Network Operations Systems

DNC-50, DNC-100, DNC-500 Dynamic Network Control System

General Description

Network Operations Systems

DNC-50, DNC-100, DNC-500* Dynamic Network Control System

General Description

Publication number: 450-1011-100
Product release: NSR27 02
Document release: Standard
Date: May 12 1989

* DNC-50, DNC-100, and DNC-500 are trademarks of Northern Telecom.

Revision history

May 12, 1989 Release NSR27 02

Table of contents

1. Introduction

Scope of this Practice

This practice describes the DNC-50, DNC-100, and DNC-500 Dynamic Network Control Systems and their hardware, software, applications, and services. It also supports Meridian MS-1* Meeting Services. Specific information regarding planning, installation, configuration, and use is given in other practices in the sequence 450-1011-zzz; as follows:

450-1011-019	Guide to Service Priority Classification Codes
450-1011-151	Provisioning Guide
450-1011-152	Site Records
450-1011-200	Installation Planning Guide
450-1011-201	Installation Guide for Cabinet Systems
450-1011-202	Installation Guide for Bay Systems
450-1011-301	A Guide to System Administrative Services
450-1011-302	A Guide to DNC Base Software Installation (NT use only)
450-1011-501	Maintenance and Troubleshooting Guide
450-1011-502	Maintenance and Troubleshooting Guide for Bay Systems
450-1011-505	A Guide to Extended Diagnostics
450-1011-511	A Guide to DNC Logs and Alarms

The DNC systems serve as platforms for various software applications. These practices are therefore considered the base DNC library and are incorporated into the libraries of the various NTP libraries for the applications (see Table 1-A).

---

* Meridian and MS-1 are trademarks of Northern Telecom.

This document describes the base DNC services that serve as underlying utilities for the various DNC applications. These applications are described briefly in Part 3 and the base DNC services are described in Part 4. The DNC architecture is described in Part 2.

The NTP libraries for the applications refer to the base DNC documents as required for procedures common to all or several applications. Most of these common procedures are accessed using System Administrative Services (SAS), while some are available to general users.

> ***Note:*** Not all applications use all the base DNC services. Consequently, some of the base DNC services described in Part 4 may not be present in your system.

This practice also outlines the role of the system administrator in the operation of a DNC system. It discusses the various functions that the administrator performs in configuring and maintaining the system hardware and software. It also describes the DNC man-machine interface (MMI). Detailed procedures for all the system administration functions are given in the Guide to System Administrative Services, 450-1011-301.

Document Release Information

The release information for this issue of this document is found on page i. The information includes the 10-digit identification number for the practice, plus the following additional information:

(a) ***Date***: This is the date the document was released for reproduction or printing. It is not intended to be the same as the software or product release date.

(b) ***Product release*** This is the software or product release number associated with the current issue of the document, plus the issue number of document. The format is NSRaa bb, where:

- NSRaa is the Network Software Release number
- bb is a sequential issue number for the document that indicates how many times the document has been released with the specified software release.

(c) ***Document release:*** A rating code of Draft, Preliminary, or Standard is assigned to the document, reflecting the current status of the document.

Changes since the NSR26 Version

This version refers to the following new features and services that have been added to the base software in NSR27.

(a) For protection against disk failures in SCSI file systems, the system administrator can now specify shadow disks. In this arrangement, two SCSI disk units are paired so that one functions as the primary disk and the other functions as a ‘shadow disk’. The system reads information from the primary disk but writes to both the primary and shadow disks. This ensures that there is a duplicate database in case the primary disk fails. (Shadow disks cannot be configured in SASI file systems.)

Note: The Business Network Management (BNM) application does not support the shadow disk capability in NSR27 release.

(b) It is now possible to reboot the system by entering a software command in the Helix Command Interpreter.

Dynamic Network Control Systems Overview

The DNC systems use the Data Voice System (DVS) architecture for hardware and software. This architecture provides a multiprocessor, multitasking computing environment for network operations. The hardware is modular, and can be easily expanded without replacing the initial installed base. (The architecture is described in Part 2.)

The DNC-50, DNC-100, and DNC-500 are all based on the same hardware and software architecture. The difference in systems is driven by the applications, particularly by the software and communications requirements.

The DNC-500 is used for operating company applications, while the DNC-100 and DNC-50 are used as servers to the DNC-500. The DNC-100 is typically located on the customer's premises for local processing and control. Many DNC applications do not require a DNC on the customer premises and therefore use only the DNC-500.

For example, all three DNC systems are used with the Business Network Management (BNM) application. In BNM, the DNC-50 is used to spool call detail records from the network switch to the customer's premises for processing.

BNM uses the DNC-100 for operations on the customer's premises and serves as the computing device for the customer's portion of a network operation. It has a data link to the DNC-500.

The DNC-500 has the software required for the operating company's network operations and is located on the operating company's premises. The DNC-500 interacts with switching equipment and other network elements.

In other applications, the DNC-500 operates in conjunction with network switching equipment for centralized administrations, operations, and maintenance function, and for control of network nodes.

Applications

The software applications are listed in Table 1-A with their respective NTP series. The applications are described in Part 3.

Table 1-A
The DNC Applications and Their NTP Libraries

Application	DNC-50	DNC-100	DNC-500
Business Network Management (BNM) (450-1021-zzz)	*	*	*
DMS Service Control Point (DMS-SCP) (450-1061-zzz and 450-1111-zzz)			*
Network Configuration Database (NCD) (450-1091-zzz)		*	

Abbreviations

The following abbreviations appear in this NTP:

ACO Alarm Cut-Off

ALIU Alarm Interface Unit

AMA Automatic Message Accounting

AMAT AMA Transmitter

APDU Application Protocol Data Unit

BIX Building Internal Cross-connect

BMS Backup Management System

BNM Business Network Management

CCE Cluster Controller Emulator

CCITT International Telephone and Telegraph Consultative Committee

DCR Dynamically Controlled Routing

DMS-SCP DMS Service Control Point

DNC Dynamic Network Control system

DNX Digital Network Cross-Connect system

DTE Data Terminal Equipment

DVS Data Voice System

EMI Electromagnetic Interference

I/O Input/Output

LAN Local Area Network

LAPB Link Access Protocol Balanced

LED Light-Emitting Diode

LIU LAN Interface Unit

MDC Meridian Digital Centrex

MMI	Man-Machine Interface
MTU	Magnetic Tape Unit
NCD	Network Configuration Database
NOP	Network Operations Protocol
NOS	Network Operations System
NSR	Network Software Release
NTM	Network Trouble Management
OSI	Open Systems Interconnection
OSS	Operational Support System
PAD	Packet Assembler/Disassembler
PRU	Program Resource Unit
RAM	Random Access Memory
RFT	Remote File Transfer
RRU	Remote Resource Unit
SAS	System Administration Services
SASI	Shugart Associates Systems Interface
SCSI	Small Computing Systems Interface
SMDR	Station Message Detail Records
SRU	Shared Resource Unit
SUN	Sending Unit
TOPS	Traffic Operator Position System
TSC	Test System Controller
TSM	Transport Services Management

2. DNC Architecture

Hardware

This part describes the DNC system hardware elements and their configuration in a DNC cabinet system. Hardware elements include the cabinets, shared resource units (SRUs), remote resource units (RRUs), peripheral equipment, and associated cabling and connectors.

Cabinets

The DNC consists of between two and eight free-standing gray cabinets, installed side-by-side and connected together. Each cabinet measures about 930 mm (36.5 in.) in height, 285 mm (11.5 in.) in width, and 560 mm (22 in.) in depth.

The cabinets run on 110 or 220 V ac, or -48 Vdc if powered from office battery. The use of an uninterrupted power supply (UPS) is recommended for systems operating on ac power (see your Northern Telecom representative for further information on UPS arrangements).

Each cabinet is an extruded plastic structure with two shelves, two cooling fans at the top of the cabinet, and a filtered air intake grill at the bottom. Floor support channels are attached to the cabinet base to ensure stability and to provide leveling adjustment. A dual-cabinet arrangement is shown in Fig. 2-1 to illustrate the features. Cabinets are secured to each other at the base with a rigid plastic interlock.

The cabinets are designed for universal mounting of the SRUs, regardless of the size of the SRU or the location of its connectors.

Figure 2-1
Cabinet Configuration

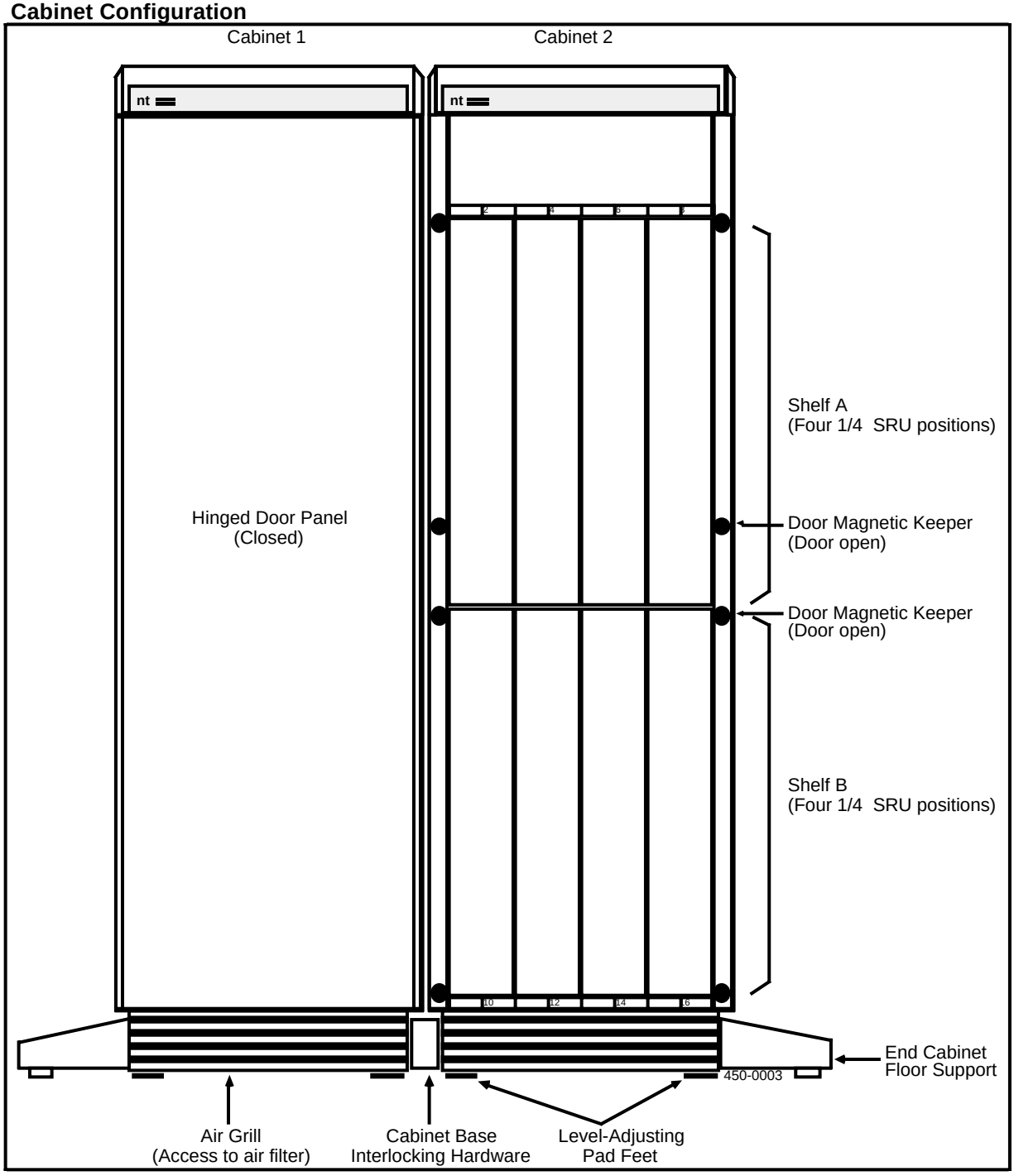
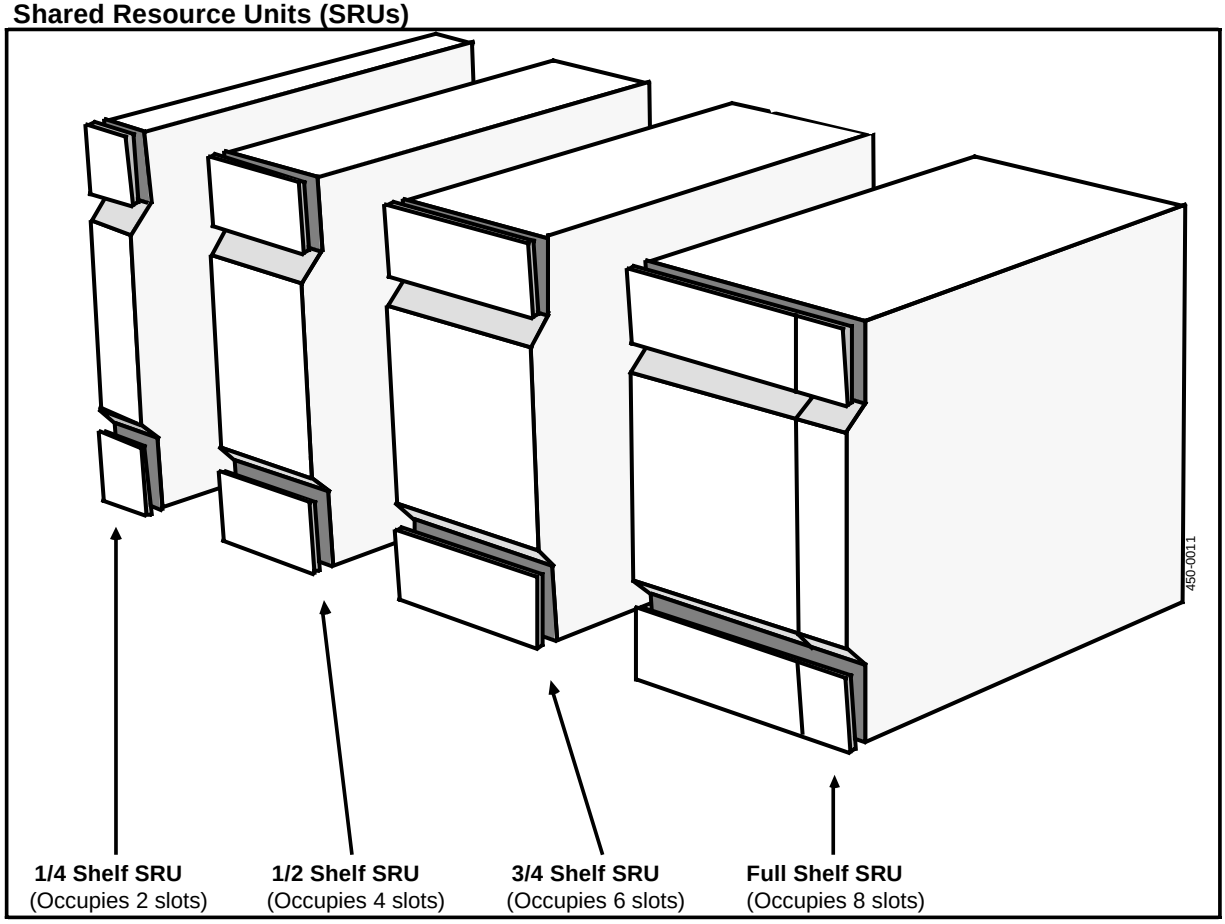


