Critical Release Notice

Publication number: 297-2663-340
Publication release: Standard 02.04

The content of this customer NTP supports the SN06 (DMS) software release.

Bookmarks used in this NTP highlight the changes between the baseline NTP and the current release. The bookmarks provided are color-coded to identify release-specific content changes. NTP volumes that do not contain bookmarks indicate that the baseline NTP remains unchanged and is valid for the current release.

Bookmark Color Legend

Black: Applies to new or modified content for the baseline NTP that is valid through the current release.

Red: Applies to new or modified content for NA017 that is valid through the current release.

Blue: Applies to new or modified content for NA018 (SN05 DMS) that is valid through the current release.

Green: Applies to new or modified content for SN06 (DMS) that is valid through the current release.

Attention!
Adobe® Acrobat® Reader™ 5.0 is required to view bookmarks in color.

Publication History

March 2004

Standard release 02.04 for software release SN06 (DMS).

Change of phone number from 1-800-684-2273 to 1-877-662-5669, Option 4 + 1.

297-2663-340

Digital Switching Systems

DMS-500

TCP/IP Application Guide

LLT00008 and up Standard 02.03 August 1998

NORTEL

NORTHERN TELECOM

Digital Switching Systems

DMS-500

TCP/IP Application Guide

Publication number: 297-2663-340
Product release: LLT00008 and up
Document release: Standard 02.03
Date: August 1998

Printed in the United States of America

Publication history

August 1998

Standard release 02.03 up–issued to reflect software release LLT00008 and up.

April 1998

Standard release 02.02 for software release LLT00008.

January 1998

Preliminary release 02.01 for software release LLT00008.

December 1997

Standard release 01.02 for software release LLT0B007.

August 1997

Preliminary release 01.01 for software release LLT0B007.

Contents

About this document **ix**
References to unsupported features x
Who needs this manual? x
How is this manual arranged? xi
Where does this manual fit in the document suite? xii
What software release does this manual apply to? xii
How to understand document numbers xii
How to determine the latest version xiii
What documents are referred to in this manual? xiii
Document conventions xiv
Input prompt (>) xiv
Commands and fixed parameters xiv
Variables xiv
Optional variables and parameters xiv
Responses xiv
Illustrations in figures xv
Numbering ranges for dialing plans xvi
What precautionary messages mean xvi

Overview of TCP/IP **1-1**
Introduction to the Internet and TCP/IP 1-1
What is the Internet? 1-1
Brief history of the Internet and TCP/IP protocols 1-2
Important features of TCP/IP 1-2
Open protocol nature, standards available to all 1-2
Computer hardware independence 1-3
Network hardware independence 1-3
Common addressing scheme 1-3
Standard high-level protocols 1-3
TCP/IP protocol suite 1-3

TCP/IP on the DMS-500 switch **2-1**
Benefits of using TCP/IP 2-1
Features of TCP/IP 2-1
ISO data communications model 2-2
OSI Reference Model (seven layers) 2-2
How TCP/IP relates to the seven OSI layers 2-2
TCP/IP architecture (four layers) 2-3
Applications layer: FTP, Telnet, and RIP 2-3
Transport layer: TLI, TCP, and UDP 2-4

Network layer: ARP, IP, and ICMP 2-5
Data Link layer: GNI, SNAP, and Ethernet 2-7

Ethernet interface unit 3-1
Overview 3-1
Ethernet connectivity 3-1
EIU software 3-2
EIU hardware 3-2
Integrated PBus and FBus card 3-3
Ethernet Interface Card 3-3
Ethernet Interface Paddleboard card 3-3
Address allocation 3-4
IP addresses 3-4
Media Access Control addresses 3-7
EIU maintenance 3-8
Summary of EIU features 3-8
Central and local maintenance 3-9
MAC layer services 3-9
Maintenance Fault Insertion Test 3-10
DCP central control 3-10
EIU protocols 3-10
Internet protocol throttling 3-10
Internet dynamic routing 3-11
LAN maintenance 3-11
LAN management from IOC MAP 3-11
Live office network datafill changes 3-11

Using FTP at the switch 4-1
Who uses FTP? 4-1
Definition of FTP 4-1
Client and server programs 4-1
Filename conventions 4-3
DMS-500 switch supported FTP commands 4-3
Using basic DMS-500 FTP client functionality 4-4
Establishing an FTP session from the DMS-500 switch 4-4
Entering the host's userid and password 4-5
Finding out where you are 4-5
Determining which files are in your directory 4-6
Changing to another directory at remote host 4-7
Changing to another directory locally 4-7
Getting an ASCII text file from the remote host 4-8
Putting an ASCII text file onto the remote host 4-9
Getting a binary file from the remote host 4-9
Putting a binary file to the remote host 4-10

Using Telnet at the workstation 5-1
Who uses Telnet? 5-1
Definition of Telnet 5-1
Client and server programs 5-1
Telnet architecture 5-2
Telnet features 5-3

Remote MAP access 5-3
EIU/Telnet enhancements 5-4
Using basic DMS-500 Telnet functionality 5-4
Establishing a Telnet session from the workstation 5-4
Logging into Telnet 5-6
Logging out from Telnet 5-6

Table datafill **6-1**
Datafill guidelines 6-1
Calculate TCP connections and configure CM and EIU 6-1
Datafill sequence 6-3
Datafilling table LIUINV 6-4
Datafilling table IPNETWRK 6-6
Datafilling table IPHOST 6-7
Datafilling table IPROUTER 6-8
Datafilling table IPPROTO 6-9
Datafilling table IPTHRON 6-10
Datafilling table RMCONFIG 6-12
Datafilling table ENSITES 6-13
Datafilling table ENTYPES 6-13
Datafilling table EXNDINV 6-15

Operations management **7-1**
OMs 7-1
Logs 7-1
Alarms 7-2
Restrictions 7-2

List of abbreviations **8-1**

Appendix A Frequently asked questions **9-1**
What is TCP/IP? 9-1
When do I use FTP and when do I use Telnet? 9-1
Why do I need to have both a MAC address and an IP address? 9-1
Who administers the MAC addresses? 9-1
How is the TCP/IP functionality activated? 9-2
Can I use FTP to upload table information from a remote workstation? For example, can I upload ANI information to table ANISCUSP? 9-2

Appendix B Ordering information **10-1**

About this document

This document describes TCP/IP architecture and explains how your computer uses Telecommunications Network (Telnet) and File Transfer Protocol (FTP) to connect to and access the Ethernet Interface Unit (EIU) located in the DMS-500 switch.

CAUTION

Assigned EIU address must be obtained from Northern Telecom

Before connecting the cable to the EIU circuit board, the customer site must obtain the unique Ethernet address assigned by Nortel (Northern Telecom).

A unique Ethernet address is assigned to each EIU via table-control datafill in the DMS-500 Core. (Hereinafter, when this document references the "DMS-500 switch" or simply "switch," it refers to DMS-500 Core.)

When a customer buys a circuit board, this assigned address must be provided by Nortel. This document describes how to obtain that address, the kind of cable to be used, and how to connect it. It illustrates the cards and the slots in which they are placed, and covers EIU installation and security issues.

This document provides information about table datafill as it relates to TCP/IP for the DMS-500 switch. Only those operational measurements and logs that relate to TCP/IP are presented. Therefore, a data field that has many entry options will show only those that pertain to TCP/IP.

For information on how data tables, operational measurements, and logs support other applications, refer to the appropriate documents listed in "What documents are referred to in this manual?"

References to unsupported features

Beginning with software release LLT00009, you will find references to the following **unsupported** hardware, applications, and features in some of the DMS-500 documentation:

- Series 20-50 Processor
- Mixed Memory
- MSB7
- INODE
- Billing Server (AP/FP)
- EOPS
- FlexDial
- SL-100 Integrated Peripheral Equipment (IPE) digital phone
- AFT (will be available with SDM on SDMC11)

DMS-500 software is made up of local features of DMS-100 and long-distance features of DMS-250. The NTPs, and other technical documents issued with each software release, include information on new software features and new hardware introduced with the release. NTPs that do not require revisions, but are still pertinent to the DMS-500 switch, are also included with each release.

