM-defined range

At the client workstation

1 Log in to the SDM as the root user

2 Restrict the ports to an SDM-defined range by typing

 # restrict_dce_ports system_defined
and pressing the Enter key.

Response:

```
The following port ranges have been configured
   TCP: 4500–4540   UDP: 4500–4540
```

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

4 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

5 Access the LAN menu level of the RMI by typing

>LAN
and pressing the Enter key.

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

Response:

```
DCE State:  InSv
```

7 Access the application (APPL) menu level of the RMI by typing

>APPL
and pressing the Enter key.

Example response:

```
# Package Description          Version     State
1  Table Access Service        8.0.19.0    InSv
2  OM Access Service           8.0.19.0    InSv
3  Log Delivery Service        8.0.19.0    InSv
4  Enhanced Terminal Access    8.0.19.0    InSv
5  Exception Reporting         8.0.19.0    InSv
```

Distributed Computing Environment
Restricting ports to an SDM-defined range (continued)

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

9 Manually busy the application software by typing

>BSY *n*
and pressing the Enter key.

where

n is the number under “#” of the application you wish to busy

Response:

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

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

10 Confirm the Busy command by typing

>Y
and pressing the Enter key.

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

12 Return the application to service by typing

>RTS *n*
and pressing the Enter key.

where

n is the number of the application (from step 9)

Distributed Computing Environment Restricting ports to an SDM-defined range (end)

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

13 You have completed this procedure.

Distributed Computing Environment Restricting ports to a specific range

Application

ATTENTION

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

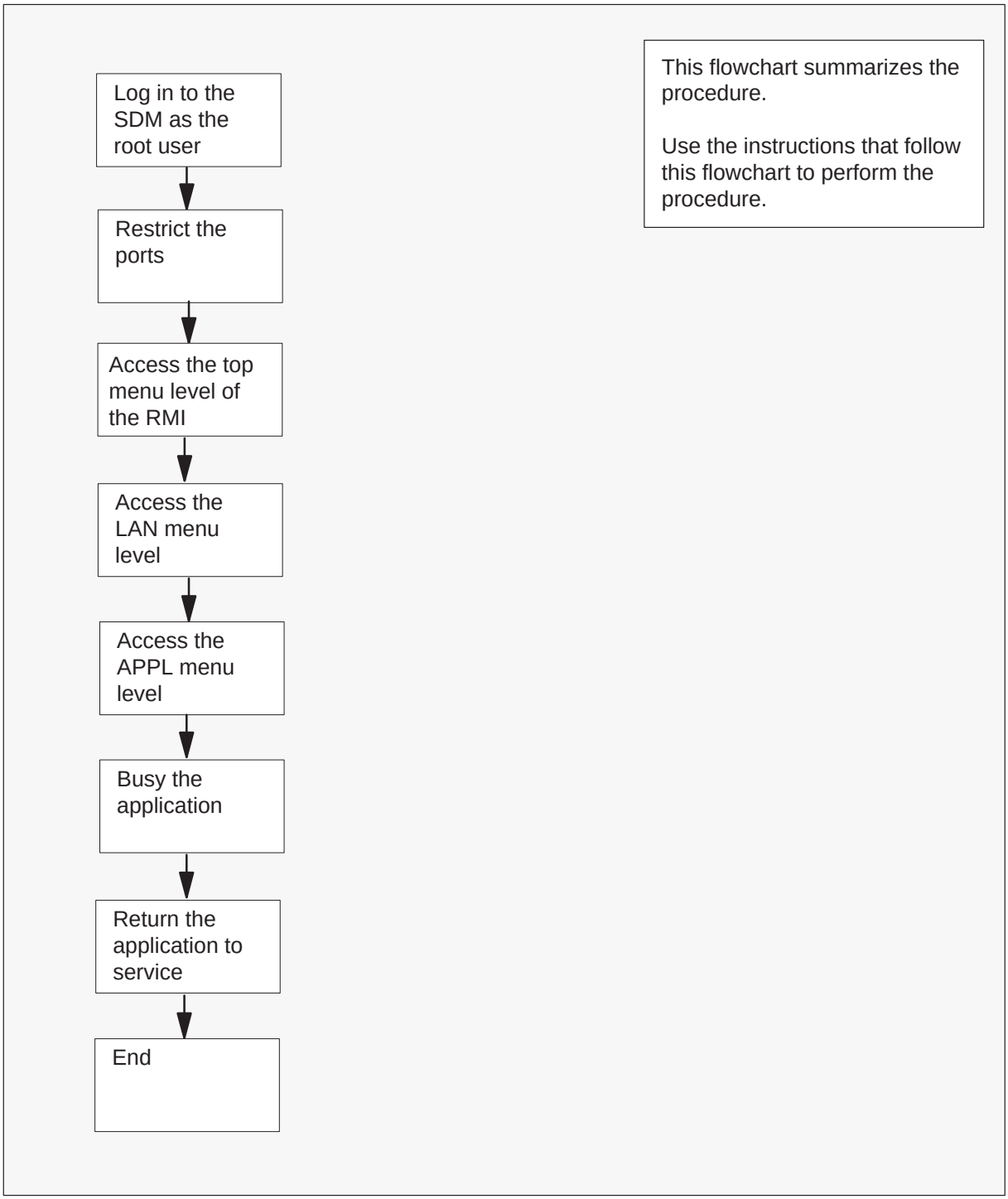
Use the following procedure to restrict the ports to a specific range. You must have root user privileges to perform this procedure.

Action

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

Distributed Computing Environment
Restricting ports to a specific range (continued)

Summary of Restricting ports to a specific range



Distributed Computing Environment
Restricting ports to a specific range (continued)

Restricting ports to specific range

At the client workstation

1 Log in to the SDM as the root user

2 Restrict the ports to an SDM-defined range by typing

 # restrict_dce_ports tcp *a:b* upd *c:d*
and pressing the Enter key.

where

a is the start of the range for TCP ports (must be greater than 1024
b is the end of the range for TCP ports (must be less than 32,000)
c is the start of the range for universal datagram protocol (UDP) ports (must be greater than 1024)
d is the end of the range for UDP ports (must be less than 32,000)

Example response:

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

3 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

4 Access the LAN menu level of the RMI by typing

>LAN
and pressing the Enter key.

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

Response:

```
DCE State:  InSv
```

6 Access the application (APPL) menu level of the RMI by typing

>APPL
and pressing the Enter key.

Example response:

```
# Package Description           Version     State
1  Table Access Service         8.0.19.0    InSv
2  OM Access Service            8.0.19.0    InSv
3  Log Delivery Service         8.0.19.0    InSv
4  Enhanced Terminal Access     8.0.19.0    InSv
5  Exception Reporting          8.0.19.0    InSv
```

Distributed Computing Environment Restricting ports to a specific range (continued)

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

8 Manually busy the application software by typing

>BSY *n*
and pressing the Enter key.

where

n is the number under "#" of the application you wish to busy

Response:

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

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

9 Confirm the Busy command by typing

>Y
and pressing the Enter key.