Figure 2-2
Shared Resource Units (SRUs)



Shared Resource Units

The shared resource units (SRUs) are independent processing devices inserted into the shelves of a cabinet. Since they have different widths (one-quarter, one-half, three-quarters, and full-width), they may occupy two, four, six, or eight slots (bus connectors) in a shelf (see Fig. 2-2). All SRUs are enclosed in metal for electromagnetic interference (EMI) shielding and they communicate with each other over a shielded backplane bus.

DNC systems are based on one of two interfaces for system control: the Shugart Associates Systems Interface (SASI) and Small Computing Systems Interface (SCSI). Most applications using NSR25 or later versions of software use the SCSI interface, which is faster than SASI and allows multiple file systems (or SCSI clusters).

A SCSI cluster consists of the Primary Processor or a File Processor SRU with associated Mass Storage and Cartridge Tape SRUs. The SCSI cluster associated with the Primary Processor is called the main SCSI cluster. Additional SCSI clusters can be added as required.

> ***Note:*** The SASI and SCSI interfaces can be mixed in a single DNC system, and SASI systems can be upgraded to SCSI. The restriction on mixing SASI and SCSI is that the Mass Storage SRUs must match the interface of the Primary Processor or File Processor they are connected to. See your Northern Telecom representative for information on upgrading from from SASI to SCSI.

There are a number of different types of SRU, each one having a specific function. These functions include supplying system power, system control, applications processing, communications interfaces, and mass storage of data and programs. They communicate with each other over the system bus, as shown in Fig. 2-3.

System Power Supply. The SRUs in DNC systems operate on -32 V, which is derived from standard 110 or 220 Vac commercial power sources or a -48 Vdc office battery. The system must be equipped with the appropriate power supply units for ac or dc sources. An upgrade kit is available for conversion from 110 Vac to 220 Vac.

The -32 V power is distributed to the SRUs over the power bus on the cabinet backplanes. The +32 V is converted inside each SRU to the specific voltages required by that SRU. Each SRU has an automatic power reset feature, which turns off power under potentially harmful conditions (such as overvoltage) and restores it when conditions are correct.

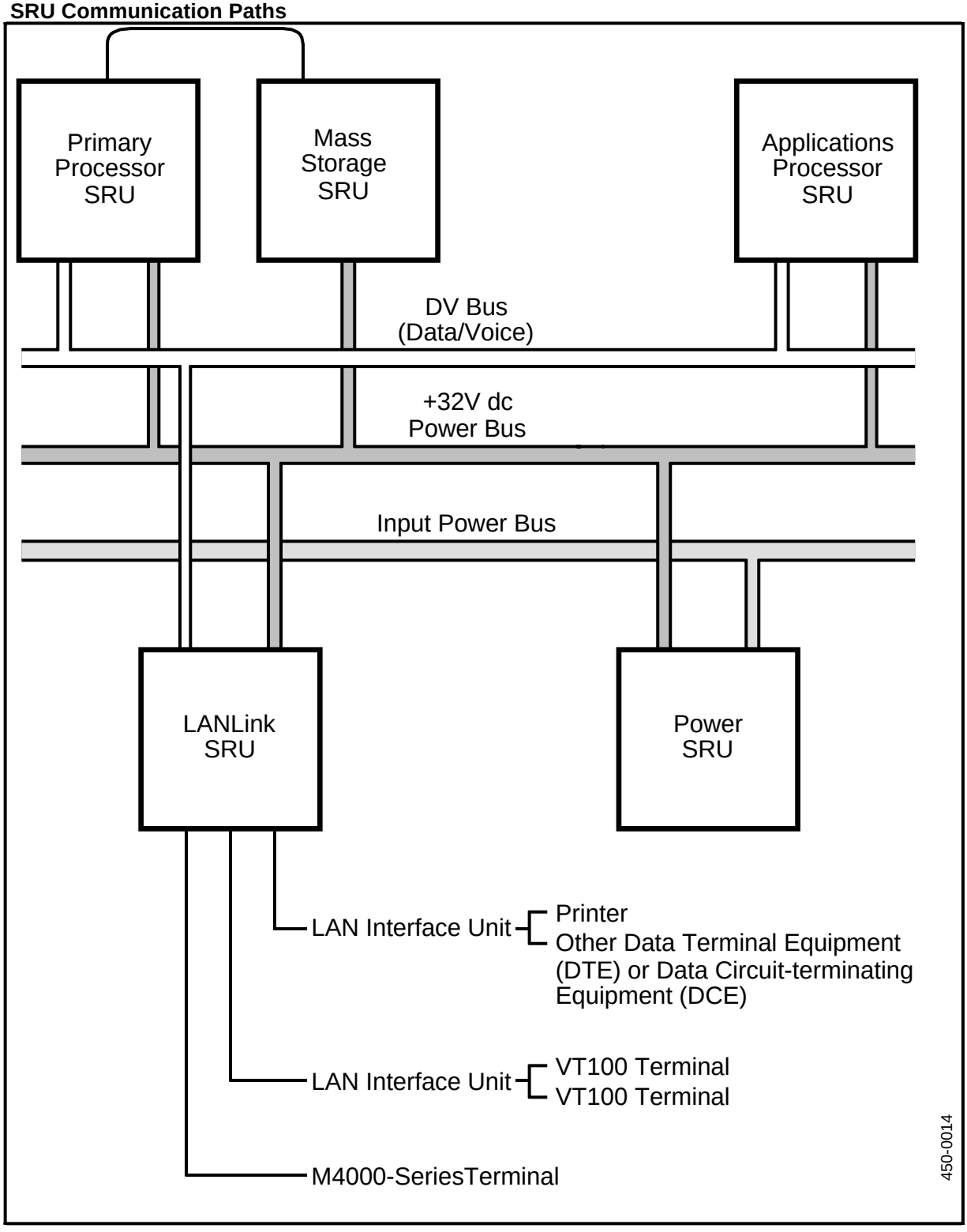
The power supplies are connected in parallel so that they share the power load. If one fails, the remaining power supplies share the load. A backup power supply can be provided.

System Grounding. Separate grounding straps are not required; ac sources are grounded through the grounding post of the input plug, and -48 V sources are grounded through the office battery supply's grounding system.

Power Supplies for ac Sources. There are two types of power supply for systems operating on ac, a Power Supply SRU and a Loft Power Supply. Prior to NSR24 (and with some NSR24 systems, depending on your application), power is supplied by half-shelf Power Supply SRUs. These SRUs are installed on the bottom shelves of the cabinets, where the cabinet is equipped with ac input connectors.

A loft power supply arrangement is standard in newer systems. In this arrangement, the power supply is installed in the air plenum at the top of the cabinet. This makes an additional two SRU positions available for each cabinet in the system. The loft power supply also offers improved performance.

Figure 2-3
SRU Communication Paths



One loft power supply is required for each cabinet in the system. A half-shelf Power Supply SRU is available with these systems to serve as a hot standby should a loft unit fail.

Power Supplies for dc Sources. The DNC can be equipped with a -48 V Power Converter SRU, which is a quarter-shelf SRU that converts -48 Vdc to -32 Vdc. To use -48 Vdc, a -48 Vdc Power Distribution System must be installed on the DNC. (See the ordering codes section of the Provisioning Guide, 450-1011-151 for the power distribution systems and upgrade kits available.)

DNC systems operating on -48 Vdc are currently restricted to those connected directly to a DMS-type host switch. In this arrangement, the grounding rules specified in 450-1011-200 and 297-1011-156 must be followed.

System Control. The Primary Processor SRU controls the operation of all other SRUs. No other processor can exercise system control. The system contains only one primary processor.

Each Primary Processor occupies two positions (that is, it is a half-shelf SRU). The SRU has a display window on its front panel to display primary status messages.

The Primary Processor SRU connects to the Mass Storage SRU via a SASI or SCSI cable. The Primary Processor SRU has five connectors on the back, two for the backplane, one for the cable to the Mass Storage SRU, and two RS-232-C connectors (a 9-pin and a 25-pin). The RS-232-C connectors are for use by Northern Telecom service personnel.

In SCSI systems, the file system that includes the Primary Processor is considered the main SCSI cluster. Additional file systems can be configured based on File Processors. (SASI systems have only one file system.)

Processing. The Primary Processor contains the core software for the system. Its processing power can be supplemented by additional Applications Processors and File Processors.

The Applications Processor SRUs are general-purpose processors that run various software programs under the control of the Primary Processor SRU. These programs include Base DNC services that do not reside on the Primary Processor, and the DNC applications software. The Applications Processor SRUs are available in several versions.

Individual Applications Processor SRUs can support different tasks, and even different operating systems. For example, one SRU can be running a services management package while another drives a testing program to help operations personnel isolate a fault. It is important to note that these SRUs run independently and simultaneously, and can transfer data as well as share a common database.

Each Applications Processor SRU occupies either one or two positions and has no front display or controls. It has a connector to the backplane and two RS-232-C connections (a 9-pin and a 25-pin) on its rear panel. Any DNC system will contain several of these SRUs, the total number depending on the application being run.

In SCSI systems, the File Processor SRUs control any Mass Storage SRUs other than the Mass Storage SRUs controlled by the Primary Processor. File Processor SRUs are available with various amounts of random access memory (RAM).

Mass Storage. Mass Storage SRUs provide hard disk storage for programs and data. The number of Mass Storage SRUs included in a system depends on two factors, the size of the system and the amount of data managed by the DNC application. Mass Storage SRUs provide the following amounts of hard disk storage:

- 80 megabytes unformatted, 71.3 formatted (also equipped with a built-in tape drive)
- 160 megabytes unformatted, (also equipped with a built-in tape drive)
- 350 megabytes unformatted, 265.6 megabytes formatted.

The SRUs use 8-inch Winchester hard disks. If an SRU with a built-in tape drive is not used, a separate tape unit is required for loading system programs and data. This tape unit may be a Cartridge Tape SRU or a Nine-Track Magnetic Tape Unit. (See the Provisioning Guide, 450-1011-151 for more information on configuring file systems.)

SASI systems can be equipped with only one file system, which must include an 80-megabyte Mass Storage Unit with built-in tape drive. A 350-megabyte unit can be added as an option.