Note: Although documentation or references appear in the NTPs, the features, applications, and hardware listed above are **unsupported** on the DMS-500 switch.

Who needs this manual?

This manual is for personnel who are responsible for setting up, administering, and maintaining the DMS-500 switch**.**

To use this manual fully

- Ensure the DMS-500 switch you are working with is installed, commissioned, and active.
- Receive Nortel (Northern Telecom)-approved training for Table Editor, datafill, translations, and maintenance.

How is this manual arranged?

The information in this manual is arranged as follows:

Chapter 1, Overview of TCP/IP

Chapter 1 provides an overview of TCP/IP communication protocols.

Chapter 2, TCP/IP on the DMS-250 switch

Chapter 2 describes the benefits and features of TCP/IP on the DMS-500 switch.

Chapter 3, Ethernet interface unit

Chapter 3 describes how Ethernet LAN connectivity is established, software and hardware, and address allocation.

Chapter 4, Using FTP at the switch

Chapter 4 defines FTP and explains how to use FTP commands on the DMS-500 switch.

Chapter 5, Using Telnet at the workstation

Chapter 5 defines Telnet and explains how to use Telnet commands on the DMS-500 switch.

Chapter 6, Table datafill

Chapter 6 contains guidelines for table datafill.

Chapter 7, Operations management

Chapter 7 explains pertinent operational measurements (OM), logs, alarms, and restrictions.

Chapter 8, List of abbreviations

Chapter 8 provides a list of abbreviations used in this manual and their meanings.

Appendix A, Frequently asked questions

Appendix A provides answers to frequently asked questions regarding TCP/IP.

Appendix B, Ordering information

Appendix B contains information on how to order Nortel (Northern Telecom) Publications (NTPs) and Product Content Loads (PCLs).

Where does this manual fit in the document suite?

This manual is written specifically for the DMS-500 switch and is part of a suite of documents for the DMS-500 switch. The documentation suite for DMS products reflect the common architecture of the DMS software. This suite includes application guides and reference guides. Application guides provide information on specific DMS-500 features and products. Technical reference guides contain information about logs, commands, operational measurements, and office parameters that are common to the DMS family. The *DMS-500 Master Index of Publications*, 297-2663-001, explains how the documentation suite for the switch is organized.

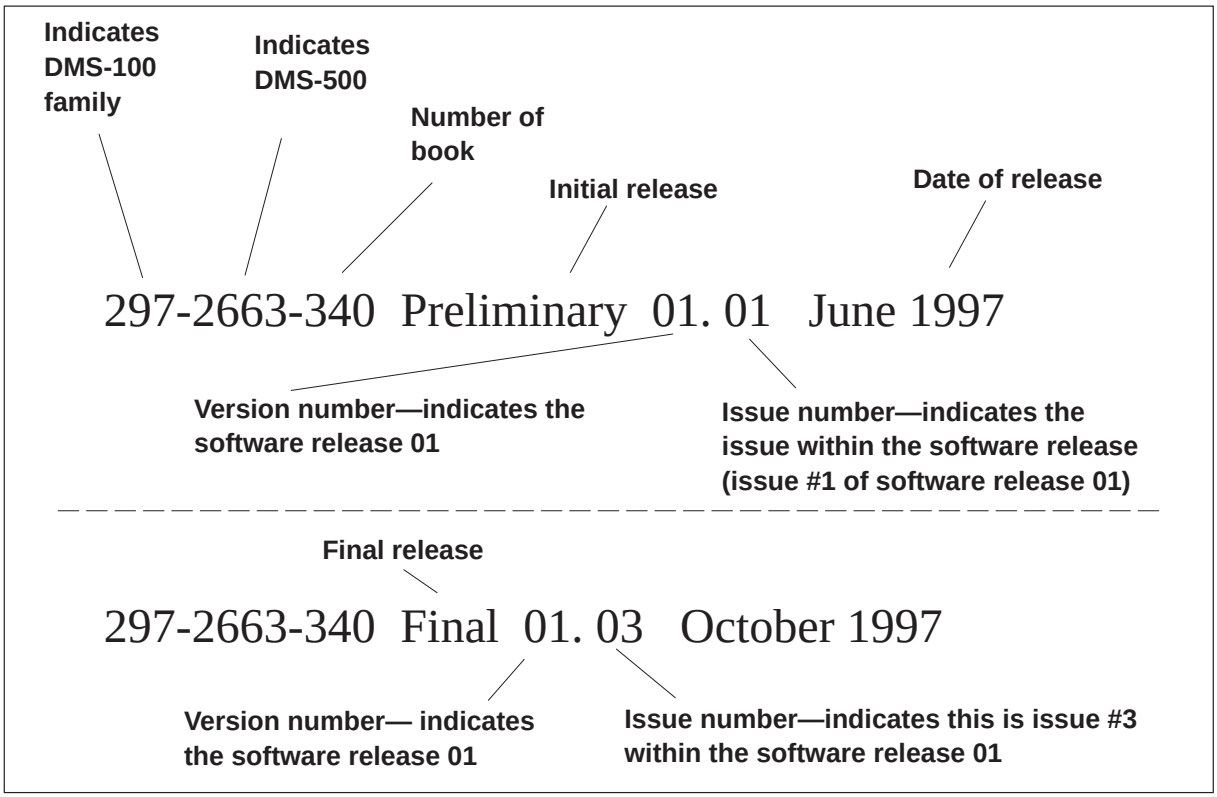
What software release does this manual apply to?

This manual applies to DMS-500 offices that have software release LLT00008 and up. Unless revised, this manual also applies to offices with software releases later than LLT00008 and up.

How to understand document numbers

As shown in the following graphic, the document naming and numbering indicates:

- the document number consisting of the family (297—for DMS family), the product (2663—for DMS-500), and the type of book (last three digits of document number)
- the release (preliminary or final)
- the software release version and the issue number within that release (01.01)
- the date the document was released



How to determine the latest version

More than one version of this manual may exist. To determine whether you have the latest version of this manual, check the release information in the *DMS-500 Master Index of Publications*, 297-2663-001.

What documents are referred to in this manual?

The following documents are referred to in this manual:

- *DMS-500 Data Schema Reference Manual,* 297-2663-851
- *DMS-500 Logs Reference Manual,* 297-2663-840
- *DMS-500 Operational Measurements Reference Manual,* 297-2663-814

Information about related documents can be found in either the *DMS-500 Master Index of Publications*, 297-2663-001, or the *Product Documentation Directory,* 297-8991-001.

Document conventions

This document conforms to the following conventions.

Input prompt (>)

An input prompt (>) indicates that the information that follows is a command:

>BSY

Commands and fixed parameters

Commands and fixed parameters that are entered at a MAP terminal are shown in uppercase letters:

>BSY CTRL

Variables

Variables are shown in lowercase letters:

>BSY CTRL ctrl_no

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

Optional variables and parameters

Optional variables and parameters are shown in brackets ([ ]):

>SS setname [INSVSYNC]

Optional variables and parameters shown in brackets use the syntax described above. Each optional variable or parameter is explained in a list that follows the command string.