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

11 Return the application to service by typing

>RTS *n*
and pressing the Enter key.

where

n is the number of the application (from step 8)

Distributed Computing Environment Restricting ports to a specific range (end)

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

12 You have completed this procedure.

Distributed Computing Environment Removing port restrictions

Application

ATTENTION

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

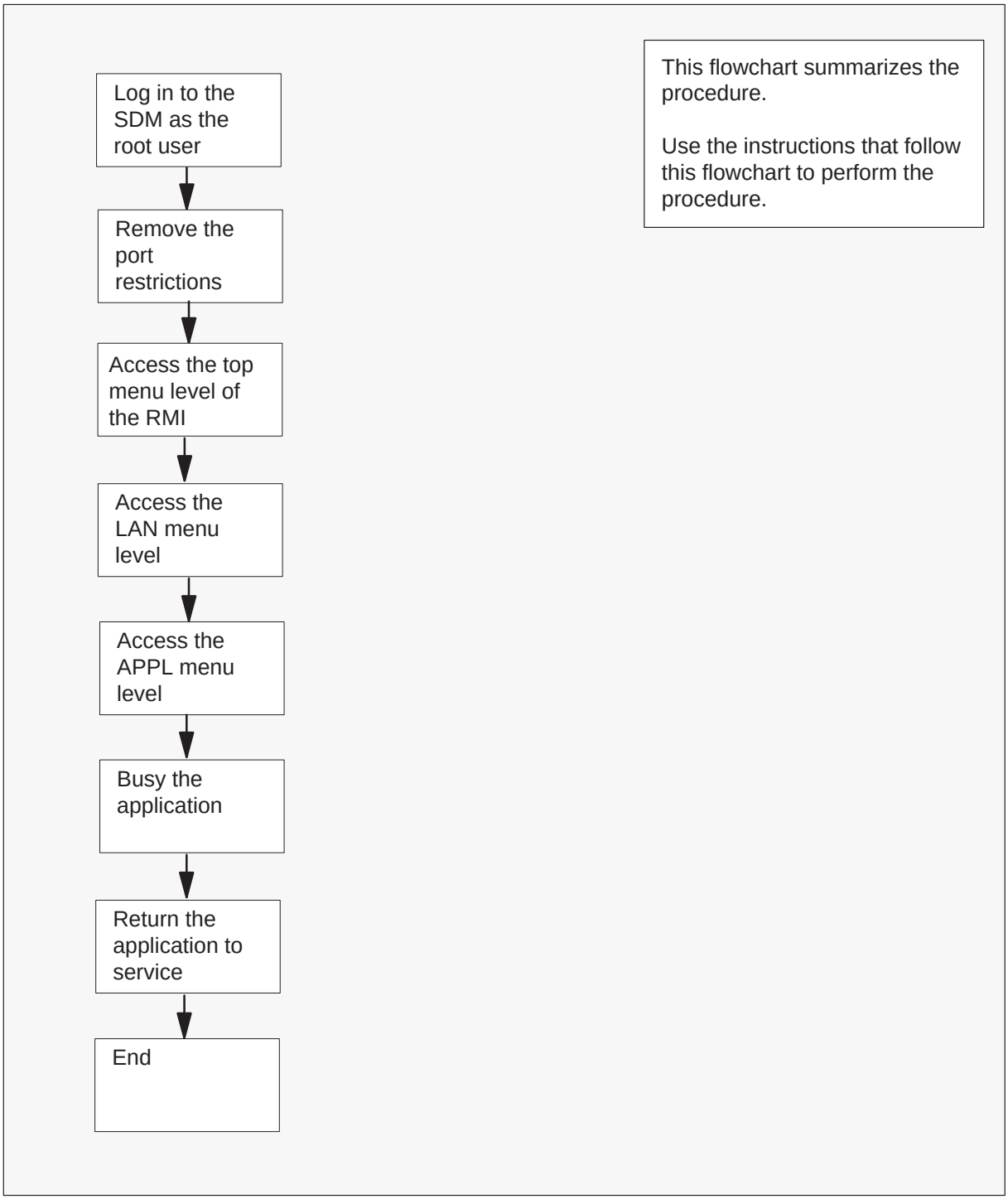
Use the following procedure to return the SDM to the system default values. DCE ports will be randomly assigned when you complete this procedure. You must have root user privileges to perform this procedure.

Action

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

Distributed Computing Environment
Removing port restrictions (continued)

Summary of Removing port restrictions



Distributed Computing Environment
Removing port restrictions (continued)

Removing port restrictions

At the client workstation

1 Log in to the SDM as the root user

2 Restrict the ports to an SDM-defined range by typing

 # restrict_dce_ports unrestricted
and pressing the Enter key.

Response:

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

3 Access the top menu level of the remote maintenance interface (RMI) by typing

 # sdmmtc
and pressing the Enter key.

4 Access the LAN menu level of the RMI by typing

>LAN
and pressing the Enter key.

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

Response:

```
DCE State:  InSv
```

6 Access the application (APPL) menu level of the RMI by typing

>APPL
and pressing the Enter key.

Example response:

```
# Package Description           Version     State
1  Table Access Service         8.0.19.0    InSv
2  OM Access Service            8.0.19.0    InSv
3  Log Delivery Service         8.0.19.0    InSv
4  Enhanced Terminal Access     8.0.19.0    InSv
5  Exception Reporting          8.0.19.0    InSv
```

Distributed Computing Environment
Removing port restrictions (continued)

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

8 Manually busy the application software by typing

>BSY *n*
and pressing the Enter key.

where

n is the number under “#” of the application you wish to busy

Response:

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

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

9 Confirm the Busy command by typing

>Y
and pressing the Enter key.

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

Response:

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

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

Response:

```
Application Bsy – Command submitted.
```

11 Return the application to service by typing

>RTS *n*
and pressing the Enter key.

where

n is the number of the application (from step 8)

Distributed Computing Environment Removing port restrictions (end)

Response:

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

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

Response:

```
Application RTS – Command submitted.
```

12 You have completed this procedure.

SDM hardware upgrade procedures

This chapter contains an SDM hardware upgrade procedure. The CPU controller module can be upgraded on the SDM as follows:

- NTRX50FK (128 MByte DRAM) to NTRX50FL (256 MByte DRAM)
- NTRX50FK (128 MByte DRAM) to NTRX50FM (512 MByte DRAM)
- NTRX50FL (256 MByte DRAM) to NTRX50FM (512 MByte DRAM)

Note: This procedure can also be used to change both CPU controller modules to a version with less DRAM, if required.

Each procedure contains the following:

- explanatory and context-setting information
- summary flowchart
- step-action instructions

Explanatory and context-setting information

The first page of each procedure contains the following headings:

- Application (why you would perform the procedure)
- Impact (how the procedure affects service)
- Action (how to use the flowchart and step-action instructions)

Summary flowchart

The flowchart is only a summary of the main actions, decision points, and possible paths you may take. Do not use the summary flowchart to perform the procedure. Instead, use it to preview what you will be doing and to prepare for it.