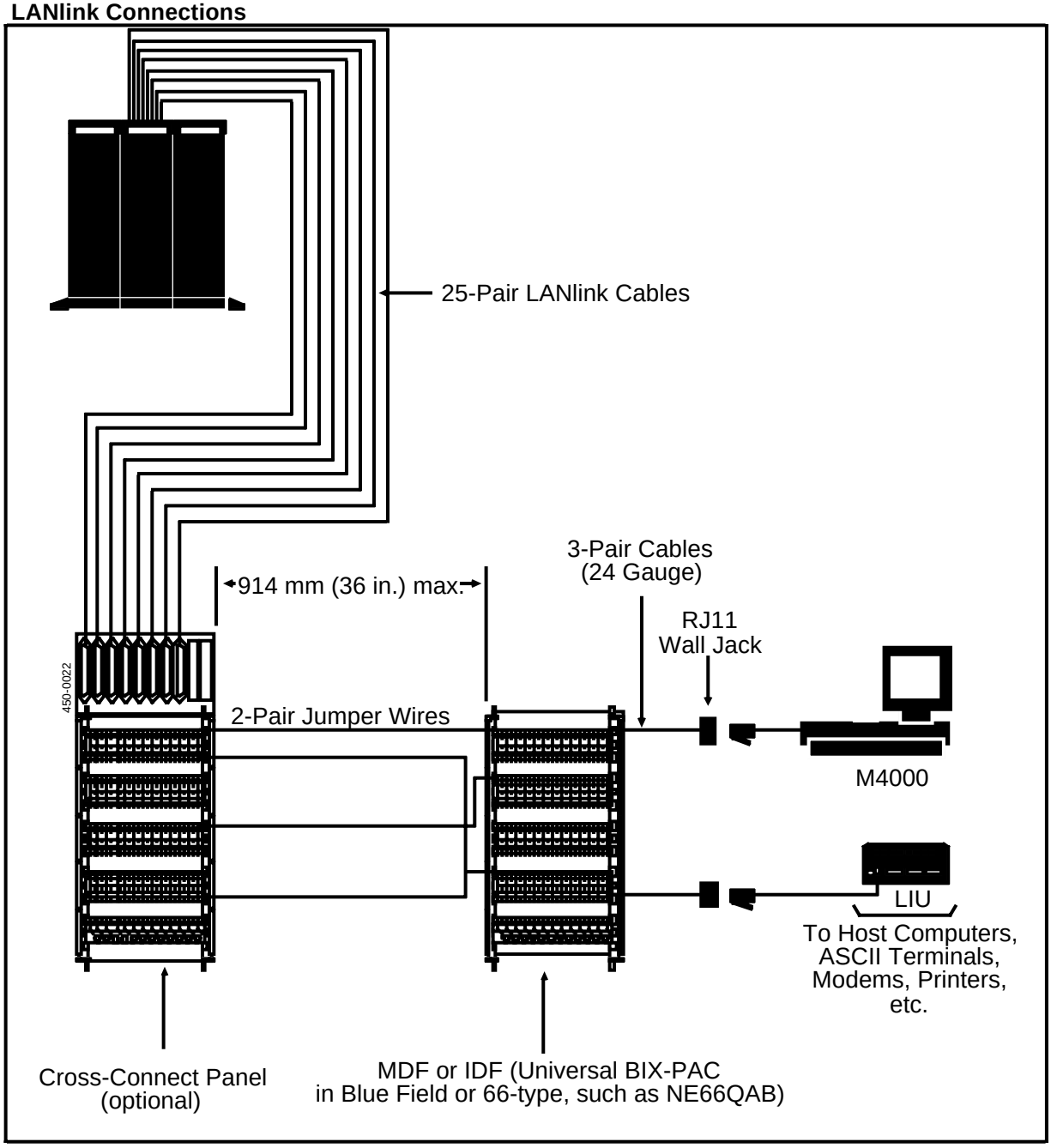
SCSI systems can contain more than one file system (or SCSI cluster), each containing up to four disk storage SRUs. Each SCSI cluster can also have two separate tape units. For greater reliability of data storage, the SCSI disk units can be paired so that one disk functions as the primary disk and the other functions as a ‘shadow disk’. In this arrangement, the system reads from the primary disk but writes to both the primary and shadow disks. This ensures that there is a duplicate database in case the primary fails.

> ***Note: The Business Network Management (BNM) application does not support the shadow disk capability in NSR27 release.***

LANlink Communications. The LANlink SRU provides the communications interface between the DNC system and the various peripheral devices, external equipment, and networks. LANlink SRUs connect to Meridian M4000 terminals and LAN Interface Units (LIUs). The LIUs in turn provide protocol conversion and physical interfaces to printers, ASCII terminals, host computers, modems, and networks (see Fig. 2-4).

The LANlink SRU is equipped with 12 ports, each of which operates at an aggregate rate of 2.56 Mb/s over twisted-pair wiring, for external connections to M4000 terminals or LIUs.

Figure 2-4
LANlink Connections



A LANlink SRU has no indicators on the front. On the back it has a connector for the backplane and a 25-pair Amphenol connector that contains all 12 output lines. Each line consists of two twisted pairs on the cable. The cable exits through an opening in the backplane and cover, and goes to the cross-connect facility.

Data Net Communications. The Local Data Net SRU (also known as the Twisted Pair Network Line Modile SRU) is a communications interface between DNC systems based on an aggregate rate of 2.56 Mb/s over twisted-pair wiring. When equipped with a Local Data Net SRU, the DNC system can be a node in a network of up to six similar DNC systems. Up to eight Local Data Net networks can be linked together, an arrangement called tandeming. The connection is established by a DNC system that acts as the tandem node. The tandem node contains one Local Data Net SRU for each Local Data Net network that is to be linked. (In the tandem arrangement, only one node can act as the tandem node.)

The Local Data Net SRU uses two 2.5 Mb/s communications ports (a master and slave interface). These ports are similar to the LANlink interface ports. Both ports can function in full duplex mode at the same time. See Part 4 for more information on Local Data Net.

Remote Resource Units

Remote resource units (RRUs) used with the DNC systems consist of LAN interface units (LIUs), which interface RS-232-C devices to the DNC systems, and connect to the LANlink SRU.

The LIU (Fig. 2-5) interfaces the LANlink SRU to various devices, such as ASCII terminals, host computers, printers and modems (for access to peripherals and networks). It has a Teladapt* jack for the connection to the LANlink SRU, and RS-232-C and parallel connectors for interfaces to the external equipment and networks.

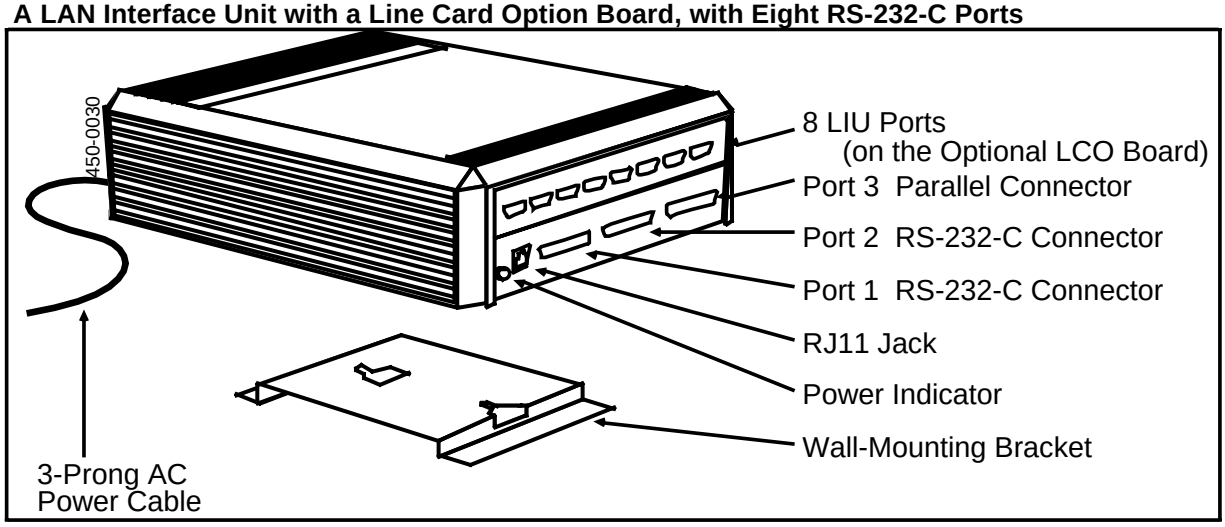
The LIU takes the high-speed 2.56 Mb/s data from one LANlink line and reformats it to make it compatible with several lower-speed RS-232-C and parallel ports. The ports operate at standard speeds up to 19.2 kb/s. (If a V.35 Option Board is installed in the LIU, the ports on that board can operate at speeds greater than 19.2 kb/s and up to 64 kb/s.)

The basic LIU has two RS-232-C ports plus one Centronics parallel port. In addition, it can be ordered with one of the following options boards:

- a Line Card Option Board (LCO Board), with eight asynchronous serial RS-232-C ports
- an Alarm Interface Unit (ALIU)
- a Mag Tape Option Board, with two 50-pin parallel ports (for SASI Nine-track Magnetic Tape Units only).

* TELADAPT is a trademark of Northern Telecom.

Figure 2-5
A LAN Interface Unit with a Line Card Option Board, with Eight RS-232-C Ports



External Devices

External devices are any devices connected to the DNC, including peripherals, host computers, and network access equipment. The equipment is connected to shared resource units (SRUs) in the DNC via cross-connect facilities. The following types of equipment can be connected to the DNC:

- Meridian M4000 terminals, as control consoles for the system, which are connected to a LANlink port in a LANlink SRU
- VT100*-compatible ASCII display terminals, as control consoles, which are connected to a LANlink port via a LAN Interface Unit (LIU)
- Host computers, printers, modems, 9-track reel-to-reel magnetic tape units (MTUs), and other peripherals connected to LANlink ports via LIUs.

Control Consoles. The M4000-series terminals (Fig. 2-6) have a 12-inch (300 mm) monochrome display and a 132-character keyboard. The monitor position and brightness are user-adjustable. The keyboard is connected by a coiled, extendable Teladapt-style cord, and the keyboard can be stored under the base when not in use. The M4020 has a built-in telephone and data capability, and the M4010 is the data-only version of the M4020.

The ASCII terminals have a similar user interface as the M4000, although they use ASCII characters to approximate the graphics of the M4000 terminals. A list of compatible ASCII terminals is available in the Provisioning Guide, 450-1011-151.

* VT100 is a deademark of Digital Equipment Corrp.

Other Peripherals. Either parallel or serial printers can be used with the system. Each LIU is equipped with one Centronics type port for parallel connections, and at least two RS-232-C ports for serial connections. The LIU also provides connections to all other external equipment, with the exception of the M4000 terminals.

The DNC can be connected via LIU ports to IBM-type, ASCII, and X.25 hosts. Network nodes (such as DNX*-100 Digital Cross-Connect Systems, controlled by the TSM application) are treated as ASCII hosts when connected to the system.

The nine-track magnetic tape unit (Fig. 2-7) is an option used when large amounts of data are to be dumped to tape and processed downstream. When used with a SASI file system, the magnetic tape unit connects to a parallel port on a Mag Tape Option Board installed in an LIU. (When used with a SCSI file system, the magnetic tape unit connects directly to the SCSI bus.) The magnetic tape unit is not usually used to load or store DNC programs or configuration data.

The LIU software does protocol conversions to allow connections to various data transport facilities, if required by the application. Modems are required if the peripheral devices are more than 15 m (50 ft) from the LIU. Null modem cables may be required to reverse wiring leads in some connections. (The LIU is configured as data terminal equipment, or DTE.)

* DNX is a trademark of Northern Telecom.

Figure 2-6
The Meridian M4010 Terminal (Data-only)