Responses

Responses correspond to the MAP display and 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

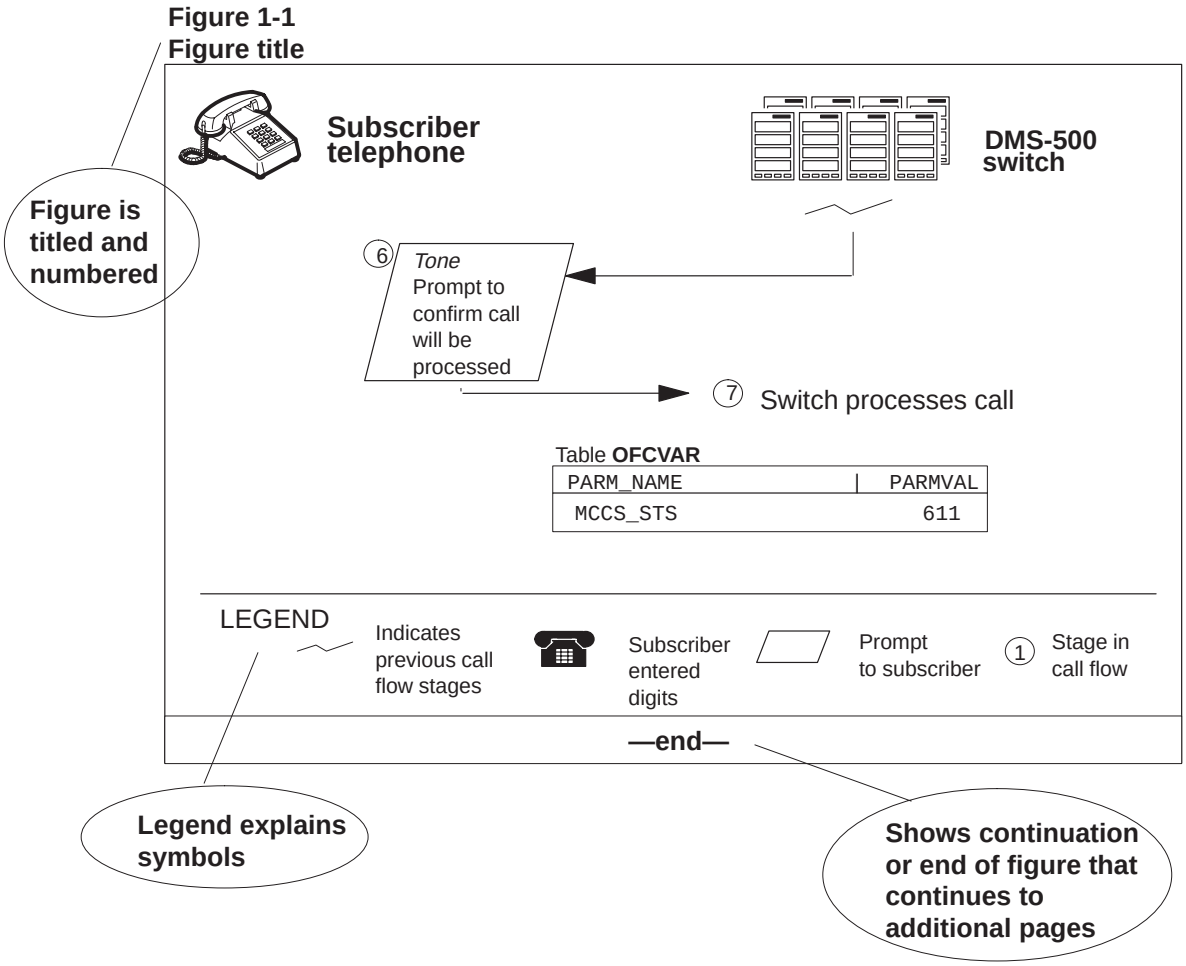
ctrl_no is the number of the CTRL (0 or 1)

Example of a MAP response:

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

Illustrations in figures

The following shows the figure conventions.



Numbering ranges for dialing plans

The following numbering ranges apply for any dialing plan listed in this manual.

- N = 2–9
- W = 0–1
- X = 0–9
- Z = 2–8

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.

Overview of TCP/IP

Introduction to the Internet and TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of communication protocols. Before TCP/IP is described in detail, it is appropriate to first present a short introduction to the Internet.

What is the Internet?

Originally, “Internet” was used only as the name of the network that was built upon the Internet Protocol (IP). It has since become a generic term used to refer to an entire class of networks.

The following are commonly accepted definitions:

- The generic term “internet” (with lowercase “i”) refers to any collection of separate physical networks interconnected (linked) by a common protocol to form a single logical network.
- The “Internet” (with uppercase “I”) refers to the worldwide collection of interconnected networks that grew out of the ARPANET network and that uses IP to link the various physical networks into a single logical network.
- Being “on the Internet” refers to using a computer that is connected to the worldwide collection of interconnected networks called “Internet.” Every computer on the Internet, from mainframe to personal computer, must use TCP/IP for the communication protocol.

Internally, the Internet is composed of heterogeneous networks that use different message formats and protocols. Externally, the Internet appears as a single network with hosts on interconnected networks appearing as interconnected hosts; this appearance is possible through the use of gateways that convert formats and protocols between networks.

In the remaining sections of this document, both “internet” and “Internet” refer to networks that are interconnected by TCP/IP. The DMS-500 switch uses TCP/IP for communication over a local Ethernet, a type of internet. The TCP/IP protocols to access Ethernet are described in this document.

Brief history of the Internet and TCP/IP protocols

In 1969, the Defense Advanced Research Projects Agency (DARPA) funded a research and development project to create an experimental packet switching network which would provide reliable, vendor-independent data communications. This experimental network was called ARPANET (Advanced Research Projects Agency Network) and soon proved the feasibility of wide area networking.

In 1975, ARPANET evolved past the experimental stage and became fully operational. However, development continued on the network. The basic TCP/IP protocols were created after ARPANET became operational.

In 1983, TCP/IP protocols were adopted as Military Standards. At that time, all hosts connected to ARPANET were required to convert to TCP/IP, and TCP/IP was soon found on a wide range of LAN systems.

Also in 1983, ARPANET was divided into two networks: MILNET and a new, smaller ARPANET. The term “Internet” was used to refer to the entire network: MILNET plus ARPANET.

During 1990, the Internet had grown far beyond its original scope, encompassing many networks worldwide, and ARPANET formally ceased to exist.

Important features of TCP/IP

The features that allow TCP/IP to meet worldwide data communication needs are as follows:

- open protocol nature, standards available to all
- computer hardware independence
- network hardware independence
- common addressing scheme
- standard high-level protocols

These features are described in the following paragraphs.

Open protocol nature, standards available to all

TCP/IP has an open protocol nature, meaning that everyone can find out about the protocol specifications through publicly available standards documents, and everyone is free to develop products to meet these open protocol specifications.

Computer hardware independence

The protocols are independent from any specific computer hardware or operating system. Because it is so widely supported, TCP/IP is ideal for communication between different hardware and software.

Network hardware independence

Being independent from any specific network hardware, TCP/IP can integrate many different kinds of networks, such as an Ethernet, a token ring, an X.25 net, a dial-up line, and virtually any other kind of physical transmission media.

Common addressing scheme

Any device, such as a computer or DMS-500 switch, can use TCP/IP to uniquely address any other device in the entire network, no matter how large the network. This is due to the use of a common addressing scheme.

Standard high-level protocols

Because they are standardized and high-level, TCP/IP protocols allow widely available, consistent user services.

TCP/IP protocol suite

TCP/IP is a suite of data communication network protocols. The suite gets its name from two of several protocols that belong to it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP and IP protocols are covered in detail in Section 2, “TCP/IP on the DMS-500 switch.”

Two other protocols, File Transfer Protocol (FTP) and Telecommunications Network (Telnet), provide popular user services. FTP permits file exchange between hosts. FTP is covered in detail in Section 4, “Using FTP at the switch.” Telnet provides virtual terminal services for interactive access by terminal servers to hosts. Telnet is covered in detail in Section 5, “Using Telnet at the workstation.”

Other protocols in the TCP/IP suite are briefly introduced in this document; however, details of them are beyond the scope of this document. These protocols include Routing Information Protocol (RIP), Transport Layer Interface (TLI), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Generic subNet Interface (GNI), SubNetwork Access Point (SNAP), and Ethernet.