Step-action instructions

The step-action instructions tell you how to perform the procedure. The successful completion of a step may depend on previous steps; therefore, always perform the steps in the order specified.

The step-action instructions provide the command syntax and system information you use or see while performing the procedure. For help on DMS and SDM commands or output, see the "About this document" chapter at the beginning of this document.

Return key and Enter key

The carriage return key is identified in different ways (such as Enter, Return or Carriage Return) on various types of terminals. It is always used to enter commands and parameters into the system.

The procedures contained in this book and in other NTPs instruct you to press the Enter key after each step. If your terminal has a Return key, press the Return key instead. Do not press the Enter key located beside the numeric key pad.

Upgrading the CPU controller module NTRX50FL, NTRX50FM

Application

Use this procedure to perform the following CPU controller module upgrades:

- NTRX50FK (128 MByte DRAM) to NTRX50FL (256 MByte DRAM)
- NTRX50FK (128 MByte DRAM) to NTRX50FM (512 MByte DRAM)
- NTRX50FL (256 MByte DRAM) to NTRX50FM (512 MByte DRAM)

Note 1: This procedure can also be used to change a CPU controller module to a version with less DRAM, if required.

Note 2: The functionalities of the CPU controller modules are all identical. The only difference is increased memory.

Impact

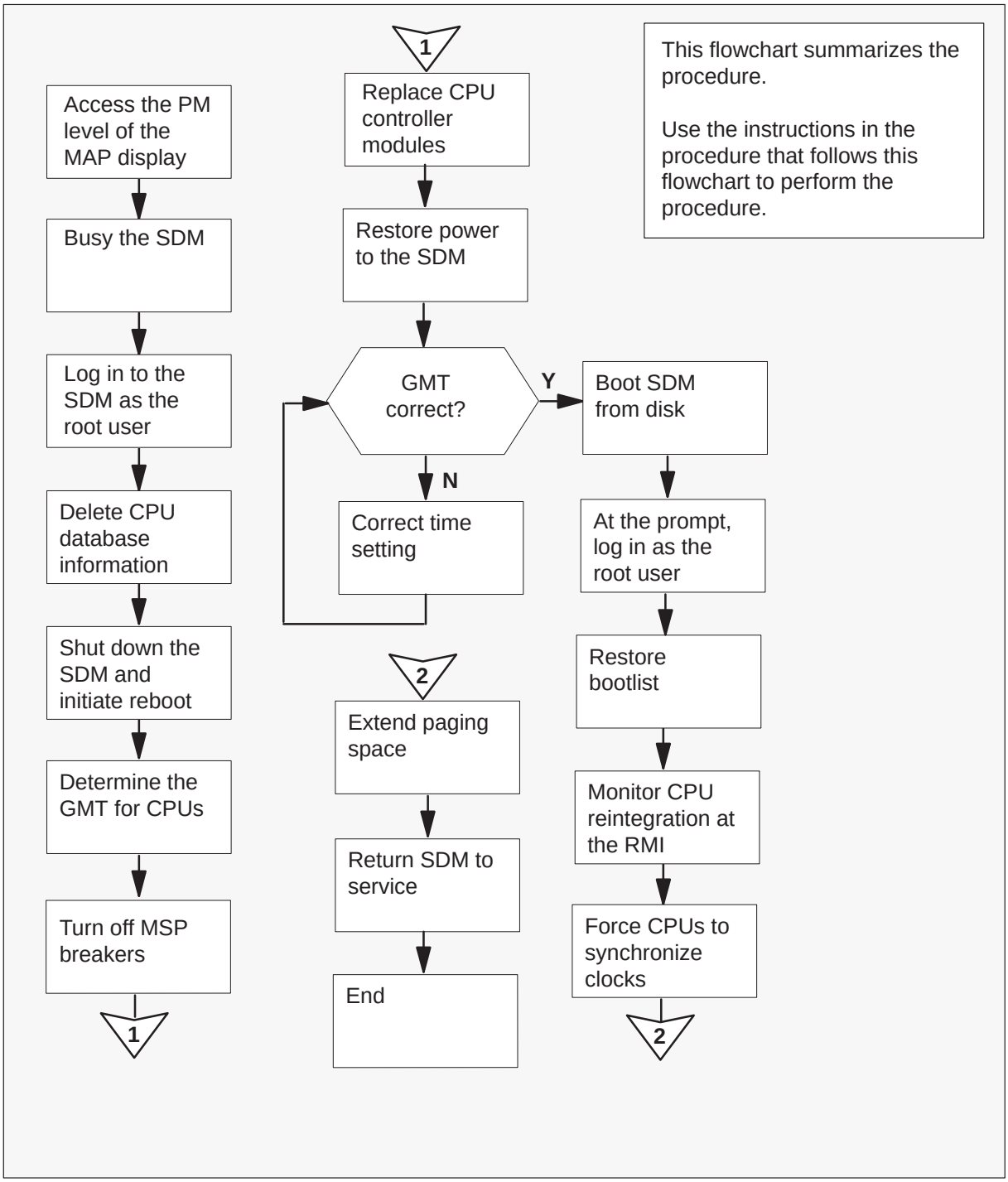
This procedure requires complete shutdown of the SDM and all its applications. Perform this procedure during a low-usage period to minimize service disruption.

Action

The following flowchart is only a summary of the procedure. To upgrade the CPU controller module, use the instructions in the step-action procedure that follows the flowchart.

Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

Summary of Upgrading the CPU controller module



Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

Upgrading the CPU controller module

1 Obtain a replacement CPU controller module. Ensure that the replacement module has the same product engineering code (PEC), including suffix, as the unit being removed. The PEC is written on the module's top locking lever.

At the MAP display

2 Access the SDM level of the MAP display by typing

>MAPCI; MTC; APPL;SDM
and pressing the Enter key.

Example response:

```
SDM   InSv
```

3 Manually busy the SDM by typing

>BSY
and pressing the Enter key.

Response:

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

4 Confirm the Bsy command by typing

>Y
and pressing the Enter key.