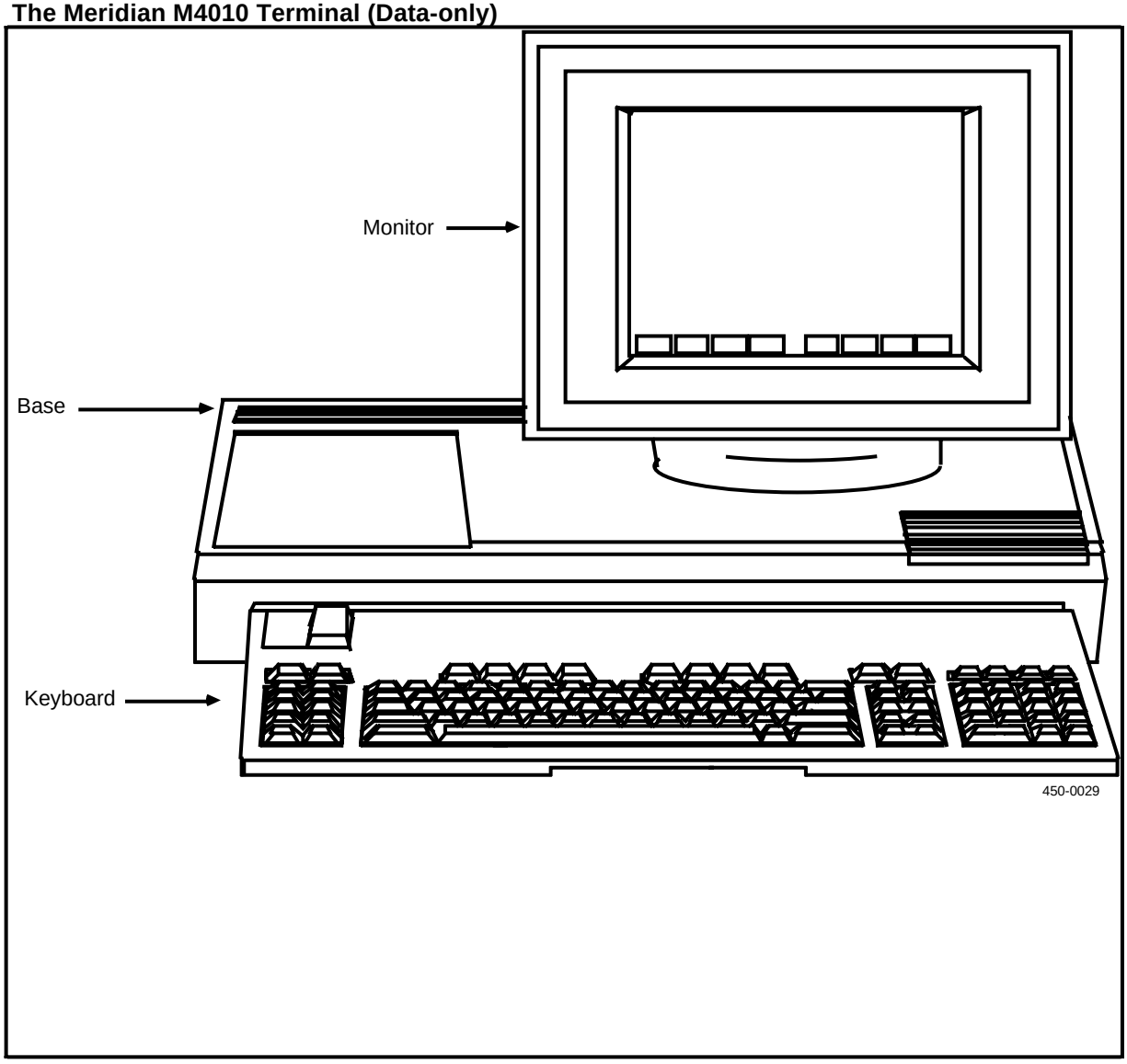
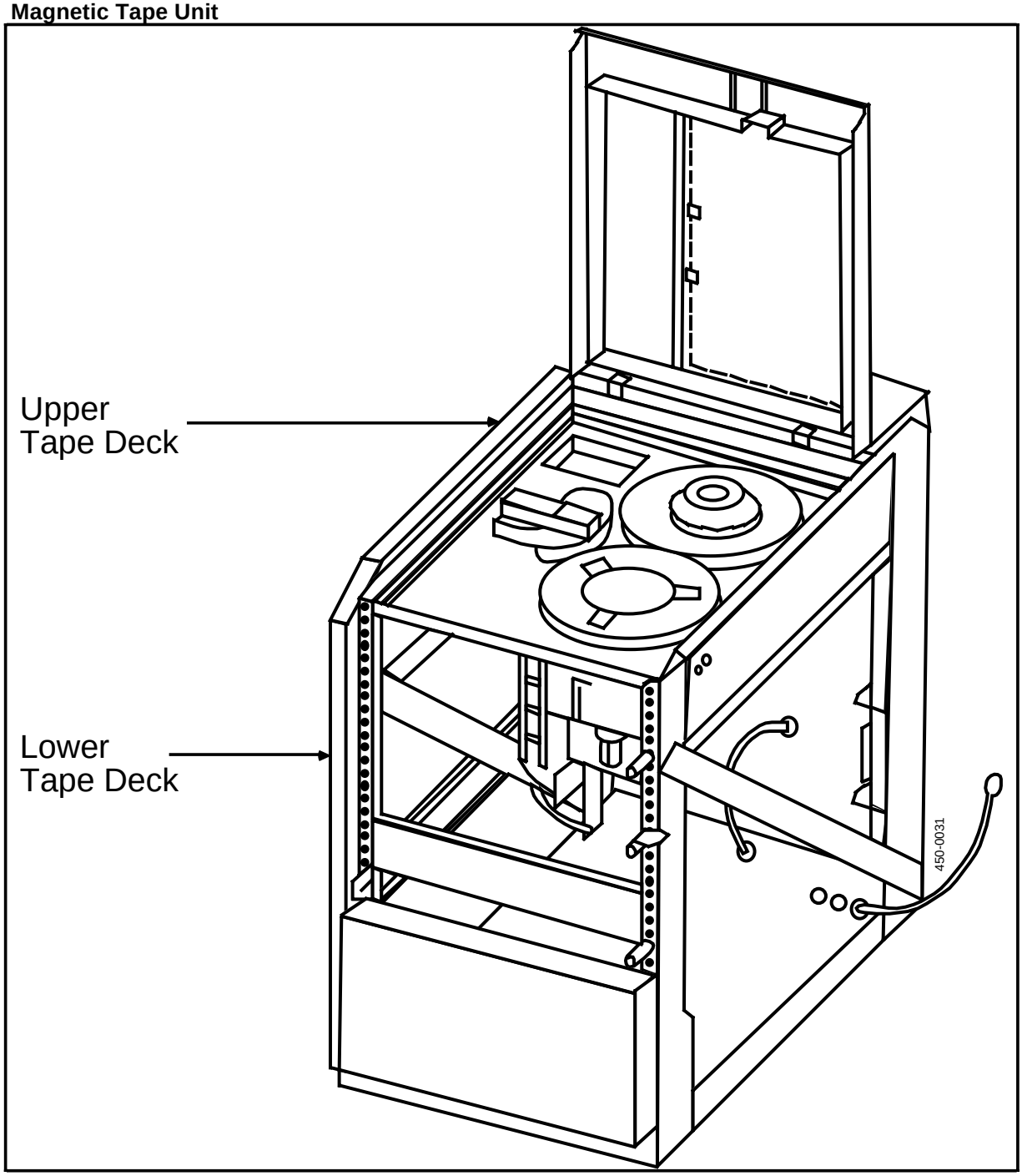


Figure 2-7
Magnetic Tape Unit



Software

DNC software is packaged in modular units called program resource units (PRUs). A PRU has its own function to perform within the overall system architecture; a PRU can be taken out of service, moved to another SRU, and put back into service without disturbing the other PRUs (unless another PRU calls up the out-of-service PRU).

Most PRUs reside on Applications Processor SRUs. However, some are required to be on the Primary Processor, notably core system PRUs. An Applications Processor SRU can hold one or more PRUs, depending on the memory required and the amount of RAM in the SRU.

Certain PRUs are provided with the base DNC software.Some of these PRUs may not be used by a given application. (The base DNC software is described in Part 4.) The DNC applications are provided as PRUs separate from the base software. (The applications are described in Part 3.) Other PRUs are provided with the DNC application. The PRUs included in this group depend on the application and the options ordered with it.

Core Software

The core software is the operating system, file system, and associated software that ensures basic system operation. It supports the DNC services and applications software (which are described in Parts 3 and 4). The core software includes the following:

(a) ***Operating System.*** The operating system for DNC is XMS (Extended Multiprocessor System), proprietary Northern Telecom operating system. When run on a DNC, the operating system is called DXMS. The operating system provides the master control for the system, controls traffic on the system bus, and monitors system performance.

(b) ***File System.*** The file system provides orderly access to data stored on the hard disks of the storage SRUs. It also controls read/write operations on the tape units. The Winchester disk storage and streaming tape (backup) for a DNC system is logically divided into multiple file systems. Access to a file system by any SRU is controlled by a bus administrator/controller function resident in the Primary Processor.

(c) ***Initialization.*** Base software initializes the SRUs during system start-up and/or software configuration changes. The system loads programs and files into the designated SRUs and attempts to initialize those SRUs. The system can also reload a PRU to an SRU after system initialization. This can be done manually by the system administrator, or automatically as a function of the diagnostics in the central maintenance software module.

(d) ***Device Managers.*** Base software includes device manager PRUs that control physical devices. Device managers are resident in those SRUs specific to base system services: the Primary Processor, Applications Processors, and LANlink SRUs.

(e) ***User Interface Base.*** This software package controls the access by users to the menus, forms and softkeys of the user interface.

(f) ***Maintenance.*** This central maintenance package monitors all SRU and PRU functions for proper operation. Diagnostic tests can be called up, and decisions made to take any device out of service. Maintenance software is a distributed function of each SRU device manager PRU. Each device manager is responsible for its own integrity checks and for reporting back to the central maintenance records. Maintenance software is always active at two levels,

local and central, to distribute responsibility downward from the central maintenance functions to the SRU level for local maintenance.

- ***Local Maintenance.*** Each SRU has its own local maintenance facility. Local maintenance completes integrity checks to verify hardware/software functions applicable for that SRU and reports to central maintenance.
- ***Central Maintenance.*** One central maintenance facility oversees the entire DNC. Central maintenance audits and maintains records of the local maintenance reports. It can direct reinitialization of PRUs and the reporting SRU. If an operation fails, central maintenance can take a unit out of service and issue warnings and messages. These can be written to a log system file for access by a system administrator using a DNC terminal.

Base DNC Services and Utilities

In addition to the core software, the base DNC software provides services and utilities including System Administrative Services (SAS), X.25, X.3 PAD, 3270 Emulation, 3780 Remote File Transfer, the Log and Alarm Subsystems, and additional utilities required by the DNC applications. The base DNC services are described in Part 4.

Communication With Nodes

DNC systems communicate with network devices by using Northern Telecom's Network Operating Protocol (NOP), or by using an X.25 Gateway and an X.3 Packet Assembler/Disassembler (X.3 PAD).

X.25 Gateway and X.3 PAD

The X.25 Gateway service and the X.3 PAD service are described in Part 4.

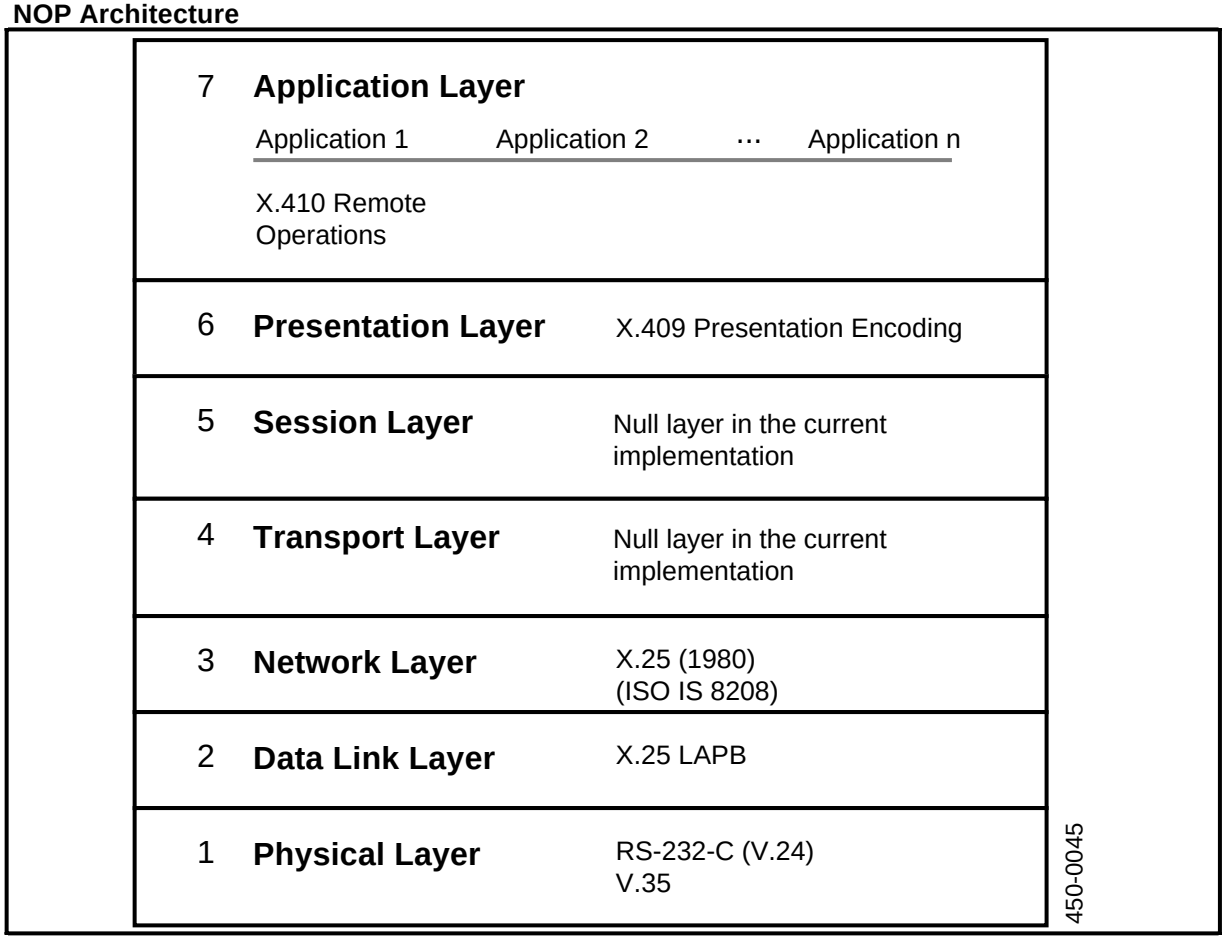
Network Operating Protocol (NOP)

Network Operating Protocol (NOP) is a packet data communications protocol based on the Reference Model for Open Systems Interconnection (OSI). The OSI model is recommended by the International Telephone and Telegraph Consultative Committee (CCITT). NOP also incorporates some other OSI and CCITT protocols and tools.