Note: The FTP and Telnet protocols can only be used if the user has some knowledge of the network; thus, all TCP/IP protocols are introduced in this document and are shown in the figures that describe the architecture. Some protocols, such as RIP, run without the user even knowing that they exist. The system administrator needs to be aware of all the applications and protocols in TCP/IP layers.

TCP/IP on the DMS-500 switch

Benefits of using TCP/IP

Many customers have indicated they have a need for a dedicated physical port because each asynchronous MAP session has caused maintenance and administration problems for them. Additionally, because ports are scarce, users tend to leave sessions up for long periods. The Telnet part of TCP/IP provides remote MAP terminal access which helps alleviate these problems.

Some customers are large organizations that frequently resell their network to other smaller organizations. This can cause a need for large and abrupt database changes. On occasion, a user might need to change 50,000 automatic number identifications (ANI) in one night or may want to use the data modification order process (DMOPRO) to add or change 500,000 ANIs during a commissioning. The FTP part of TCP/IP helps alleviate these problems by providing high-speed manual file transfer capabilities to the workstation from the DMS-500 switch.

Features of TCP/IP

TCP/IP on the DMS-500 switch provides the following features and service tools:

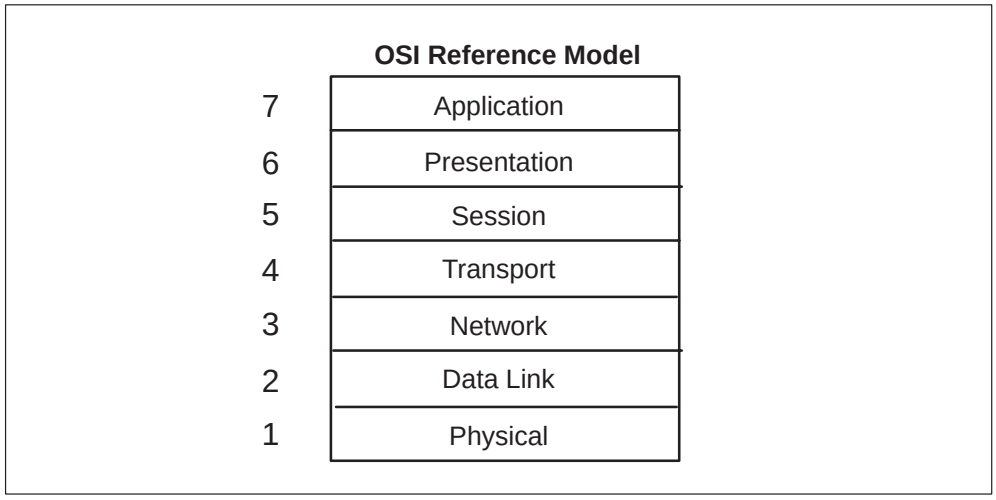
- TCP/IP allows communication between equipment connected to any number of heterogeneous networks including land-based, long-haul X.25 Public Data Networks, satellite, and high-speed LANs.
- IP datagrams may travel several hops and be processed by several intermediate nodes in going from an Internet source (a host computer or the DMS-500 switch) to an Internet destination (the DMS-500 switch or a host computer). Additionally, on repeated messaging, the datagrams may take entirely different paths.
- A configurable number of TCP connections is supported for each node.
- Record-marking with RFC 1006 header is available in TCP.
- The SuperNode ping tool is available for checking the status of remote nodes.

ISO data communications model

The services provided by the TCP/IP protocol suite can be broken down into layers that correspond to the International Standards Organization's (ISO) seven-layer Open Systems Interconnection (OSI) Reference Model.

Figure 2-1 gives an overview of the OSI Reference Model.

Figure 2-1
Seven layers of the OSI Reference Model



OSI Reference Model (seven layers)

The OSI Reference Model presents basic function blocks in terms of seven "layers" that should be provided by any networking system. These layers each build upon the lower ones in that

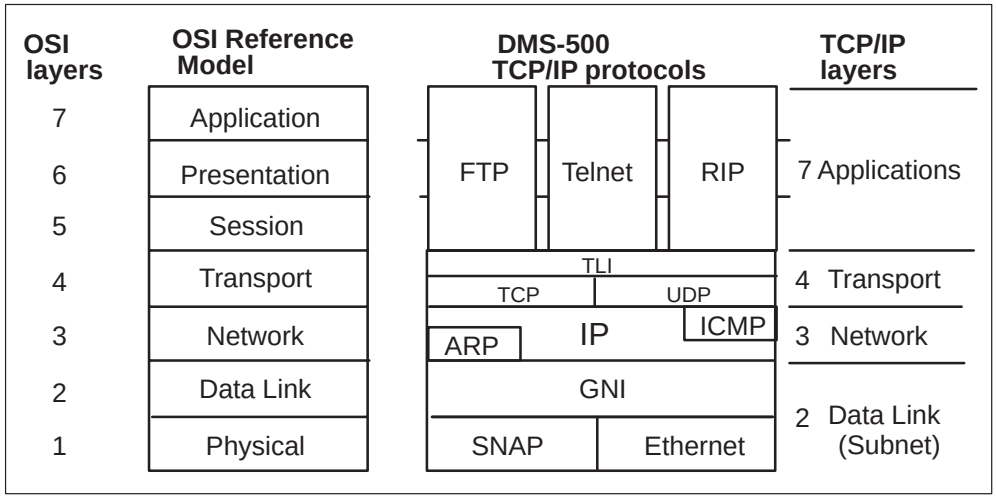
- Each layer provides a particular kind of service to the layer above it.
- Each layer expects a particular kind of service from the layer below.

To provide a communication service between networks or devices, each layer must communicate with its peer layer in a different communications unit, typically called a "host." In this document, a "host" could be a DMS-500 switch or a remote computer. The communication between the two hosts requires "protocols" which are a set of rules that govern communication transactions between peer layers.

How TCP/IP relates to the seven OSI layers

Figure 2-2 shows the correlation between the seven layers of the OSI model and the four layers of the TCP/IP stack. Note that, although the term TCP/IP refers to the entire four-layer stack including applications, TCP and IP are also discrete protocols located in the Transport layer and the Network layer of the stack.

Figure 2-2
Levels of the DMS-500 TCP/IP protocol



TCP/IP architecture (four layers)

The DMS-500 switch supports the TCP/IP protocol suite in a four-layer architecture stack that contains several services and tools. These layers, shown in Figure 2-2, are described in the following paragraphs.

Applications layer: FTP, Telnet, and RIP

The Applications layer includes FTP, Telnet, and Routing Information Protocol (RIP). These are described in the following paragraphs.

FTP

FTP is a protocol that allows files to be transferred to and from the DMS-500 switch to a remote workstation at a host computer. FTP supports two types of data transfer: binary and text.

- Binary allows any kind of file to be transferred.
- Text restricts transfers to files that contain text only.

Telnet

Telnet is a terminal emulation protocol that lets you log in from a workstation on your host computer to the remote DMS-500 switch. Using Telnet, you can sit at your workstation and run programs that are resident on the remote DMS-500 switch—just as if your workstation were attached to the switch. The MAP screen data from the switch is displayed on your computer screen. The commands and data you enter from your keyboard are sent across the network to the remote switch.

The Telnet tool is useful when you have a large amount of data on the switch that you need to process in some way. Rather than using FTP to transfer that

large amount of data from the switch across the network for local processing on your computer (which could be a time-consuming task that reduces the available network capacity for other users), Telnet lets you perform tasks on that data and do maintenance remotely.

RIP

RIP is a protocol that is used by network devices in the exchange of routing information. The industry standard RIP is implemented for an Ethernet interface unit (EIU) to enable it to participate in the exchange of dynamic routing information with other IP routers on the Ethernet LAN. The dynamic routing information is required on the switch to be able to route datagrams to hosts on distant LANs.