Response:

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

At the local or remote VT100 console

5 Log in to the SDM as the root user.

Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

6 Display information for the root volume group (rootvg) by typing

 # lsscsi -v rootvg
and pressing the Enter key.

Example response:

```
Volume Group: rootvg
Type        : fault tolerant
CMS state   : ft_full

Physical Volume Information:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
pv       domain  cms_state  module  vg      pps  (Mb)   free (Mb)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
hdisk0  0        online     I/O-0   rootvg  509  (2036) 209  (836)
hdisk3  1        online     I/O-2   rootvg  509  (2036) 209  (836)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Note: Only the relevant portion of the response is shown.

7 Note which hard disks (physical volumes) provide rootvg storage on the SDM, and record this information. (In the example shown in step 6, the hard disks are hdisk0 and hdisk3.)

8 Delete the SDM configuration database information for the CPU controller modules currently installed on the system by typing

 # ftcpuclean
and pressing the Enter key.

9 Shut down the SDM and initiate a reboot by typing

 # shutdown -Fr
and pressing the Enter key.

10 Interrupt the boot process when the “COLD start” message appears by pressing the Break key.

Example response:

```
FX-Bug>
```

Note: The “COLD start” message does not appear for about 2 min.

11 Determine the current Greenwich Mean Time (GMT) setting on the existing CPU controller modules by typing

FX-Bug>time
and pressing the Enter key.

Example response:

```
FRI APR 11 18:41:49:00
```

Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

12 Record the date and time response.

Note: If you are using a clock set to your local time to set the GMT on the new CPU controller modules, use the response in step 11 to calculate the number of hours that your local time differs from GMT.

At the MSP

13 Interrupt power to the SDM by turning both MSP breakers, located at the front of the MSP, off. The MSP breakers supply power to the SDM. Proceed according to the chassis structure of your system.

If your system contains	Do
a main chassis only	turn top two breakers off
contains a main and I/O expansion chassis	turn all four breakers off

At the front of the SDM

14

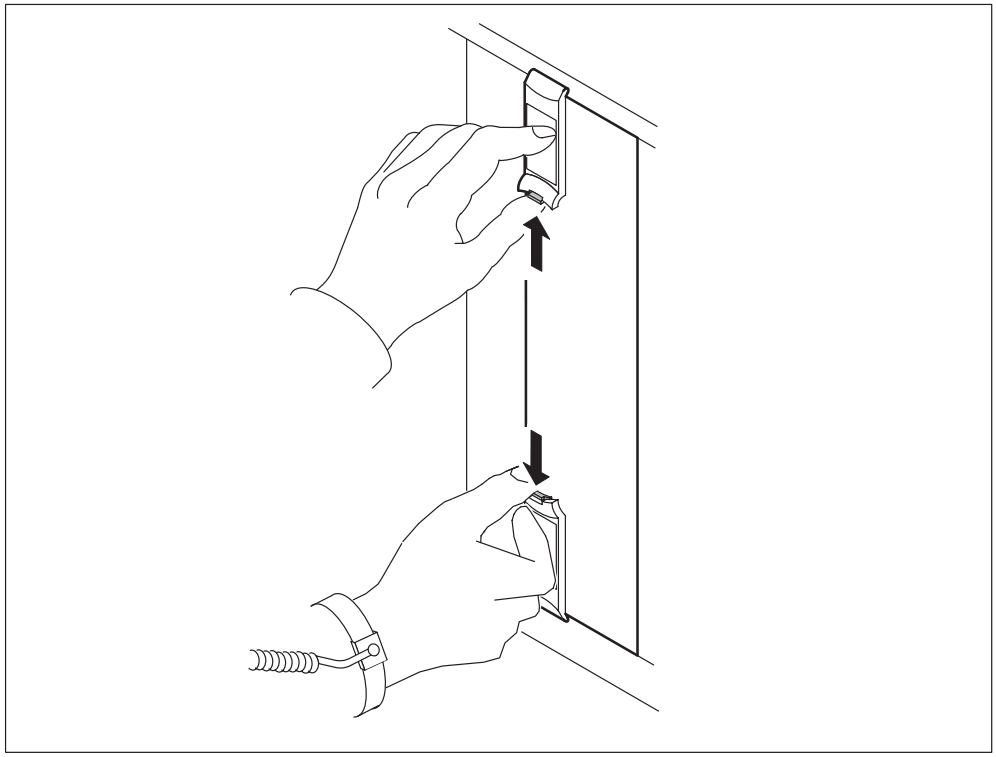
WARNING
Static electricity damage
Wear an electrostatic discharge (ESD) grounding wrist strap connected to the C28B cabinet when handling a module. This protects the module against damage caused by static electricity.

Undo the thumbscrews located on the top and the bottom of the CPU controller module.

Note: The thumbscrews are the captive type, and cannot be removed from the module.

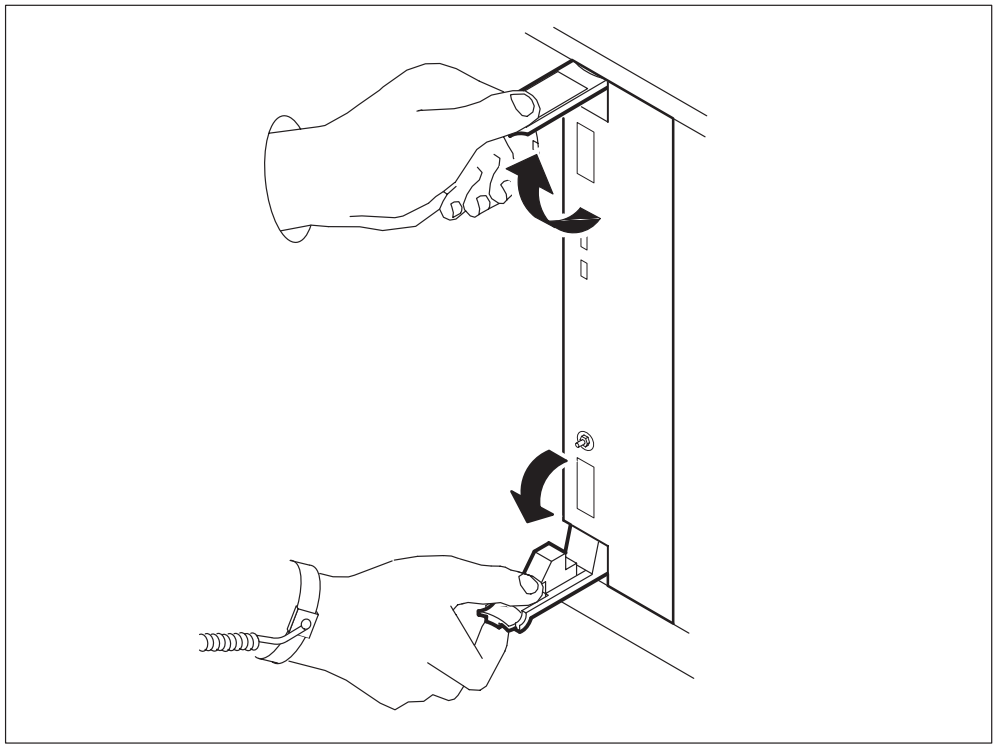
Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

15 Depress the tips of the locking levers on the face of the CPU controller module.



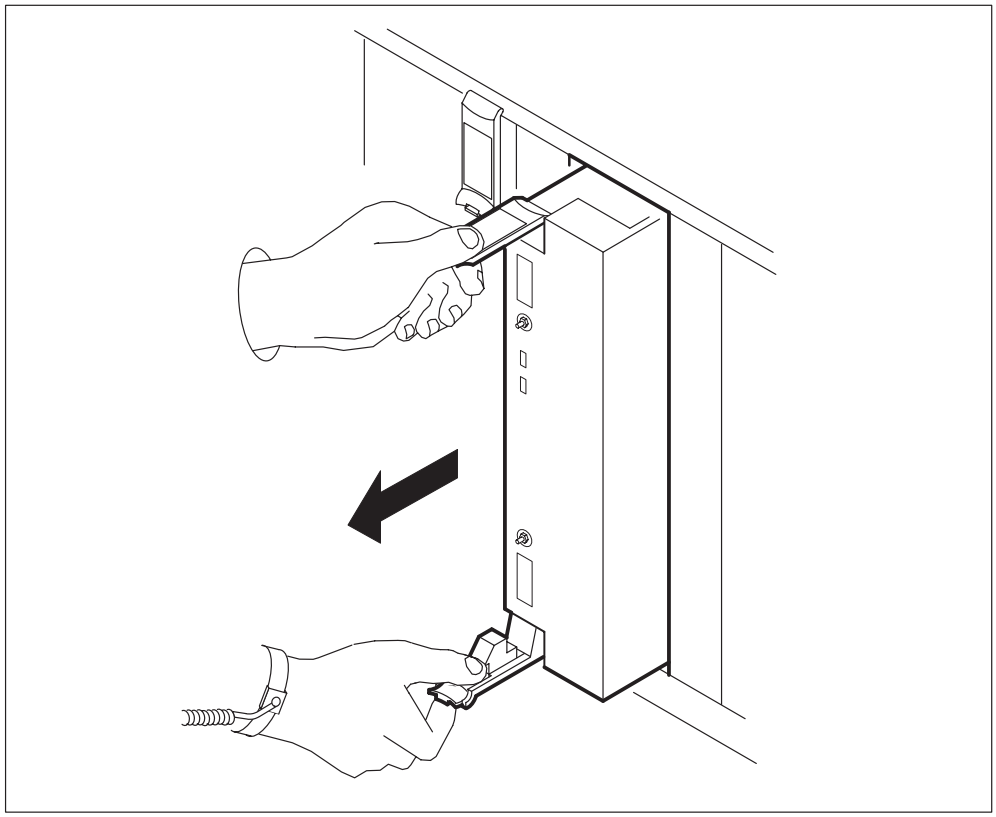
Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

16 Open the locking levers on the face of the module by moving the levers outwards.



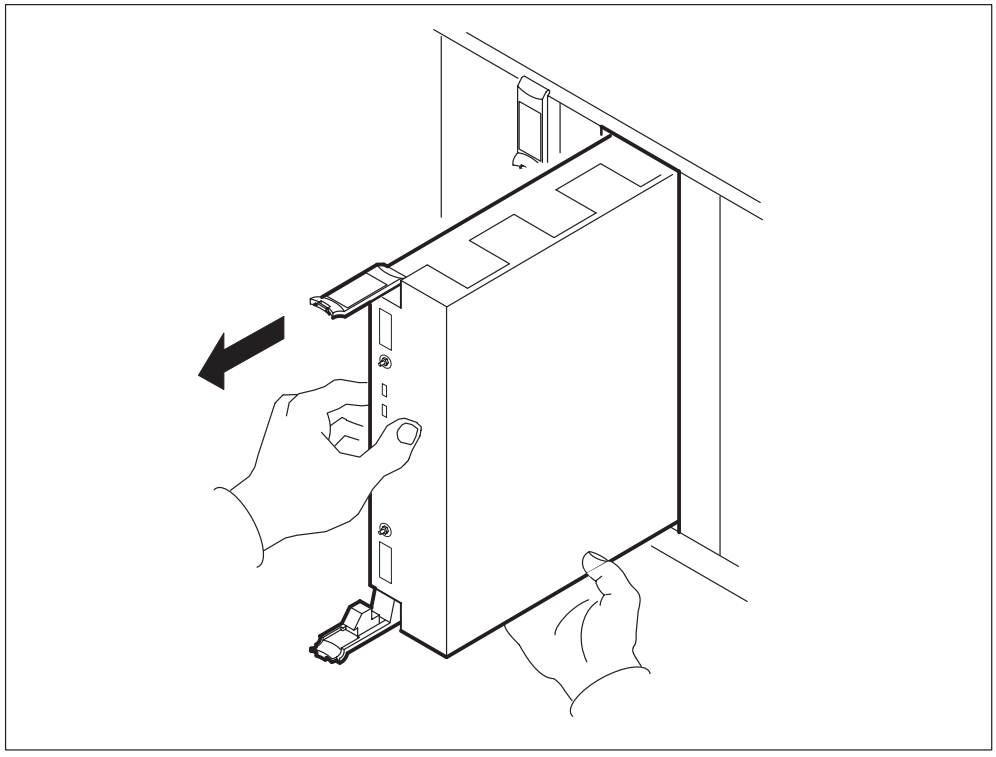
Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

17 While grasping the locking levers, gently pull each module towards you until it protrudes about 2 in (5.1 cm) from the SDM shelf.



Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