NOP is organized into layers, each layer providing part of the communications requirements for interconnected systems. The upper layers of NOP are designed to be independent of whatever lower layer protocols are chosen. Each layer of NOP has been defined by selecting particular options from existing standards. Thus, all components of NOP are fully compliant with the international standards.

NOP, as is consistent with the OSI model, has been structured into seven layers. Each layer has its optional and required components. The layers, shown in Fig. 2-8, are the following:

Figure 2-8
NOP Architecture



(a) ***Physical Layer (Layer 1).*** The physical layer is the lowest in the model. The functions within this layer are responsible for activating, maintaining, and deactivating a physical circuit between a DTE and a DCE. This layer provides the basic capability to transfer electrical signals between two directly connected systems. NOP can use either the RS-232-C standard (equivalent to CCITT V.24) or the CCITT V.35 standard. In the future, other standards such as RS-449, DS0, DS1 and ISDN (Integrated Services Digital Network) may be considered to take advantage of new transmission technology and to provide greater speed.

(b) ***Link Layer (Layer 2).*** The link layer is responsible for the transfer of data over the channel. It synchronizes the data to delimit the flow of bits from the physical layer. It also provides for the identity of the bits. It ensures that the data arrives safely at the receiving DTE. It provides flow control, mechanisms for detecting transmission errors, and and error-recovery mechanisms. For layer 2, NOP uses the X.25 Link Access Protocol Balanced (LAPB) standard.

(c) ***Network Layer (Layer 3).*** The network layer provides multiplexed, independently controlled virtual circuits between communicating systems. NOP uses X.25 (1980) switched virtual circuits for packet switching. For point-to-point operation without an intervening packet network, NOP uses ISO IS 8208, the DTE-to-DTE (data terminal equipment) variant of X.25.

(d) ***Transport Layer (Layer 4).*** The transport layer of NOP is not available for NSR27. The transport layer is supposed to provide the interface between the communications network and layers 5, 6, and 7, to isolate the user from some of the physical and functional aspects of the network. There is no transport layer in the current implementation of NOP.

(e) ***Session Layer (Layer 5).*** The session layer is supposed to provide dialog structuring and synchronization. There is no session layer in the current implementation of NOP.

(f) ***Presentation Layer (Layer 6).*** This layer provides the presentation transfer syntax. The presentation transfer syntax used is defined in CCITT Recommendation X.409 (identical to ISO DIS 8825 - ASN.1). X.409 also provides a precise specification notation for the application messages (also identically defined in ISO DIS 8824).

(g) ***Application Layer (Layer 7).*** The NOP application layer contains elements common to all applications and elements specific to applications. In the current implementation of NOP, this layer contains the ***Remote Operations Protocol.*** Remote operations are a way of structuring application-related dialogues. They are similar to high-level language procedure calls. Remote operations are defined in CCITT Recommendation X.410.

NOP is under continuing development, and requirements of some network elements are of a basic nature. The NOP minimum subset is a subset of full OSI. It involves substituting null protocols in some OSI upper layers where such protocols are not yet required. The NOP minimum subset meets the current requirements of all applications while creating a framework for future development.

3. DNC Applications

This part provides a brief description of the DNC applications. The applications are listed in Table 1-A with references to their associated NTP libraries for detailed information.

Business Network Management

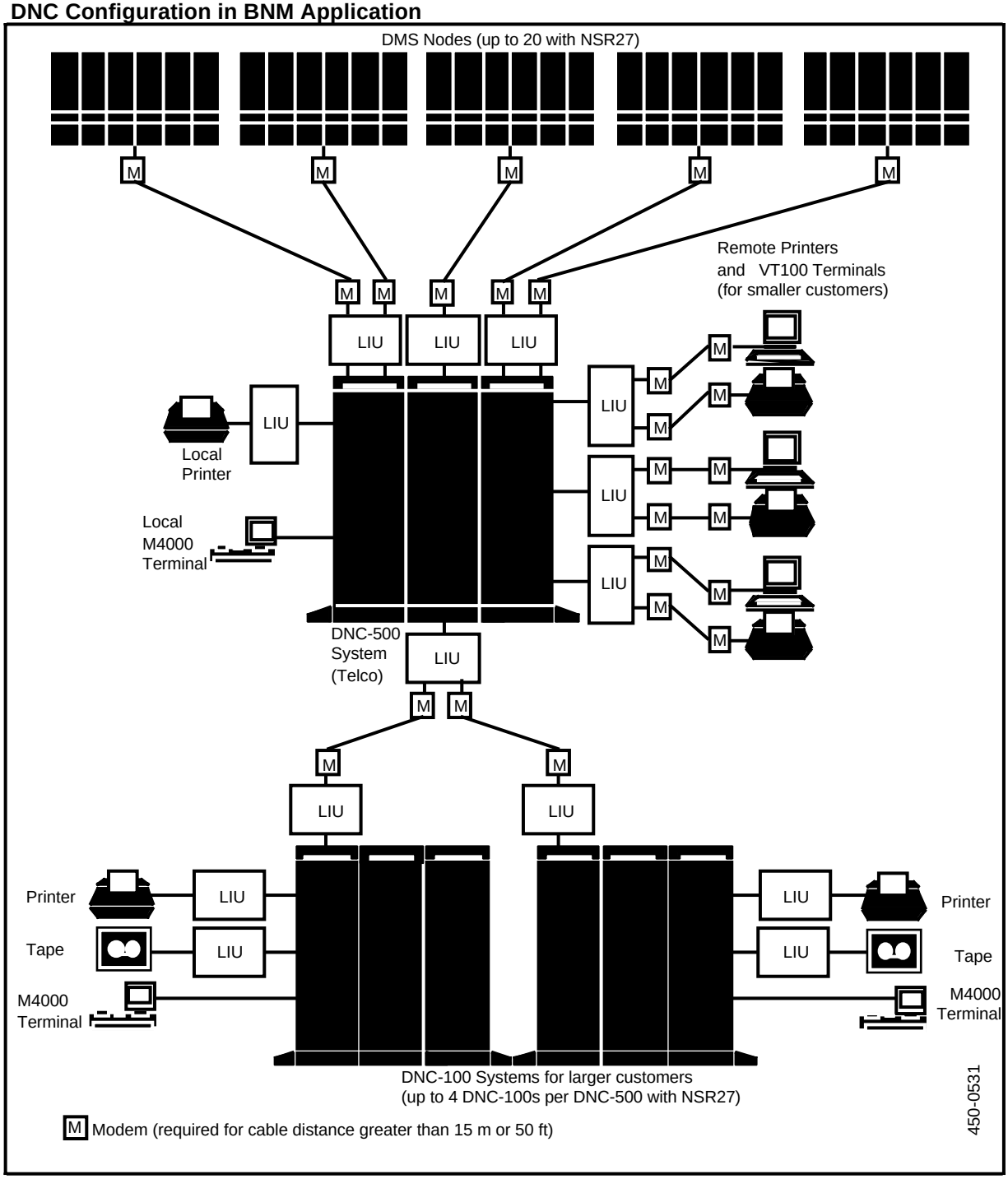
Business Network Management (BNM) enables businesses that buy Meridian Digital Centrex telephone services from a telephone operating company (telco) to manage some aspects of their telephone networks themselves, instead of relying completely on the telco. BNM helps these businesses to

- track and allocate communication costs
- detect and locate problems in their networks
- control and adjust their available communication services to meet the actual demand efficiently.

BNM also helps the telco to manage Meridian Digital Centrex networks on behalf of its customers.

Business Network Management runs on a DNC-500 on the telco's premises. The DNC-500 is connected to the DMS switch or switches from which the telco provides MDC service to its customers. The DNC-500 is also connected to DNC-100s or to remote terminals on customers' premises. A single DNC-500 can serve up to 64 customers. The configuration of DNCs for BNM is shown in Fig. 3-1.

Figure 3-1
DNC Configuration in BNM Application



DMS Service Control Point

DMS Service Control Point (DMS-SCP) is a system of hardware and software that supports databases for the centralization of network services, such as verification of credit card (billing number) calls and flexible 800-type call routing.

DMS-SCP is located in a CO environment, providing network processing to allow several DNC-500s and DNC-100s to communicate with DMS switches. DMS-SCP uses the same principles of distributed processing as the DNC-500/DNC-100 but has more processors and speed for the applications that require it.

DMS-SCP combines with DNC-500 systems to administer, operate, and maintain the network services databases. Fig. 3-4 shows the configuration of DMS-200 Traffic Operator Position System (TOPS) switches, DMS-SCPs and DNC-500s in a DMS-SCP network. The major elements in the network are:

(a) ***Switches.*** The DMS-200 TOPS switches initiate queries to the databases as part of their call processing operations.

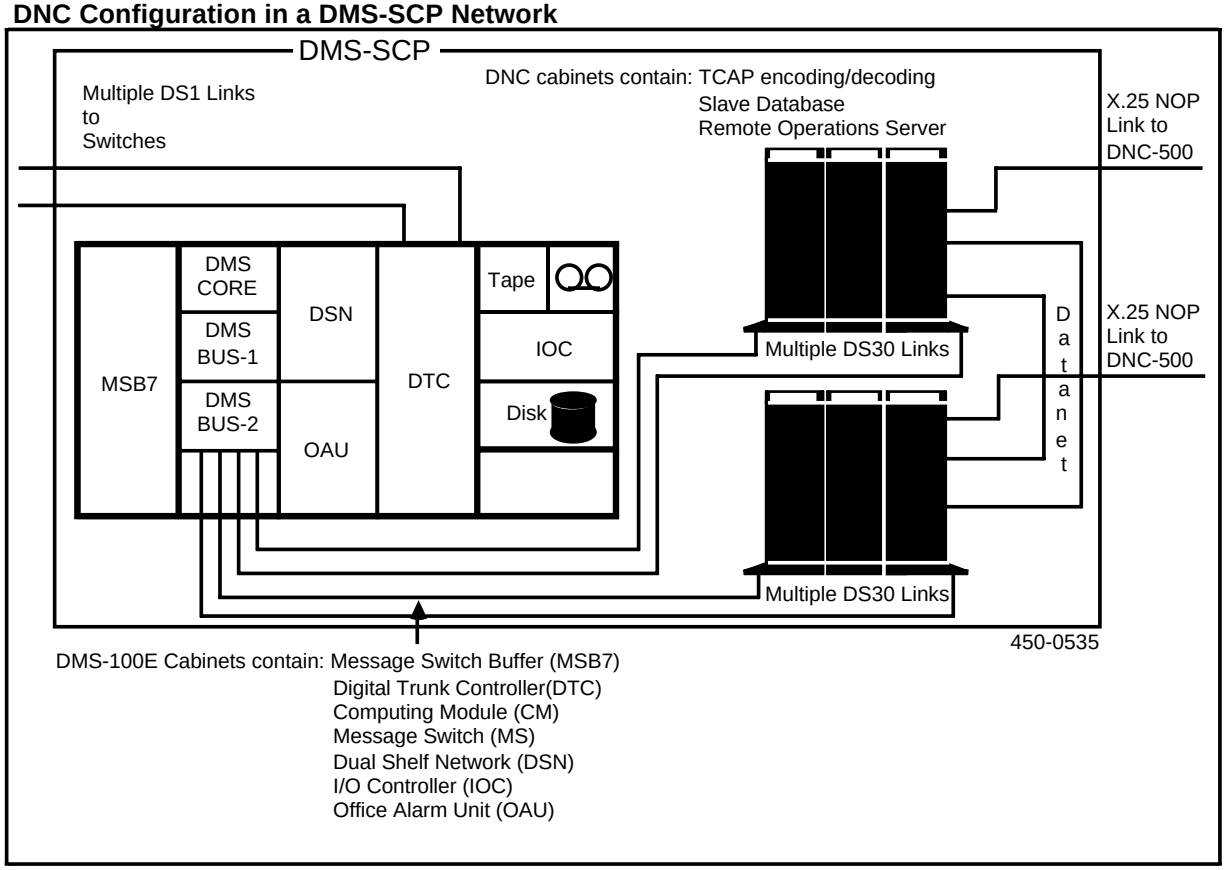
(b) ***DS1 Links.*** Each switch in the network communicates with each DMS-SCP in the network over a DS1 transmission link.

(c) ***DMS-SCP.*** There can be one or two DMS-SCPs in the network. Each switch in the network has its own link to each of the DMS-SCPs. The DMS-SCP processes the database query operations, and returns results to the switches. Each DMS-SCP stores a complete copy of all the DMS-SCP databases on hard disk. The DMS-SCP databases are the slave databases. Each DMS-SCP can update its database from one or more DNC-500 systems.

(d) ***X.25 NOP Links.*** Each DMS-SCP in the network is connected to a DNC-500 over a Network Operations Protocol (NOP) link.

(e) ***DNC-500.*** The DNC-500s in the network are the tools used by the customers to update and monitor their own portions of the slave database on the DMS-SCP. Each DNC-500 contains a master database which controls a portion of the DMS-SCP slave database. Customers update and maintain their master databases on their DNC-500, and the changes are propagated to the slave database on the DMS-SCP.