This protocol is transparent to the FTP or Telnet user.

Note: The FTP and Telnet protocols require the user to have some knowledge of the network; details needed by the FTP and Telnet user are provided in this document. Other protocols, like RIP, for example, run transparent to the user; these protocols are introduced in this document and shown in some illustrations. Full details of them are beyond the scope of this document. Unlike the FTP and Telnet user, the system administrator needs to be aware of all applications and protocols in TCP/IP layers and may need details provided in other documentation.

Transport layer: TLI, TCP, and UDP

The Transport layer includes Transport Layer Interface (TLI), TCP, and User Datagram Protocol (UDP). Both TCP and UDP exist in the DMS-500 switch; however, one can exist without the other.

The Transport layer interfaces are described in the following paragraphs.

TLI

This protocol is transparent to the FTP or Telnet user. It is not described in this document.

TCP

TCP provides a connection-oriented, byte-stream service at the Transport layer. It serves as the basis for reliable, orderly transmission of user data by handling, for example, detection of lost datagrams and automatic transmission.

The TCP part of the protocol suite separates the information you want to send across the Internet into smaller, easily managed pieces, which TCP numbers sequentially. The numbered information pieces are then sent across the Internet to their destination. As each piece of information arrives at the destination, TCP verifies it ands puts the small, numbered pieces of your

information back together in the proper order. If a numbered piece of information is garbled or missing, TCP requests that the originator resend the specific garbled or missing piece. When TCP has assembled all the information in the correct order, TCP sends the information to the software program (application) using its services.

TCP allows you to send any kind and size of information, ranging from a brief e-mail text message to a complete encyclopedia of information with text, graphics, sound, video, and even software programs.

The process of using TCP, which happens at several thousand bits per second, is transparent to users. Most readers of this document, as TCP/IP users, will be mainly interested in the Telnet and FTP sections. However, all sections will be of interest to the system administrator, who needs to configure and troubleshoot TCP/IP.

UDP

UDP is a protocol used by applications programs to provide direct, low-overhead, connectionless datagram delivery service between two peer application layers. UDP is used for transaction-oriented applications, where TCP provides connection-oriented data transport services.

This protocol is transparent to the FTP or Telnet user.

Network layer: ARP, IP, and ICMP

The Network layer includes Address Resolution Protocol (ARP), IP, and Internet Control Message Protocol (ICMP). These are described in the following paragraphs.

ARP

ARP is a network access layer protocol that performs the translation of IP addresses to Ethernet addresses. This mapping of IP addresses to physical Ethernet addresses is done so datagrams can be delivered between the host computer and the switch.

This protocol is transparent to the FTP or Telnet user.

IP

All dataflow in and out of the system goes through the IP. The IP delivers data from the network (via Ethernet) to the correct transport service (TCP or UDP) and the IP delivers data from the upper layers to the network.

Thus, the IP provides transaction services or end-to-end datagram delivery service at the Network layer. Additional functionality includes support for address identification by both Network Number and host Node Number as

well as the fragmentation and reassembly of IP datagrams for transmission through a variety of networks.

The IP part of the TCP/IP protocol suite manages the addressing of your "message"—which is what the IP calls your information. The IP serves the same purpose as an addressed paper envelope that contains a message on paper that you want to mail to a friend via the U.S. Postal Service.

Consider how the paper mail gets routed from you to your friend. A paper envelope contains both the return address of the sender (you) and the destination address of the receiver (your friend). The return address is necessary in case the message cannot be delivered to the destination address and needs to be returned to the originator (you, the sender). You leave your envelope containing your paper message in the mailbox outside your home and put up the mailbox flag. Your local mail carrier retrieves the envelope from your mailbox and takes it by truck to your local post office. There, it is sorted and then sent on its way over a series of routes by truck, plane, or ship. The final resorting is done at a remote post office near your friend's address and, after final routing, the message is delivered by truck to its destination address and put into your friend's mailbox.

This is how electronic mail gets routed from you to your friend. The networks that make up the Internet are connected by special-purpose computers called "routers" because they determine how to route the information traffic on the Internet. These router computers are the network equivalent of the post offices which sort the paper mail and send it out on the correct (truck, plane, or ship) routes. Like a post office, each router computer knows what different connections are available and which is the best next destination to get a message closer to its final destination. The router computers are physically connected by Ethernet networks and telephone lines which are the network equivalents of the U.S. Postal Service's use of trucks, planes, and ships.

ICMP

The ICMP protocol is the part of the Internet layer that sends messages that perform control, error reporting, and information functions for TCP/IP.

ICMP is part of IP (the Network layer), but ICMP datagrams are sent using IP; therefore, it is encoded as if it were the Transport layer. Nodes use ICMP to communicate IP status and errors. For example, ICMP could be used to inform a source node that the intended destination node is unreachable or that there is network congestion.

This protocol is transparent to the FTP or Telnet user.

Data Link layer: GNI, SNAP, and Ethernet

The Data Link layer (sometimes referred to as “Subnet layer”) detects and, where possible, corrects data transmission errors as it “hides” the layers above from the physical functions of translating bits of data into a format suitable for data transmission or receiving a transmission and then translating it back into bits.

The Data Link layer includes Generic subNet Interface (GNI), SubNetwork Access Point (SNAP), and Ethernet protocols. These are briefly described in the following paragraphs.

GNI

The GNI provides a generic interface, hiding the actual interface-to-subnet layer from IP. The Subnet layer can be present or absent from a platform where IP is running. Messages are simply sent and received through the GNI layer rather than the actual Subnet layer interface.

This protocol is transparent to the FTP or Telnet user, and is not further described in this document.

SNAP

The SubNetwork Access Point (SNAP) protocol is transparent to the FTP or Telnet user, and is not described in this document.