18 Hold the module by the face plate with one hand while supporting the bottom edge with the other hand. Gently pull the module toward you until it clears the shelf.

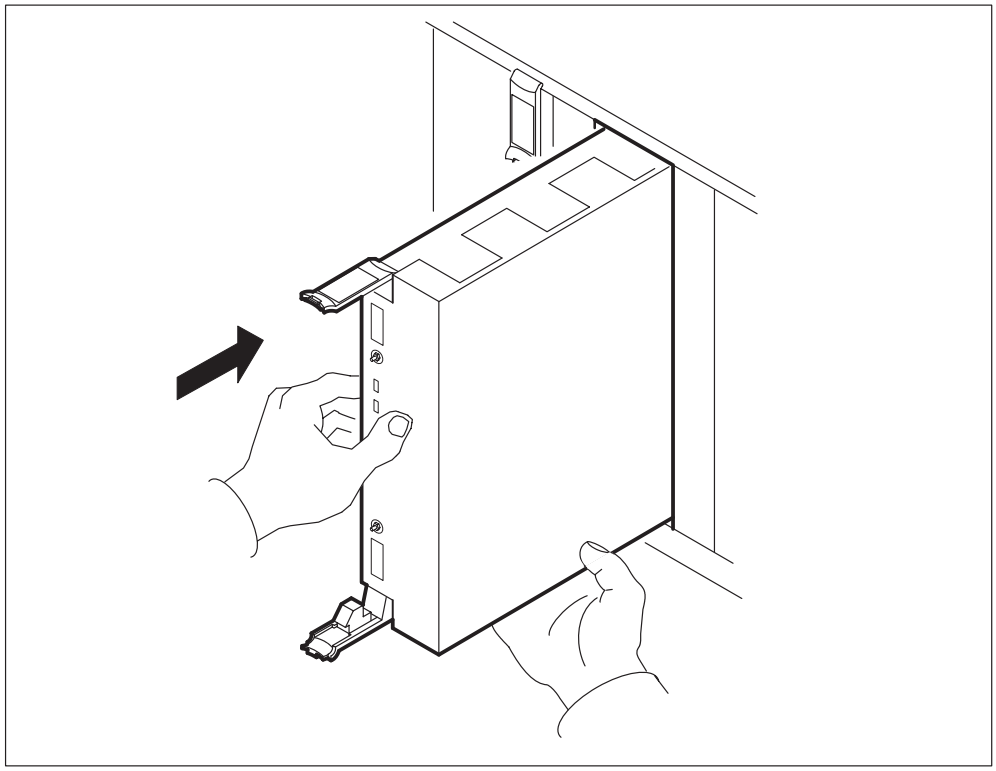


19 Place the module you have removed in an ESD protective container.

20 Insert the replacement module into the SDM shelf.

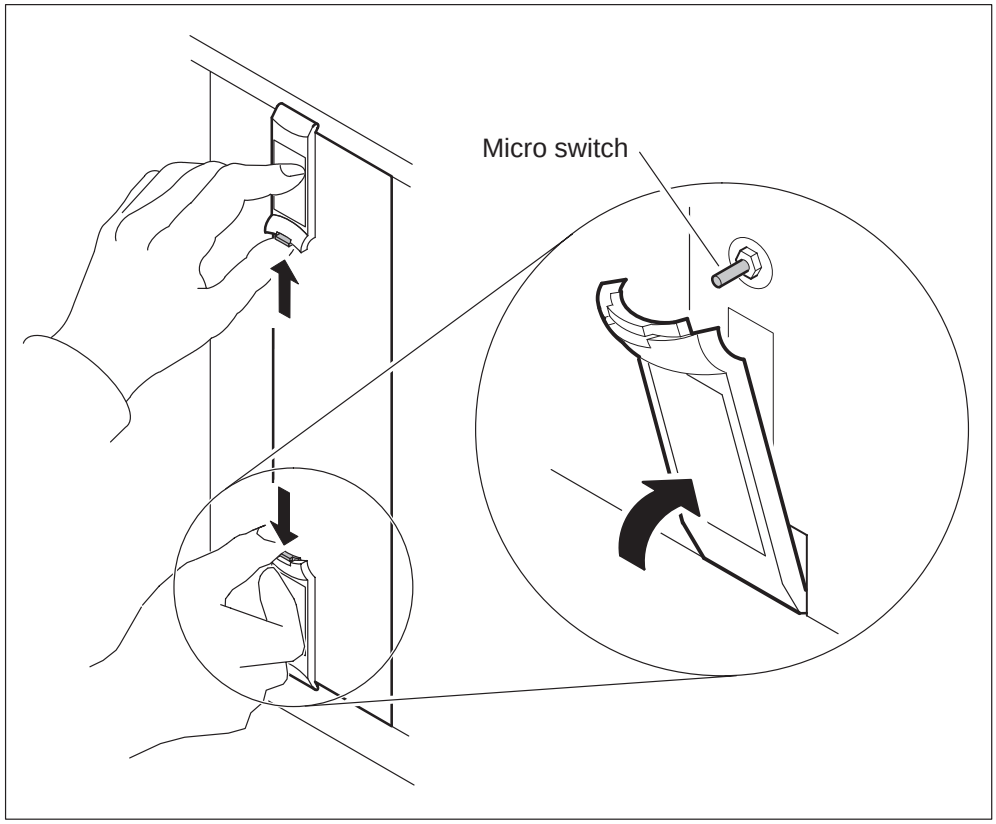
Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

21 Gently slide the module into the shelf until it is fully inserted.



Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

22 Close the locking levers to secure the module. Ensure that both the top and bottom micro switches are lined up with the locking levers to properly seat the module.



23 Tighten the thumbscrews on the module.

24 Proceed according to the the number of CPU controller modules you have replaced.

If you have replaced	Do
one CPU controller module	step 14
both CPU controller modules	step 25

Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

At the MSP

25 Restore power to the SDM by turning the MSP breakers on. Proceed according to the chassis structure of your system.

If your system contains	Do
a main chassis only	turn top two breakers on
contains a main and I/O expansion chassis	turn all four breakers on

Note: When the replacement CPU controller module is inserted, both LEDs on the module turn on briefly and then off, indicating that the module is seated correctly, is receiving power, and has passed its self tests. The in-service light on the CPU controller module then turns on in about 1 min, and the out-of-service light remains off.

At the local or remote VT100 console

26 Interrupt the boot process when the “COLD start” message appears by pressing the Break key.

Example response:

```
FX-Bug>
```

Note: The “COLD start” message does not appear for about 2 min.

27 Determine the current Greenwich Mean Time (GMT) setting on the new CPU controller modules by typing

FX-Bug>time
and pressing the Enter key.

Example response:

```
FRI APR 11 18:21:41:00
```

28 Determine if the GMT setting for the new CPU controller modules is correct.

If the GMT setting is	Do
correct	step30
incorrect	step 29

Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

29 Correct the time setting to the current GMT by typing

FX-Bug>set *mmddyyhhmm*
and pressing the Enter key.

where

mm	is the the numeric month of the year (01 to 12)
dd	is the the numeric day of the month (01 to 31)
yy	is the the last two digits of the current year (00 to 99)
hh	is the current hour (00 to 23)
mm	is the current minute (00 to 59)

CAUTION
Potential loss of service
Ensure that the GMT setting on the new CPU controller modules is later than the setting on the previous CPU controller modules (as recorded in step 12). If the system is rebooted with a GMT setting that is earlier than the time the system was shut down, system configuration and status information may be corrupted.

30 Boot the SDM from disk by typing

FX-Bug>pboot 1 0
and pressing the Enter key.

31 Allow the reboot to continue uninterrupted.

32 At the login prompt, log in to the SDM as the root user.

33 Restore the bootlist by typing

 # bootlist -m normal *hdiskn1 hdiskn2*
and pressing the Enter key.

where

hdiskn1 and *hdiskn2*	are the two physical disks which provide rootvg storage, as recorded in step 7

Upgrading the CPU controller module NTRX50FL, NTRX50FM (continued)

34 Log in to the RMI by typing

 # sdmmtc
and pressing the Enter key.

35 Access the hardware (Hw) menu level by typing

>HW
and pressing the Enter key.

36 Allow the CPU controller modules to complete reintegration.

Note: At the hardware menu level of the RMI, the status of one CPU controller module appears as a dot (.), indicating that it is in-service. The status of the other CPU controller module appears briefly as “F”, then changes to “S”, indicating that it is reintegrating with the other CPU controller module. The reintegration process takes about 2 min to complete, after which the status of the second CPU controller module changes from “S” to “ . ”.

37 Exit the RMI by typing

> QUIT ALL
and pressing the Enter key.

38 Force each CPU controller module to assume mastership to synchronize their clocks by typing

 # ftctl
and pressing the Enter key.

Then type

 # ftctl
and press the Enter key.

39 After you expand the CPU memory, you must extend the paging space. Go to the directory where you will extend paging space by typing

 # cd /sdm/mtce/sct
and pressing the Enter key.

40 Extend the paging space by typing

> ./customize -m
and pressing the Enter key.

The paging space is now reset at twice the memory size of the CPU.

Upgrading the CPU controller module NTRX50FL, NTRX50FM (end)

At the MAP display

41 Return the SDM to service by typing

>RTS
and pressing the Enter key.

Response:

```
SDM RTS initiated.
SDM RTS completed.
```

42 The system automatically returns all modules to service.

43 You have completed this procedure.

List of terms

802.3 10BASE-T

An IEEE standard for operating Ethernet LANs on twisted-pair cable with a transmission rate of 10 Mbit/s.

10BASE-T

An Ethernet LAN that works on twisted pair wiring similar to telephone cabling.

Access Control List (ACL)

A set of entries associated with a file that specify permissions for all possible user ID and group ID combinations.

ACL

See Access Control List (ACL).

Advanced Interactive Executor (AIX)

The IBM implementation of UNIX. AIX is the base operating system in the SDM.

AIX

See Advanced Interactive Executor (AIX).

alarm

A signal that is visual, audible, or both that is used to alert operating company personnel to a condition requiring attention.

backplane

Connector blocks and special wiring on the rear of a shelf. Printed circuit board modules normally mount in front of the backplane.

boot

The process of loading, initializing, and running an operating system.

C28B

See C28 model B DMS streamlined cabinet (C28B).

C28 model B DMS streamlined cabinet (C28B)

A cabinet used to house customer-specified equipment.

cell

In DCE, a collection of objects that are controlled by a registry database.

channel service unit (CSU)

Line bridging devices that allow several inputs to share one output. CSUs exist to handle any input/output combination of synchronous or asynchronous terminals, computer ports, or modems. These units are also called modem sharing units, digital bridges, port sharing units, digital sharing devices, modem contention units, multiple access units, control signal activated electronic switches or data-activated electronic switches.

client

A computer or program that requests one or more services from a server.

CLLI

See common language location identifier (CLLI).

CM

See computing module (CM).

common language location identifier (CLLI)

A standard identification method for trunk groups in the following form:

aaaa bb xx yyyy

where:

aaaa
is the city code
bb
is the province or state code
xx
is the trunk group identifier
yyyy
is the trunk number

computing module (CM)

The central processor and memory element of DMS SuperNode. The CM consists of a pair of CPUs with associated memory that operate in a synchronous matched mode on two separate planes. Only one plane is active; it maintains overall control of the system while the other plane is on standby.

correlated log

An incoming log report that has been processed (correlated) by the knowledge base. A problem instance is associated with this log.

CSU

See channel service unit (CSU).

data service unit (DSU)

Also called digital service unit. Converts RS-232-C or other terminal interface to DSX-1 interface.

datavg

See data volume group (datavg).

data volume group (datavg)

A logical volume on the SDM used to store application data. If datavg is not present on a system, application data is stored in the root volume group group).

DCE

See Distributed Computing Environment (DCE).

directory

A named portion of the UNIX file system.

disk mirroring

The SDM stores a mirror copy of all data that is written to a logical volume. In the event of a filure to one disk, the system is able to read from and write to the remaining disk without interruption.

Distributed Computing Environment

An architecture consisting of standard programming, interfaces, conventions and server functionalities (remote procedure call) for distributing applications transparently across networks.

DMS SuperNode

The central control and messaging component of the DMS-100 switch. DMS SuperNode consists of two major elements, the computing module (CM) and the message switch (MS). The CM is the central processing and memory element. The MS is the messaging hub for the switch.

DRAM

Dynamic random access memory

DSU

See data service unit (DSU).

dynamic information

Information that is displayed and updated automatically. Dynamic information can be displayed without typing a command. An alarm banner, for example, is updated automatically. Other information that requires a command input does not require the command to be invoked a second time to show updates to the displayed screen.

electromagnetic interference (EMI)

The phenomenon resulting when electromagnetic energy causes an unacceptable or undesirable response, malfunction, degradation, or interruption of the intended operation of the electronic equipment, subsystem, or system.

Enhanced Terminal Access (ETA) application

The Enhanced Terminal Access application provides secure access to the SDM and the CM from a GUI running on a remote workstation.

erasable programmable read-only memory (EPROM)

A type of read-only memory in which data is initially programmable as in programmable read-only memory (PROM). Unlike PROM, in which the program is fixed (cannot be changed) after initialization, EPROM internal data can be erased and changed after the initial program has been installed.

ESD

Electrostatic discharge

Ethernet

A physical and data link protocol used for LANs.

exception report

A log that indicates that a certain number of logs have been generated in a certain time period. All exception reports are log type EXC900, by default.

Exception Reporting (ER) application

The Exception Reporting application performs event correlation, and generates exception reports.

fault tolerant

On the SDM, a hardware platform that can survive a single point of failure without an associated loss of service.

file system

A hierarchical structure of files and directories that resides on a single logical volume. A file system must be mounted onto a directory mount point. When multiple file systems are mounted, a directory structure is created that presents the images of a single file system.

file transfer protocol (FTP)

A service that supports file transfer between local and remote consoles over a TCP/IP network.

FTP

See file transfer protocol (FTP).

graphical user interface (GUI)

Point and click iconic interface for user-to-computer interaction.

GUI

See graphical user interface (GUI).

halting

Bringing the system to a complete stop so that no processes are running.

HP

Hewlett Packard

IEEE

Institute of Electrical and Electronic Engineers

IOC

See I/O controller (IOC).

I/O controller (IOC)

An equipment shelf that provides an interface between up to 36 I/O devices and the central message controller (CMC). The IOC contains a peripheral processor (PP) that independently performs local tasks, thus relieving the load on the CPU.

inference engine

A software module that generates exception report logs.

IP

Internet protocol

I-tape

Incremental software backup tape

knowledge base

The knowledge base analyzes incoming computing module (CM) logs and identifies the type of exception report to be generated.

LAN

See local area network (LAN).

LED

See light-emitting diode (LED).

light-emitting diode (LED)

A solid-state device which emits light when the appropriate voltage is applied to it. The LEDs are used in the DMS-100 switch components as front panel indicators, and they are usually off when equipment status is normal.

LIM

See link interface module (LIM).

link interface module (LIM)

A peripheral module (PM) that controls messaging between link interface units (LIU) in a link peripheral processor (LPP). The LIM also controls messages between the LPP and the DMS-bus component. A LIM consists of two LIM units and two frame transport buses (F-bus). The two LIM units operate in a load-sharing mode with each other. *See also* link peripheral processor (LPP).

link peripheral processor (LPP)

The DMS SuperNode equipment frame or cabinet that contains two types of peripheral modules (PM): a link interface module (LIM) and one or more application-specific units (ASU). *See also* link interface module (LIM).

local area network (LAN)

A network that permits the interconnection and intercommunication of multiple computers, primarily for the sharing of resources such as data storage devices and printers.

local console

A console that is connected directly to the SDM with an RS-232 null modem cable. Any other console is a remote console.

log category

A common group of log types that the knowledge base handles in a generic fashion.

Log Delivery application

The Log Delivery application delivers computing module (CM) and SDM log reports to an operations support system by way of a TCP/IP connection.

log report

A message sent from the DMS switch whenever a significant event has occurred in the switch or one of its peripherals. A log report includes state and activity reports as well as reports on hardware and software faults, test results, and other events or conditions likely to affect the performance of the switch. A log report can be generated in response to a system or manual action.

Two types of log reports apply to the SDM. The main DMS log stream reports SDM events in the PM series of logs. The SDM also reports events locally in the SDM series of logs - this log stream is not part of the main DMS log stream. The SDM Log Delivery application provides access to both streams through the SDM. For additional information on log reports applicable to the SDM, see the Maintenance Overview chapter of this document.

log type

A string used to identify a log. The string is made up of two parts: a log name of up to five characters, and a 3-digit log number. This string is used as the key for customizing threshold values.

logical volume

A storage device, similar to a disk section but of flexible size, that can hold a file system, raw data, application programs, or swap.

LPP

See link peripheral processor (LPP).

maint (maintenance) user

Monitors SDM system performance, and performs required maintenance tasks. Maint users have restricted shell access.

maintenance and administration position

See MAP.

master replica

In DCE, the first instance of a specific DCE server in the cell. The master replica is the only replica that can be modified. Only one master replica exists at one time.

MAP

Maintenance and administration position. A group of components that provides a user interface between operating company personnel and the DMS-100 family of switches. The interface consists of a video display unit (VDU) and keyboard, a voice communications module, test facilities, and special furniture.

MAPCI

MAP command interpreter

MAU

Media access unit

message switch (MS)

A high-capacity communications facility that functions as the messaging hub of the dual-plane combined core (DPCC) of a DMS SuperNode processor. The MS controls messaging between the DMS-bus components by concentrating and distributing messages and by allowing other DMS components to communicate directly with each other.

modular supervisory panel (MSP)

A hardware device that accepts the frame battery feed and ground return from the power distribution center (PDC). The MSP distributes the battery feed, by means of subsidiary fuses and feeds, to the shelves of the frame or bay in which it is mounted. The MSP also contains alarm circuits.

MS

See message switch (MS).

MSP

See modular supervisory panel (MSP).

MTC

An abbreviation for maintenance. MTC is the first-level maintenance subsystem of the MAP. *See also* MAP.

netmask

A 32-bit bit mask which shows how an Internet address is to be divided into network, subnet and host parts.

node

The terminating point of a link. With respect to DMS peripheral modules, a node is defined as a unit of intelligence within a system. The SDM is viewed by the DMS system as a peripheral module, linked to the DMS

system by an Ethernet link. See the chapter Understanding the fault tolerant SDM for additional information.

OAM

See operation, administration, and maintenance (OAM).

OAM&P

Operation, administration, maintenance, and provisioning

operating company (OC)

The owner or operator of a DMS switch.

operation, administration, and maintenance (OAM)

All the tasks necessary for providing, maintaining, or modifying the services provided by a switching system. These tasks include provisioning of hardware, creation of service, verification of new service, billing and trouble recognition and clearance.

OSS

Operations support system

PEC

See product engineering code (PEC).

PID

See process ID (PID).

PowerPC

Performance Optimized with Enhanced RISC for Personal Computers; the microprocessor architecture used in the SDM. PowerPC by is used by Motorola, Inc. under license by IBM. The term PowerPC is a trademark of IBM.

process

In UNIX, a program that is currently executing.

process ID (PID)

An integer assigned to a UNIX process that uniquely identifies the process. No two processes can have the same process ID.

product engineering code (PEC)

An eight-character unique identifier for each marketable hardware item manufactured by Nortel.

read-only replica

In DCE, a type of replica. The read-only replica is a copy of a directory that contains changes made to the master replica. The read-only replica is used only for looking up information.

reboot

Taking the operating system from a running state down to a stopped state, and back to a running state.

remote console

Any console that is not connected directly to the SDM with an RS-232 null modem cable.

remote maintenance interface (RMI)

The user interface for the SDM which provides node maintenance, administration, and monitoring functions. This interface is accessible to the root or maint user at the local or remote VT100 terminal, or from the operating company LAN. See the "SDM maintenance overview" and the "SDM system administration overview" chapters of this document for a full description of the RMI.

remote procedure call (RPC)

A protocol which allows a service running on one host to cause code to be executed on another host. RPC is used to implement the client server model of distributed computing. An RPC is implemented by sending request messages to a remote system (the server) to execute a designated procedure, and a result message returned to the caller (the client).

replica

In DCE, each physical copy of a directory, including the original. Two types exist: master, and read-only.

restricted shell

A shell is restricted when a user is restricted to using specific UNIX commands.

RMI

See remote maintenance interface (RMI).

root user

The SDM system administrator. Responsibilities include adding and removing users from the SDM, assigning and restricting user access, and password administration. A root user has unrestricted shell access.

rootvg

See root volume group (rootvg).

root volume group (rootvg)

A logical volume on the SDM used to store the AIX operating system, platform software, application executables, shared libraries, static and configuration files.

RPC

See remote procedure call (RPC).

RS-232

The industry standard for a 25-pin interface that connects computers and peripheral equipment such as modems and printers.

SCC2

Switching control centre 2. Log header used for logs sent to an SCC2 mini computer for processing.

SCSI

Small computer system interface

SDM

SuperNode Data Manager

STD

Standard. Standard or normal log header format

Secure File Transfer

An SDM application that provides secure file transfers to the computing module (CM) and/or the SuperNode Data Manager (SDM) from a remote node across an operating company's TCP/IP wide area network (WAN).

server

A powerful, centralized computer (or program) designed to provide information to clients upon request. The SDM acts as the server for distributed software applications.

shell

A command line interpreter that reads user input and executes UNIX commands.

SMIT

System management interface tool.

SNMP

Simple Network Management Protocol

S-tape

System image software backup tape

static information

Information that is displayed once each time a command is invoked.. Updates to the information on the screen are not automatically displayed.

SuperNode Billing Application (SBA)

SBA provides a distributed, high capacity scalable billing system that enhances the functionality of all SuperNode switch types.

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

telnet

A program that acts as a terminal emulator, allowing you to connect remotely to other terminals.

UI

User interface

UNIX

A computer operating system.

uncorrelated log

An incoming log report for which there are no rules in the knowledge base, or the rules have been disabled. Enabling and disabling the rules is done using the Log Customization Utility and does not require resetting the expert system.

unseat

Cards can be unseated from line concentrating modules (LCM), ISDN line concentrating modules (LCMI), remote cluster controllers (RCC), ISDN remote cluster controllers (RCCI), and remote maintenance modules (RMM).

unshielded twisted pair (UTP)

A cable medium with one or more pairs of twisted insulated copper conductors bound in a single plastic sheath.

UTP

See unshielded twisted pair (UTP).

Index

Symbols

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

DMS-100 Family
SuperNode Data Manager
Fault-tolerant User Guide

Product Documentation—Dept 3423
Northern Telecom
P.O. Box 13010
RTP, NC 27709–3010
1–800–684–2273
(1–800–NTI–CARE)

Publication number: 297-5051-906
Product release: SDMN0009
Document release: Standard 03.04
Date: October 1998
Printed in the United States of America

NORTEL
NORTHERN TELECOM