Figure 3-4
DNC Configuration in a DMS-SCP Network



Network Configuration Database

The Network Configuration Database (NCD) contains the configuration for a network, giving the logical and physical relationships between the network elements. On the DNC-100, the configuration information is displayed on the screens of the user interface.

The database is stored on the DNC-100 supplying the BNM application, but is called up by the other DNC-100s with other applications, as required.

4. Base DNC Services

This part describes the services available with the DNC systems. Not all applications use all the base DNC services. Consequently, some of the services described in this part may not be present in your system.

System Administrative Services

System Administrative Services (SAS) provides access to the base DNC software, available to two levels of user: the superuser and regular system administrators. (For detailed procedural information for SAS, see the Guide to System Administrative Services, 450-1011-301.)

The system administrator accesses SAS via the system's main menu. Selecting System Administrative Services displays the SAS menu of services.

> ***Note.*** System Administrative Services is only available to system administrators.

The System Administrative Services item in the main menu provides access to the following SAS functions:

(a) ***Set Date and Time.*** This feature allows you to set the date and time when the system is initialized for the first time and each time following reinitialization.

(b) ***Maintenance.*** This service monitors the system's operational status, and controls the service state of each hardware unit (SRU and RRU) and software unit (PRU) in the system. The system administrator uses this facility to check the current status of each device. The administrator can select an SRU, PRU, or peripheral device, and take any of the following actions:

- take it out of service
- run a test on it
- put it back into service.

(c) ***Configuration.*** The configuration service allows the system administrator to perform the following functions:

- Maintain the System Map, which identifies the address (physical location) of each hardware unit (SRU or RRU) and software unit (PRU) in the system for bus polling and communication.
- Add, delete, or change the sign-on name and password of any DNC user to ensure overall system security.
- Set up the operating parameters of applications resident on the system.

The configuration menus may be accessed in one of three modes: BROWSE (read-only mode), ON-LINE UPDATE (for making changes immediately), and SCHEDULED UPDATE (to be changed at a scheduled time in the future).

(d) ***Helix CI.*** This is the Helix Command Interpreter, used for various system support functions available only to the superuser. The functions include the batch configuration of ASCII devices and the running of special diagnostic tools.

(e) ***System Log.*** The System Log accessed through System Administrative Services is the base DVS log service. This service interacts with the DNC Log System, which is a separate service that consolidates the functions of of the DVS System Log service and adds additional capabilities. (See the description of the DNC Log System later in this part.).

The DVS System Log service generates a log for every event that relates to base DVS software. Most of these logs are passed on to the DNC log system, but a few are not. The logs retained by the DVS System Log must be accessed through SAS. (Those passed on to the DNC log system are accessed from the main menu, using the DNC Log Query screens.)

(f) ***Save and Restore.*** This service enables the system administrator to save and restore files to and from tape.

(g) ***Call Details and DV-Measurements.*** These services are reserved for future use.

The System Map

Each hardware and software unit (SRU, RRU, PRU and LIU port personality) must have its physical location defined in the system map as an address for bus polling and communications. PRUs are shown as part of the Applications Processor on which they reside. Port personalities are shown as part of the LIU on which they reside.

NT personnel do the initial system configuration when the system is installed. The system administrator must confirm this configuration on initialization (or reconfigure it as required) to ensure the appropriate addressing. When adding equipment or software to an existing system, the system administrator must enter the configuration data for the changes.

The configuration data should be stored in hardcopy form on the planning worksheets in the Site Records (450-1011-152).

The hardware and software units are represented in SAS as follows:

SRU Shared resource units are hardware units that plug into the cabinet shelves.

RRU Remote resource units are hardware units that are connected to LANlink ports. For SAS purposes, these include LAN Interface Units and M4000 terminals. (An LIU in turn interfaces with peripheral devices, such as modems, ASCII terminals, host computers, and printers).

PRU Program resource units are packages of software that are stored and executed within processor SRUs, and interact with other PRUs in the system.

PP Port personalities are packages of communications software stored and executed in an LIU, and are associated with a particular port type on the LIU.

User and Group Administration

The system administrator retains control of overall security by being able to add, change, or delete any user's profile as required.

A user profile identifies a user to the system and includes the user's name, a sign-on name and password for accessing the system, and internal DVS reference information, such as a user ID, group ID, and other information.

All users are assigned to one or more of 256 groups, numbered 0 through 255. Groups are associated with a specific set of functions and have their access restricted accordingly. Each group may have up to 50 user profiles. Two groups are defined by default when a system first starts up:

(a) Group 0 is the administrator's group. It contains the Superuser and the other system administrators. There is only one superuser in the system. The superuser has complete access to all system functions. Regular system administrators have some restrictions (for example, they cannot use the Utilities Service), but have access to most capabilities of SAS.

(b) Group 1 is the generic user's group. The group contains a set of default profiles that can be customized to serve the various needs of the DNC applications when creating new groups.

(c) The other groups are assigned to users according to the needs of the DNC applications.

System Access

Input/Output System

The Input/Output (I/O) system consists of programs that enable the I/O devices (such as the M4000-series terminals, external host computers, printers, and other devices) to communicate with the system. Input and output signals are routed through the I/O system, which provides a consistent format for communicating with the system. The I/O system provides:

- access security using passwords
- multiple terminal operation
- access to host computers
- formatting for writing data to reel-to-reel tape, in certain applications.

Users can communicate with the system using M4000 terminals or VT100-compatible ASCII terminals.

Man-Machine Interface

The software provides a man-machine interface (MMI) system of displays and softkeys (programmable key functions). The MMI is consistent across all applications and terminal types. However, the M4000 terminal makes more use of graphics, which the ASCII terminals approximate with ASCII characters.

Throughout all DNC practices, the textual references to hardkeys (identified with keytops) and softkey names are designated as follows:

Hardkeys The designated name is denoted by upper case, for example, ENTER or RETURN

Softkeys The designated name is denoted by mixed case bracketed by the less-than and greater-than symbols, for example, <Exit Service>.

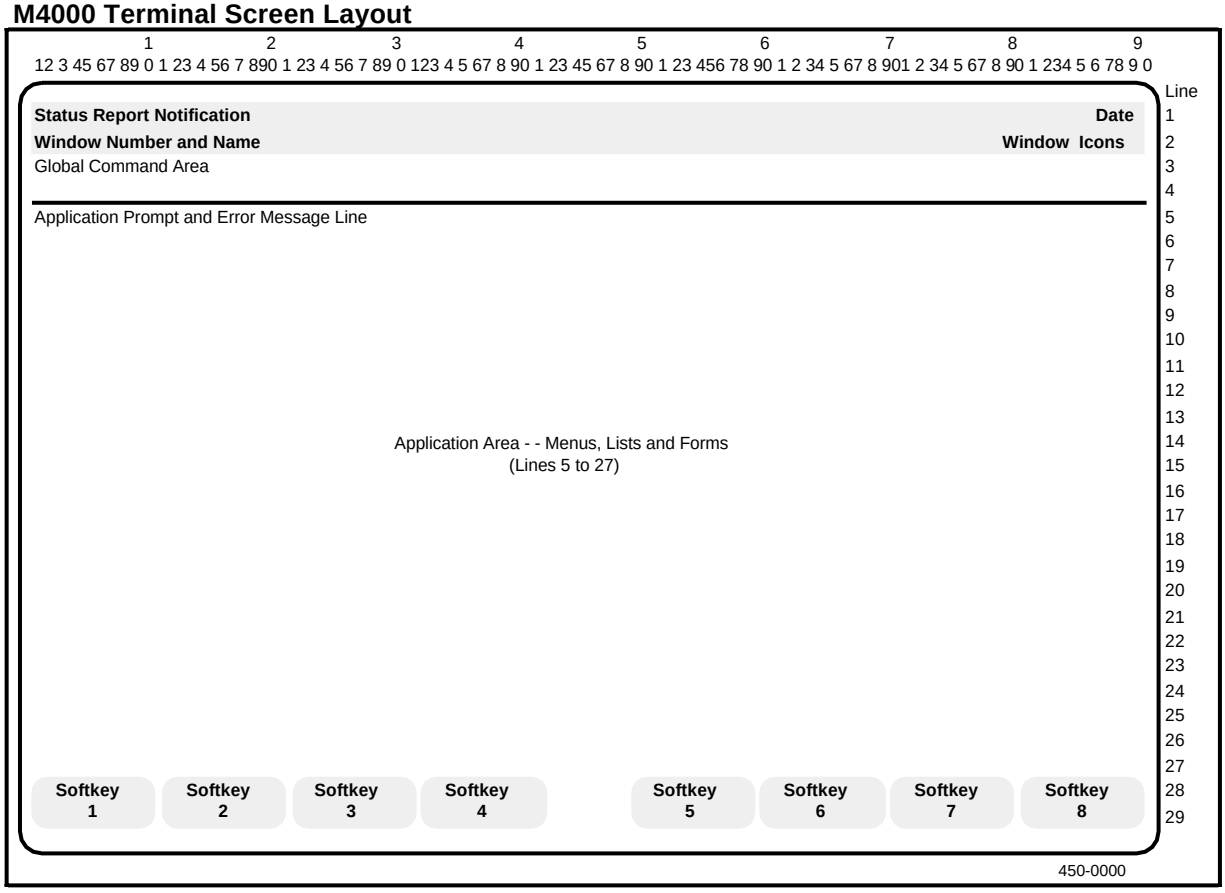
M4000 Terminals

The Meridian M4000 terminal serves as a local control console for accessing the system. It offers a keyboard with hardkeys labeled with the fixed functions of the DNC user interface, with single-keystroke command entry. Eight unlabeled keys are used to activate the softkey functions.

The M4000 connects to the system via a LANlink port. It uses a Teladapt cord to connect to a standard telephone wall jack, and communicates with the system over standard twisted-pair telephone wiring. It does not require modems to connect to the system, but must be located within 610 m (2000 ft) of the cabinets.

The screen is 90 characters by 29 lines in size, and supports graphics icons for an enhanced user interface. The screen layout for DNC system access is standardized across applications. (See Fig. 4-1 for the screen layout.)

Figure 4-1
M4000 Terminal Screen Layout



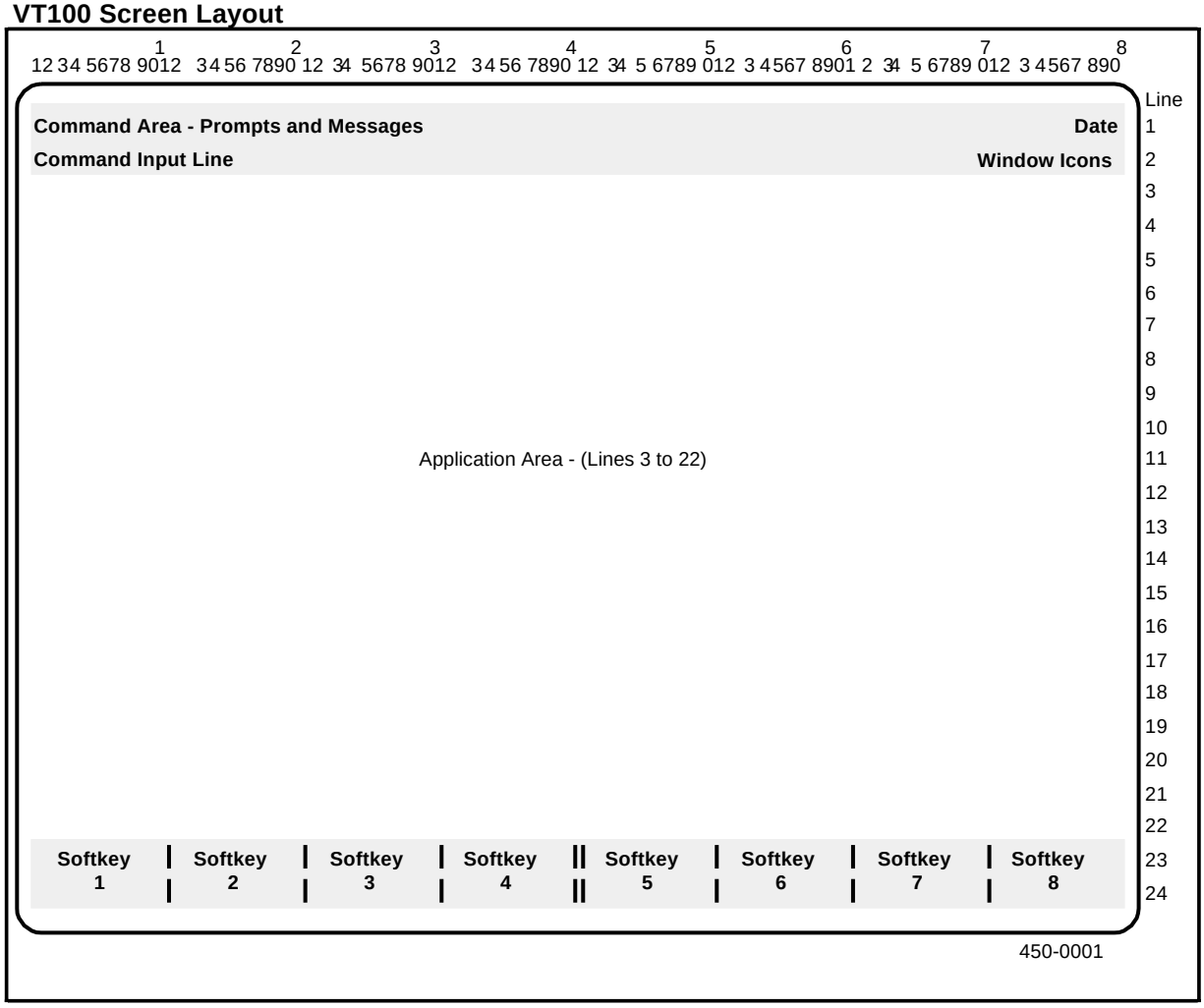
ASCII Terminal Access

In addition to the M4000 terminals, the DNC can be accessed by ASCII terminals compatible with Digital Equipment Corporation's VT100 terminal. Although ASCII terminals vary in terms of specific attributes, hardkeys, and display characteristics, the DNC system standardizes the displays as much as possible by basing the displays on the ASCII character set.