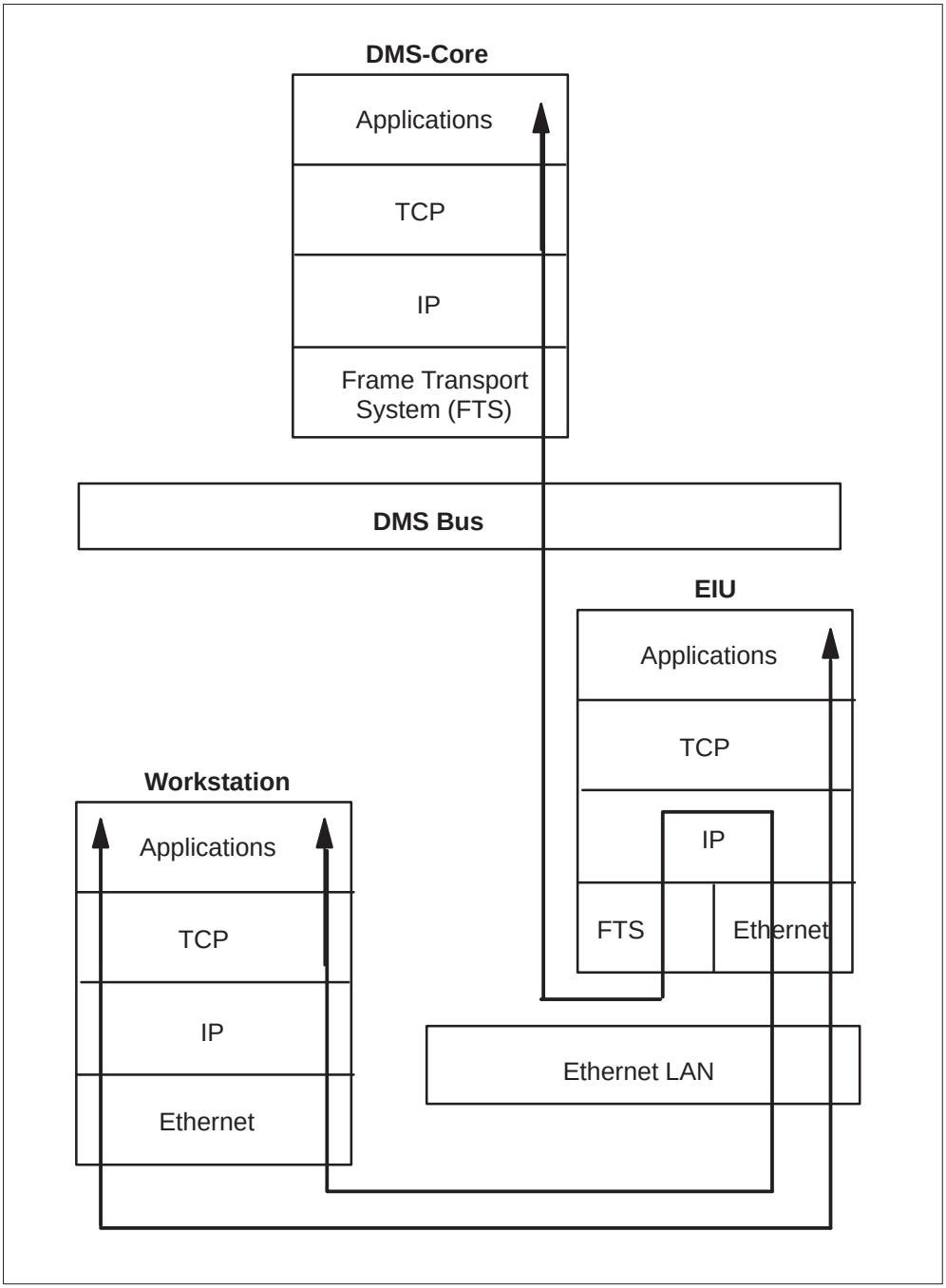
Ethernet

The functionality of the EIU, which establishes connectivity with the Ethernet network, is described in detail in Section 3, “Ethernet Interface Unit.”

This protocol is transparent to the FTP or Telnet user who may want to skip Section 3. The system administrator, however, will find the information necessary.

Figure 2-3 is useful only to the system administrator. It shows what FTP and Telnet ride upon. This information is transparent to the FTP or Telnet user.

Figure 2-3
TCP/IP message flow



Ethernet interface unit

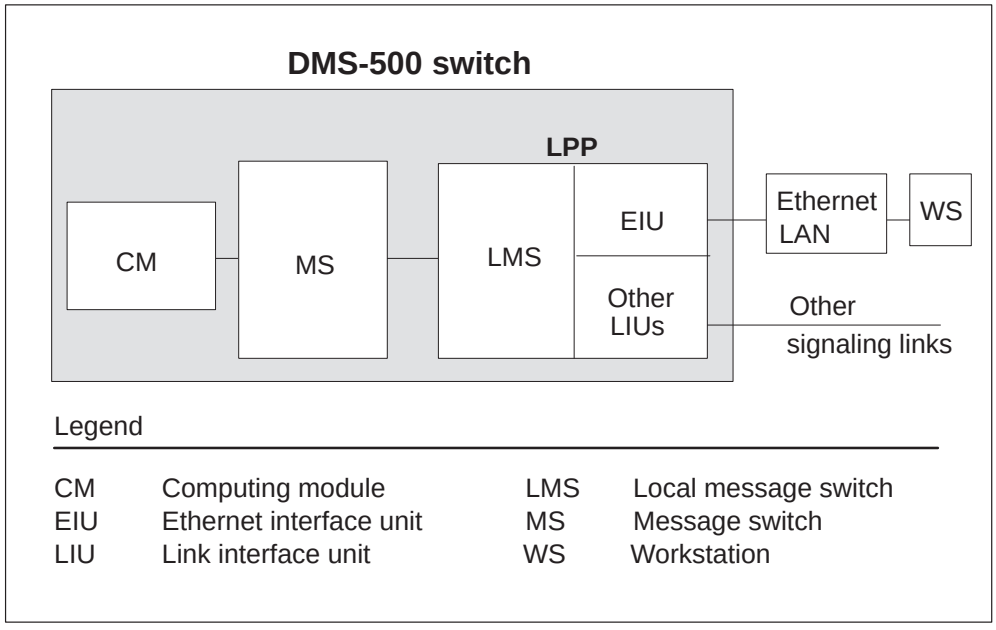
Overview

The Ethernet Interface Unit (EIU) functionality is comprised of hardware, software, and table datafill that includes IP addresses and specific Nortel (Northern Telecom) assigned Ethernet addresses for each EIU. This section describes how Ethernet LAN connectivity is established, lists the required software and hardware, and discusses address allocation. It presents the IP and Media Access Control (MAC) addressing schemes. This section also summarizes EIU maintenance features. For details on table datafill, see Section 6, “Table datafill.”

Ethernet connectivity

A link peripheral processor (LPP) containing an EIU is deployed in a DMS-500 switch to establish Ethernet connectivity via TCP/IP. This is illustrated in Figure 3-1.

Figure 3-1
EIU on the DMS-500 switch



An LPP is a frame that can hold up to a total of 32 link interface units (LIUs).

LIUs are devices that serve as termination points for a variety of signaling links such Ethernet, CCS7, and frame relay.

You can have a maximum of four EIU cards allowed per switch; installing EIUs in LIU slots reduces the number of possible LIUs.

Ethernet connectivity is considered sufficient connection for messaging between the DMS-500 switch and any external node or hardware that has an address and responds to a standard communications protocol. An Ethernet node responds to Internet Control Message Protocol (ICMP) Echo Request messages and has an IP address.

EIU software

The following EIU software load is required:

- ERSxxxx EIU Telnet customer load

The following tables require datafill:

- LIUINV
- IPNETWRK
- IPHOST
- IPROUTER
- IPPROTO
- IPTHRON
- RMCONFIG
- ENSITES
- ENTYPES
- EXNDINV

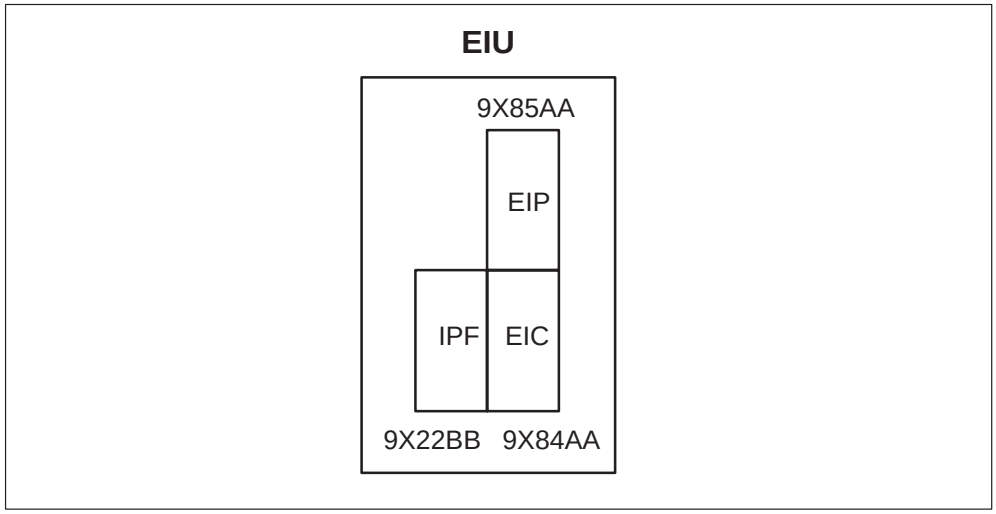
EIU hardware

EIU hardware consists of the following two circuit packs and a paddleboard. An EIU application user interface (AUI) cable is also needed.

- NTEX22BB card: Integrated PBus and FBus card (IPF)
- NT9X84AA card: Ethernet Interface Card (EIC)
- NT9X85AA card: Ethernet Interface Paddleboard (EIP) card

The cards are shown in Figure 3-2 and described in the following paragraphs.