The ASCII screen displays approximate those of the M4000 terminals as closely as possible. ASCII terminals require a two-keystroke sequence for entering commands. These key sequences are equivalent to the single-keystroke commands of the M4000 terminal. (A keyboard map for executing M4000 commands on an ASCII console is provided in the Guide to System Administrative Services, 450-1011-301.)

The VT100 screen is 80 characters by 24 lines and provides for cursor addressability (that is, it allows full manipulation of the data on the screen using the cursor keys). Supported display attributes are blink, highlighting, reverse video and blank. The layout of the VT100 terminal screen is shown in Fig. 4-2.

Figure 4-2
VT100 Screen Layout



The ASCII terminal is connected to an LIU. The LIU is in turn connected to the system using twisted-pair wiring and a LANlink interface. Software uploaded to the LIU allows the ASCII terminal to interact with the DNC as if it were an M4000 terminal.

An RS-232-C cable connects the ASCII terminal to the LIU.

Alternatively, the ASCII terminal can be connected via a packet-switched network. In this case, there must be an X.3 packet asssembler/disassembler (PAD) device at the ASCII terminal, and the X.3 PAD and X.25 Gateway features must be configured in the DNC. (For information on these DNC features, see Parts 16 and 17 of the Guide to System Administrative Services, 450-1011-301.)

System Security

User Access and Security

User access and security defines the following:

- the users allowed to access the system, and their capabilities and restrictions
- the security parameters that apply to the entire system
- the main menu shown to a user when signed on.

SAS assumes that the customer has secured each operator console by:

- restricting physical access to local consoles
- using automatic dial-back modems for dial-up ASCII consoles.

Signing On

To access the system from a control console, the user must sign on with a valid sign-on name and password. For SAS functions, this sign-on name must be a designated system administrator's sign-on name. The system is initially configured with the following sign-on names and passwords for system administrators:

	SUPERUSER	**REGULAR ADMINISTRATOR**
Sign-on Names:	SUPERUSER	SYSADM00
Passwords:	SUPERUSER	SUPERUSR

The administrator should change the passwords as soon as possible when the system is first initialized.

Other Security Considerations

When planning physical security for terminals, the degree of security required will vary according to the customer's needs and the application. The following aspects of system operation should be kept in mind:

(a) Users can leave windows active, sign off, then sign on again using a different sign-on name. The user can then access the active windows, whether or not the new sign-on name normally allows access to them.

(b) On-line help can be accessed by pressing the HELP key even though the user has not yet signed on.

Save and Restore

The Save and Restore feature allows the DNC user to save application-related data on a tape cartridge. The user can then restore the data from the tape at a later time, instead of reentering it manually.

Only the application data is saved and restored with this feature. The system programs, application programs, and data are resident on tape supplied by Northern Telecom.

Backup Management System

The Backup Management System (BMS) lets DNC users save (back up) the contents of Mass Storage SRUs. Unlike Save and Restore, which gives users a menu from which they can choose individual files to be saved, BMS copies the entire contents of a Mass Storage SRU to tape. BMS also provides for incremental backups, that is, only those data blocks that have changed since the last backup.

Using the BMS Administrator Menu, the system administrator can configure backup policies (sets of rules) for each file server. These policies determine the conditions for saving files.

Users with backup operator passwords are prompted by BMS when a backup is required. Although only designated backup administrators can create, modify, and disable the policies, all users with backup passwords can display and print the policies, the list of backups to be done, and records of previous backups.

Restoring the data from the tapes requires the utility called DV1FSRESTORE. This utility is operated from the system administrator's console when rebooting the system.

DNC Log System

The DNC log system provides menu access to logs relating to system software. Logs are generated for each event in the DNC system, including both the base DVS and DNC software, and any applications and services operating on the system.

> ***Note:*** The DNC Log System is interactive with the base DVS System Log service, which generates the logs against base DVS software. Most base DVS logs are passed on to the DNC log system, but a few are retained by the DVS System Log, and must be accessed through SAS.

In the DNC log system, logs are assigned a descending severity value from 1 to 16. Those with severity values of 1, 2, or 3 are considered critical, major, or minor faults requiring alarms. These logs are screened from the log system and passed to the alarm system.

Logs that are accepted are recorded in a history file on the disk of the Mass Storage SRUs associated with the Primary Processor. The history file is circular; it holds a configurable number of logs and beyond that, each new log overwrites the oldest existing log record.

Using a man-machine interface (MMI), users can query the log file and display or print the messages corresponding to the logs. These messages are available in up to three languages (English, French, and Spanish). System administrators can select the language and edit the messages.

When displayed, log messages appear in the notification area of the terminal. The classes of log received by each user is set by the system administrator.

Logs can also be routed to other DNC systems. Logs are assigned a time, date, and severity which can be passed to the destination system. A fail-safe system ensures that logs are saved if the destination log system is unavailable.

Alarm System

The alarm system provides error detection and a mechanism to signal those errors. The detection system includes:

- a resource manager which informs the alarm system of all PRUs/SRUs/RRUs which change from working to faulty condition and from loading to working condition (usually a fault recovery)
- disk query that compares the amount of free disk space to a configurable threshold with a configurable frequency
- DNC application programs that detect faults in their operation
- the log system that passes high severity logs as errors

The signal devices include:

- every terminal that has a notification area reserved for alarm messages
- a designated terminal that can sound a speaker tone
- an alarm interface unit (ALIU) including LEDs for critical, major, and minor alarms plus an alarm cut-off`(ACO) button.

The ALIU (Fig. 4-3) can be linked to the central office alarm system, so that whenever an alarm condition occurs, the visual and audible alarms in the central office alarm system are activated (see Fig. 4-4).

The alarm system records alarms in a circular alarm history file. Using the alarm query MMI, system administrators can:

- display alarm records
- print alarm records
- cut off audible alarms using a softkey
- change the cut off alarms from the active to the pending state so that they can be cleared
- clear pending alarms.

All other users who have access to the alarms MMI can display and print the alarms common to all users and those available to their group.

As with the log system, the alarm message is displayed by the notification server according to the group ID and userID.

Figure 4-3
Front Panel of an Alarm Interface Unit (ALIU), Installed in the Option Slot of an LIU

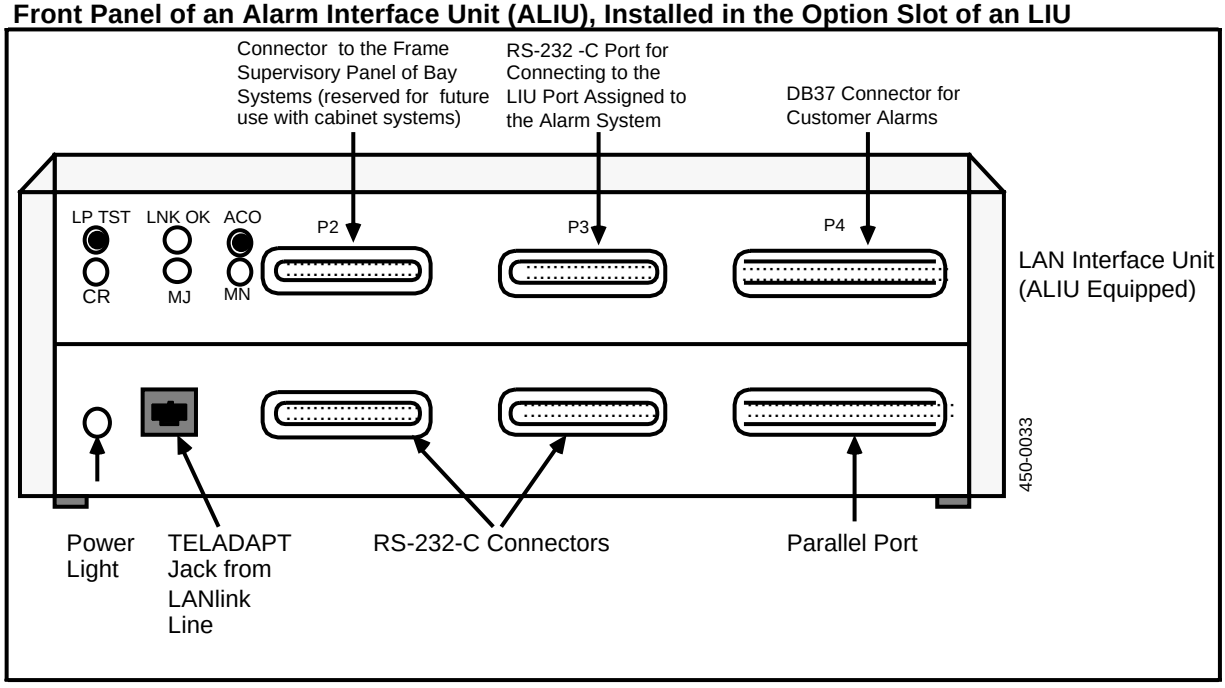
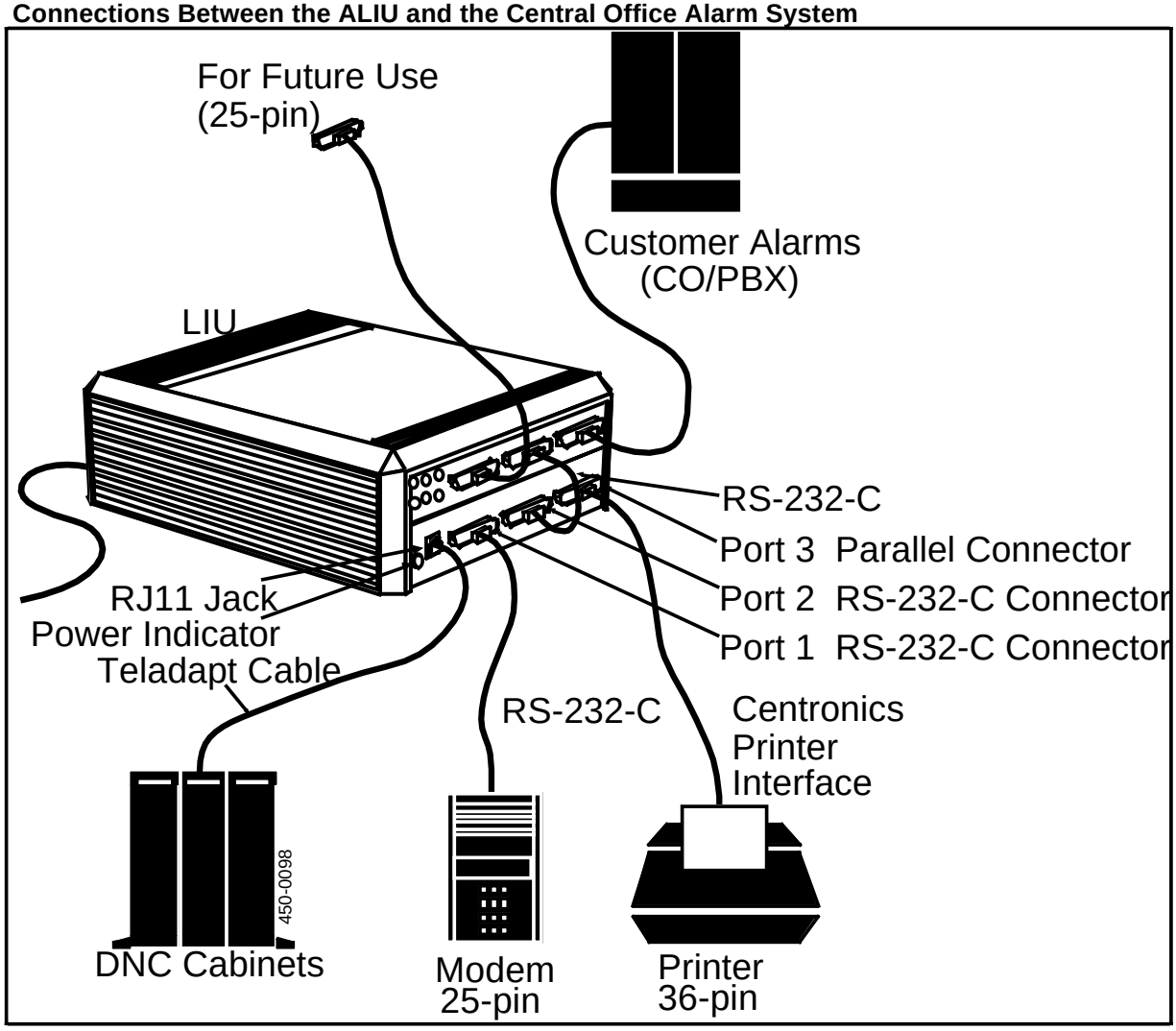


Figure 4-4
Connections Between the ALIU and the Central Office Alarm System



Printer Administration

The printer port configuration screens allow the system administrator to gain an overall view of the printers configured on the system. The screens still allow for new devices to be attached.