Figure 3-2
EIU hardware on an LPP



Integrated PBus and FBus card

The NTEX22BB IPF card is a processor board that contains the Motorola M68030 and 8 Mbyte of RAM. It also contains the PBus to FBus interface which connects the processor bus (PBus) with the frame bus (FBus). The FBus in turn connects to the local message switch (LMS) through a rate adaptor. The IPF card is a common processor card used in most LIUs and runs the Support Operating System.

Ethernet Interface Card

The NT9X84AA EIC card has a local high speed buffer and implements most of the MAC layer on a single chip. It has 384 kbytes of high-speed buffer for holding Ethernet packets.

Ethernet Interface Paddleboard card

The NT9X85AA EIP card provides the physical link to the LAN. The paddleboard implements an unshielded twisted pair AUI interface.

Address allocation

Within a single SuperNode switch, multiple hosts and multiple applications within a single host may simultaneously request TCP/IP services. To provide for application address uniqueness across the network, the following TCP/IP address allocation scheme is used:

- TCP provides individual port numbers to distinguish between applications in the same host.
- Each host processor in the internet SuperNode switch is assigned a unique IP address. This is a logical address and, when concatenated with a TCP port number, forms a unique network end-point or "socket."
- Within the network, each node is physically identified by its own unique subnetwork address. The logical IP address is translated to a subnetwork address prior to datagram delivery to the destination node.
- Within the network, each node, such as DMS-Core and EIU, has a unique frame transport address (FTA) that uniquely identifies the subnetwork node on the SuperNode. The EIU also has a MAC address (also called an Ethernet address) which uniquely identifies it on the Ethernet LAN.

The IP and MAC addressing schemes are described in detail in the following paragraphs. Both addressing schemes are needed. The MAC addressing scheme is needed to handle addressing for the Subnet. The IP addressing scheme is needed to handle addressing on the Network layer.

IP addresses

IP addresses are the means by which each host is uniquely identified, much like a street address. Composed of a network designation and a host designation, IP addresses are 32 bits long, but are typically displayed as four fields, one byte (0–255) each, separated by a period.

These four fields are interpreted differently based on which of three distinct network classification types the address represents.

Networks are classified as either class A, B, or C:

- Class A indicates a large number of hosts on a few networks.
- Class B indicates a balance between host and networks, both medium.
- Class C indicates a few hosts on many networks.

Note: Class D and E addressing schemes are not supported.

Accordingly, the first most significant byte of the IP address for class A can take on the values 0–127, class B values 128–191, and class C values 192–223. For example, a class A IP address might be 47.192.45.8.

Table 3-1 shows further details about IP address class structure.

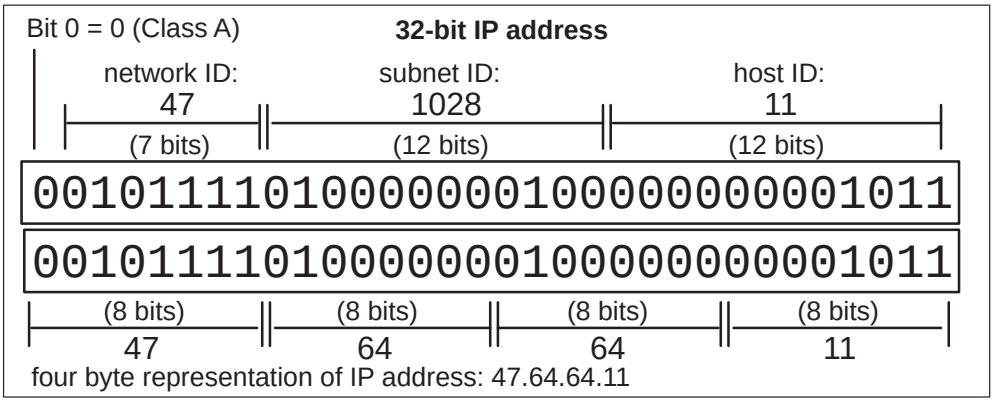
Table 3-1
IP address class structure

Class	Initial binary bits (first byte)	Number of network bits	Number of host bits	32-bit hex net mask
A	0	7	24	FF000000
B	10	14	16	FFFF0000
C	110	21	8	FFFFFF00

As mentioned earlier, within the network, each node is physically identified by its own unique subnetwork address that is used for routing to the individual destination nodes.

For example, suppose your site's network is designated class A. Given a site class A IP address 47.64.64.11 and an internal subnetwork with addresses 12 bits long, the Network ID is 47, subnet ID is 1028, and host ID is 11. See Figure 3-3 for clarification.

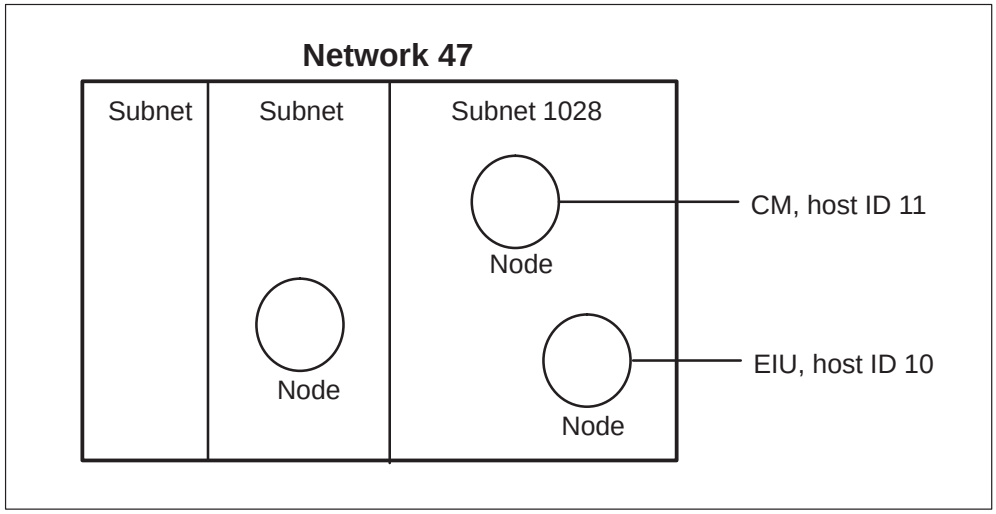
Figure 3-3
Clarification of example Class A IP address 47.64.64.11



Note: You do not datafill the subnet ID, but the subnet ID bit width in table IPNETWRK. In the example in Figure 3-3, this number is 12.

Your physical layout could be as shown in Figure 3-4.

Figure 3-4
Example physical mapping of IP address



IP addresses are supplied by the customer. IP addresses for all DMS-500 hosts are assigned via datafill in tables IPNETWRK, IPROUTER, and IPHOST.

EIUs are assigned two IP addresses, one to address the switch side node and the other to address the Ethernet LAN side node. The EIU host application is addressed from within the switch or from external LAN workstations by addressing the EIU switch side IP address. However, the Routing Information Protocol (RIP) application addresses the EIU host application via the LAN side IP address.

IP addresses are datafilled entities on the DMS-500 switch. A number of methods are available for determining IP addresses on the switch. Three methods of IP address assignment are described in the following paragraphs.