In DNC, each LIU being used for a printer port is uploaded with a copy of LIU Port - Printer Port. These ports are listed on the printer ports screens with the cabinet, slot (of LANlink), line and port of each printer identified.

The printers are divided into groups. Each group has its own characteristics, such as baud rate. The system administrator can assign similar printers to the same group, then adjust the group characteristics as a whole unit.

Similarly, a system administrator can control printers using queues for the jobs sent to those printers. The printers have to have been configured before any queues can be administered for them. The system administrator can:

- assign a printer class for each printer (thus defining some of the printer's characteristics, such as interface type)
- add a queue to a list of available queues
- assign an available queue to a printer
- delete a queue from a list of available queues
- unassign an available queue from a printer
- edit a queue to change its users or administrator.

X.25 Gateway

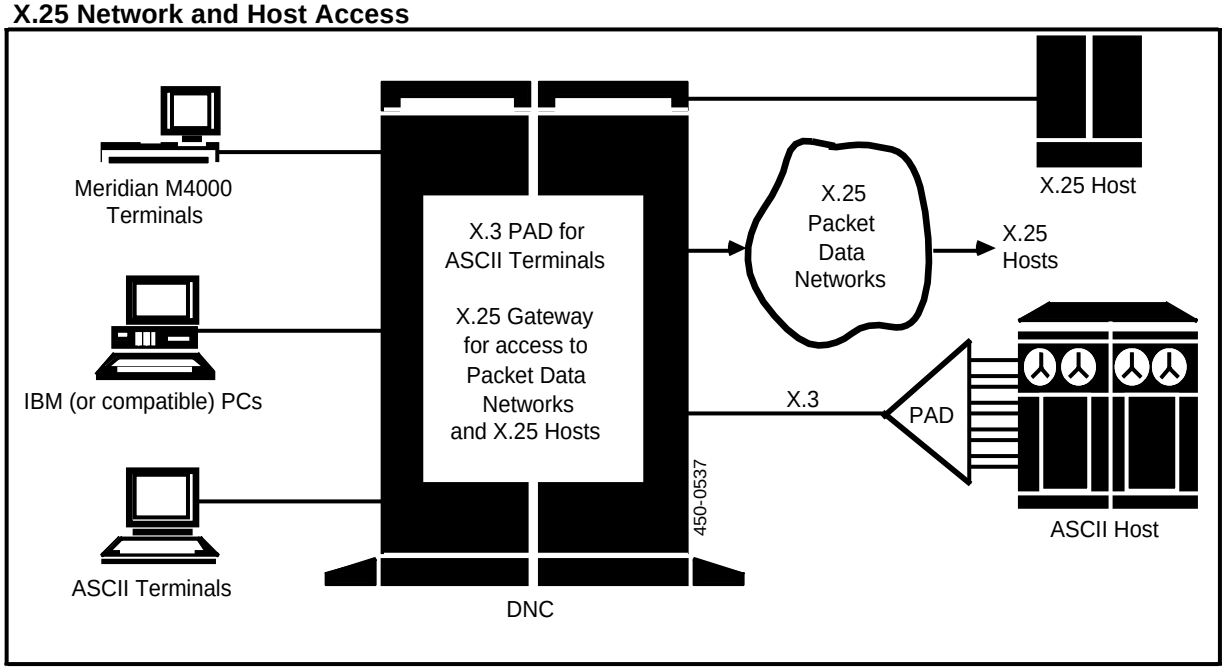
The X.25 Gateway is a base DVS service that provides access to packet switched data networks based on the X.25 Recommendation of CCITT. DNC systems also use the X.25 Gateway to implement the Network Operations Protocol (NOP), which is a Northern Telecom-proprietary protocol for network communications. (See Part 2 for a description of NOP.)

> ***Note:*** If a DNC is to access a packet switched data network, it needs both an X.25 Gateway and an X.3 PAD. NOP connections do not require X.3 PAD.

X.3 PAD

The X.3 Packet Assembler/Disassembler.(X.3 PAD) provides terminal access to packet-switched X.25 networks. The X.3 PAD allows the terminal (ASCII or M4000) to access an X.25 gateway. Each X.3 PAD supports up to 16 terminals; each X.25 gateway supports up to 64 simultaneous terminal sessions. Fig. 4-5 shows a configuration of the X.25 network and host access.

Figure 4-5
X.25 Network and Host Access



Local Data Net

Local Data Net is a means of interconnecting DNC systems in a ring topology using twisted-pair telephone wiring. The link supports full duplex communication between DNCs, with an aggregate data rate of 2.5 Mb/s.

Using a ring topology, packets can be transferred from each Local Data Net SRU to the next link while other packets travel in the opposite direction. Should any link fail, the packets can be routed around the remaining network to reach their destination.

Multiple networks of DNC systems can be linked using a common system with a Local Data Net SRU for each of the two networks. Local Data Net networks can also be configured in a line, with reduced performance and reliability. (The line configuration is used when the last node in the network is located more than 610 m (2000 ft) from the nearest node.)

3270 Emulation

The 3270 Emulation Service allows the DNC to imitate an IBM 3274-1C or 3274-51C cluster control unit and 3278 display stations. A DNC user with an M4000 or an ASCII terminal can use 3270 Emulation to access an Operational Support System (OSS), or other IBM host compatible with the 3270 family of products. The terminal imitates the functions and displays of an IBM terminal. (A list of supported and unsupported 3274 control unit features is provided in the Guide to System Administrative Services, 450-1011-301.)

The physical connection between the DNC and the host is made via an RS-232-C connection on an LIU equipped with the appropriate software for protocol conversion.

There are two types of cluster controller emulator (CCE):

- SNA, for hosts operating in SDLC protocol
- BSC, for hosts operating in bisynchronous protocol.

Up to 32 CCEs, of mixed SNA and BSC, can reside on an Applications Processor SRU, but only one of them may be active at any one time on the same SRU. Two CCEs may be active at the same time on different Applications Processors. (A CCE must be active before it can be used to access its host.) The inactive CCEs can be used as ‘standby’ CCEs, ready to access a different host when the currently active CCE is deactivated.

3780 Remote File Transfer

The 3780 Remote File Transfer (RFT) service provides batch file transfer between a local DNC file server system and remote hosts or terminals. The service emulates IBM's 3780 BSC protocol. The physical link for 3780 RFT is a half-duplex RS-232-C connection.

Up to 16 ‘logical hosts’ can be configured per file server. That is, up to 16 transmission paths for 3780 RFT are identified by host names. These can be separate paths to one or more remote hosts or terminals.

Only two of the paths can transmit or receive at any time. Those two host names are configured as active by the system administrator using the SAS 3780 RFT Configuration Utility. The remaining host names, configured as inactive, can be reconfigured as active if a path is available or one of the active host names is made inactive.

The local DNC controls the file transfers. The DNC assigns a separate queue for each host name, containing jobs (file transfers) to be sent to or received from that host name when it is active. All jobs received from the logical hosts are written directly on the file server's hard disk; there are no receive queues.

A job can be up to six files concatenated for a single transfer; a queue supports up to 256 jobs (to a maximum of 100 jobs times the number of active queues). Host names made active have their queues restored and jobs transmitted. Host control commands can be included with a job that will route the transfer through the remote host to another host on its network.

Log messages generated by 3780 RFT are written to the 3780 RFT log file which can be purged when full. This log file is separate from the DNC log system. Some of the messages, such as responses to commands, are sent to the user's terminal or a system printer.

5. Maintenance

Routine Maintenance

In addition to the menu-driven functions of System Administrative Services (SAS), the system administrator is responsible for the following maintenance functions that may be required on a periodic basis:

- creating backup tapes for data (see the Guide to System Administrative Services, 450-1011-301)
- cleaning the air filters in the cabinets (see the Maintenance and Troubleshooting Guide, 450-1011-501)
- cleaning the tape heads in the tape drives (see the Maintenance and Troubleshooting Guide, 450-1011-501).

Periodically, the Save and Restore feature can be used to save application-related data on tape as a database backup. The data can then be reloaded from tape instead of being input manually.

Air filters require periodic cleaning to ensure proper flow of cooling air from the fans. Filters used at the bottom of cabinets may be vacuumed or replaced.

Tape heads on the tape units should be cleaned on a periodic basis to ensure proper operation. They should also be cleaned after the first use of a new tape.

Fault Location and Recovery

When the system is not responding in the correct manner, consult the Maintenance and Troubleshooting Guide, 450-1011-501, which provides troubleshooting procedures to determine the most probable cause and the recommended action to be taken. The faulty units should be tested and, if a fault persists, the faulty SRU or RRU replaced. Faults may be indicated by messages displayed in the:

- primary processor display window
- log history file
- alarm history file
- notification area of the terminal screen.

Faults in a PRU or SRU can often be cleared by courtesying it down, then putting it back into service.

In cases where disk data has been corrupted, it may be necessary to reload the system. The procedure for this is detailed in the Guide to DNC Base Software Installation, 450-1011-302.

6. Specifications

The following are general specifications that apply to the DNC system regardless of application. The exact system configuration depends on the application for which the DNC is being used (see the appropriate NTP for the application).

DNC System Specifications (SASI)

Environmental Requirements

Temperature, Operating:	10℃ to 35℃
Temperature, Non-operating:	-30℃ to 55℃
Humidity, Operating:	20° to 80%
Humidity, Non-operating:	5% to 90%
Atmospheric Pressure:	785 mm-522.2 mm (30.9 in. -20.56 in.) Hg. (about 1000 ft BSL to 10,000 ft ASL.)
Thermal Gradient (Max):	10℃ per hour
Heat Dissipation:	819 BTU per hour per cabinet

Vibration

Frequency range:	15 to 200 Hz
Acceleration level:	0.20 g
Force application:	3 axis

Floor Loading

Weight, fully equipped cabinet:	91 kg (200 lb) or less

Accoustic Noise

at 1.2 m from cabinet:	-45 dBA

Power Requirements

Voltage, 2-4 cabinets:	110 V ac (97.5 V-126.5 V), or 220 V ac (187 V-242 V)
Voltage, 5-8 cabinets:	220 V ac (187 V-242 V)
Outlet, 110 V:	NEMA 5-15, 2-pole, 3-wire, duplex
Outlet, 220 V:	NEMA 16-20, 2-pole, 3-wire, single
Hertz:	60Hz, ±20%
Demand:	240 W or less, full cabinet
Power Cord:	2.74 m (9 ft), grounded
Grounding:	No grounding straps are required for cabinet systems

Telephone Wire

Gauge:	24 AWG
Loop Resistance:	51.9 Ω per 305 m (1000 ft) or less
Recommended Type:	Polyolefin Insulated

DNC System Specifications (SCSI)

Environmental Requirements

Temperature, Operating:	0℃ to 40℃
Temperature, Non-operating:	-40℃ to 70℃
Humidity:	5% to 95% non-condensing
Atmospheric Pressure:	85 mbar @ -40°C (non-operating), 650 mbar @ 0℃ (operating)
Thermal Gradient (Max):	1°C per minute

Vibration

Frequency range:	5 to 200 Hz
Force application, Operating:	0.5 g for two hours on each axis
Force application, Non-operating:	1.5 g for 30 minutes on each axis

Floor Loading

Weight, fully-equipped cabinet:	91 kg (200 lb) or less

Accoustic Noise

at 1.2 m from cabinet:	-45 dBA

Power Requirements

Voltage, 2-4 cabinets:	110 V ac (85 V-140 V) or 220 V ac (170 V-264 V)
Voltage, 5-8 cabinets:	220 V ac (170 V-264 V)
Outlet, 110 V:	NEMA 5-15, 2-pole, 3-wire, duplex
Outlet, 220 V:	NEMA 16-20, 2-pole, 3-wire, single
Hertz:	60 Hz (47-63 Hz)
Max. Demand per SRU:	40 W per quarter-wide shelf
Power Cord:	2.74 m (9 ft), grounded
Grounding:	No grounding straps are required for cabinet systems

Telephone Wire

Gauge:	24 AWG
Loop Resistance:	51.9 Ω per 305 m (1000 ft) or less
Recommended Type:	Polyolefin Insulated

M4000 Terminal

Power Requirements

Voltage:	110 V ac (97.5 V-126.5 V)
Current, Max:	1.7 A rms, 2 A fuse
Power:	75 W
Power Cord:	3 m (10 ft), grounded

LAN Interface Unit

Power Requirements

Voltage:	110 V ac (97.5 V-126.5 V)
Current, Max:	1 A rms, 2 A fuse
Power:	43 W
Power Cord:	1.52 m (5 ft), grounded

450-1011-100
NSR27
02
Standard
May 12, 1989
Canada