IP address assignment method 1

Table IPNETWRK, the second field, CMIPADDR, lists the computing module (CM) IP address. In the following example, the CM IP address is 47.76.137.82. In this example, the subnet ID bit range is 19.

```
TABLE: IPNETWRK
KEYREF CMIPADDR SUBNET OPTION PARMAREA
-------------------------------------
0 47 76 137 82 19 (EIU 208) (EIU 102) $ (SCRNFLAG N) $
```

IP address assignment method 2

Table IPHOST, the third field, NODEINFO–subfield SNADDR, lists the EIU IP address. In the following example, the EIU 208 switch side IP address is 47.96.192.68.

```
TABLE: IPHOST
INDEX NODENAME NODEINFO
----------------------
0 CM 0 16 2 2
1 EIU 102 47 96 192 67 47 177 75 4 8 2 2
2 EIU 208 47 96 192 68 47 177 75 5 15 0 0
3 EIU 109 47 96 192 69 47 177 75 6 8 2 2
```

IP address assignment method 3

Table IPROUTER, the third field SNIPADR lists the EIU IP address. In the following example, the EIU 109 switch side IP address is 47.96.192.69.

```
TABLE: IPROUTER
RKEY ROUTER SNIPADR ETHIPADR ETHARP ETHPARP
-------------------------------------------
0 EIU 102 47 96 192 67 47 177 75 4 YES YES
1 EIU 208 47 96 192 68 47 177 75 5 YES YES
2 EIU 109 47 96 192 69 47 177 75 6 YES YES
```

Media Access Control addresses

Each EIU has a Media Access Control (MAC) address (also called the Ethernet address) that uniquely identifies it on the Ethernet LAN. MAC addresses are 48 bits long on the DMS-500 switch. For example, 000075F00254 in hex. The fields for the Ethernet address are shown in Table 3-2.

Table 3-2
Ethernet address format

Bit 0	Bit 1	Bits 2–23	Bits 28–31	Bits 24–27 and 32–47
I/G	U/L	Northern Telecom's Vendor ID (in bits)	System (in bits)	System dependent field
IEEE assigned	IEEE assigned	00 0000 0000 0000 1010 1110 IEEE assigned	1111 (NT selected)	

The MAC addresses are administered by Northern Telecom (Nortel). Nortel assigns its addresses via datafill in table LIUINV.

CAUTION
Assigned EIU address must be obtained from Nortel
Before connecting the cable to the EIU circuit board, you must obtain the unique Ethernet address that was assigned by Nortel.

Although Nortel installs the EIU boards, your site provides the cable that connects to it, and your site administrator must know the assigned EIU address before connecting that cable.

You are strongly discouraged to assign arbitrary Ethernet addresses to EIUs. It is the responsibility of Nortel to distribute blocks of Ethernet addresses to its customers. If you do not have one assigned by Nortel or are not sure what it should be, contact Nortel.

EIU maintenance

EIU maintenance is available through generic LIU maintenance which is CM resident. It provides for access to a MAP screen, logs, OMs, table control, EIU Manager, as well as messaging to the EIU resident local maintenance.

Local maintenance is split into node maintenance and EIC MAC layer maintenance. The MAC layer, a sublayer of the Data Link layer, dictates how a medium is shared by multiple nodes. Local maintenance principally ensures EIU operability despite CM failure.

Configuration specific data is stored in table LIUINV.

Summary of EIU features

The features below are grouped into central and local maintenance, MAC layer services, maintenance Fault Insertion Test (FIT), Data Communications processor (DCP) central control, EIU protocols, IP throttling, Internet dynamic routing, LAN maintenance, LAN management from IOC MAP, and live office network datafill changes.

Central and local maintenance

The EIU features listed below are concerned with central and local maintenance and the MAC layer services of the EIU, formerly DCP. These features provide

- CM resident maintenance for
  - loading and initializing the EIU
  - manual command and control of EIU
  - interface to local maintenance
  - fault detection and handling
  - EIU manager
  - inventory table control
  - MAP display and commands by adding an EIU sub-level to the peripheral module (PM) level
- EIU resident local maintenance for
  - processing CM maintenance requests and queries
  - supporting all restarts
  - interfacing to MAC layer
  - EIC initialization
  - EIC interrupt handlers

MAC layer services

The MAC layer services include

- interrupt handling
- message buffering
- messaging services
- message byte ordering
- Ethernet address allocation scheme for the DMS-500 switch
- enhancement of
  - table LIUINV
  - MAP commands
  - CM to local maintenance interface
  - EIC initialization
  - EIC interrupt handlers

Maintenance Fault Insertion Test

The EIU maintenance Fault Insertion Test (FIT) features provide

- additional diagnostics to increase FIT coverage for detecting, isolating, and recovering from faults in the EIC
- I/O interrupt throttling
- EIU overload controls
- internal data loopback
- inservice audits
- reports of excessive LAN faults to local maintenance
- migration to 2 card LIU NEX22AA

DCP central control

The DCP central control feature enhances EIU maintenance to allow the raising of INServ trouble conditions for thresholded LAN transmissions and reception errors, as well as adopting the new name of EIU for the old DCP. The name EIU refers to the physical transmission media the peripheral employs: Ethernet.

EIU protocols

The EIU protocols feature provides

- ICMP echo request and reply messages, as well as some error message generation for bad or undeliverable datagrams
- Remote Log System (RLS), which resides on the CM as a log server and on the CM or a remote node as a log client, to offload the DMS log system
- LOG group, ITN (InTerNet), which generates LOG messages for all protocol layers
- support to local applications
- improved performance, reliability, and recovery mechanism

Internet protocol throttling

The IP throttling feature implements a mechanism to avoid congestion on the DS30 links between the MS and the LMS caused by IP traffic to and from EIUs.

This feature ensures that non-IP traffic, such as CCS7 messaging, through the DS30 links does not experience message loss caused by an overload of IP traffic.

Internet dynamic routing

The Internet dynamic routing feature provides

- dynamic routing to extend the DMS-500 switch's ability to handle faults due to routing failures
- RIP, which allows EIUs to exchange routing information with third party internet gateways
- ICMP in the area pertaining to message routing

LAN maintenance

The LAN maintenance feature provides the MAP operator with the ability to datafill and manipulate configuration data for external nodes reachable by way of the EIU. This feature provides

- detailed information about external nodes as viewed from Table Control
- configuring external nodes as components of the system from the MAP terminal
- preparing work for datafill later

LAN management from IOC MAP

This feature enhances the MAP monitoring and control capabilities for External Nodes (EXNDs). This feature provides

- an additional EXND sub-level to the PM MAP level
- a minor alarm when an EXND fails
- expandable base components to support other LAN technologies for future development

Live office network datafill changes

Functionality for allowing live office network datafill changes provides the

- ability to alter the following tables
  - LIUINV
  - IPNETWRK
  - IPHOST
  - IPROUTER
  - IPPROTO
  - IPTHRON
  - RMCONFIG

  - — ENSITES
  - — ENTYPES
  - — EXNDINV

- notification to appropriate applications when table data is modified
- transferring of control to applications, supporting them in determining consequences of changed data, and taking necessary actions to comply with changes
- downloading of instantly modified data to all nodes without waiting for restarts

Using FTP at the switch

Who uses FTP?

File Transfer Protocol (FTP) is a standard protocol for a user at a MAP terminal on a DMS-500 switch. FTP provides high-speed file transfer capabilities between the DMS-500 switch and a remote workstation at a UNIX host computer.

Note: A user at a UNIX host workstation who wants high-speed file transfer capabilities between that host workstation and a remote DMS-500 switch must use Telnet (described in Section 5, "Using Telnet at the workstation").

Definition of FTP

FTP is an internationally accepted protocol for exchanging files between computing devices. The FTP implementation on the DMS-500 switch conforms to industry standards. Therefore, files can be exchanged between the computing module (CM), workstations, mainframes, and other computing platforms that have FTP implementations. The files can be of many formats, and the computing devices can be hosts with different file systems.

FTP is a session-oriented tool. This means a session must be established through login before files can be exchanged. This implies the need for userids and passwords.

Client and server programs

The FTP software consists of two parts:

- a client program that resides on the accessing computer (switch)
- a server program that resides on the accessed computer (workstation)

Server and client protocols are required for both ends of two cooperating application processes that are communicating across a network. The cooperating applications could be remote login, file transfer, or any arbitrary application.

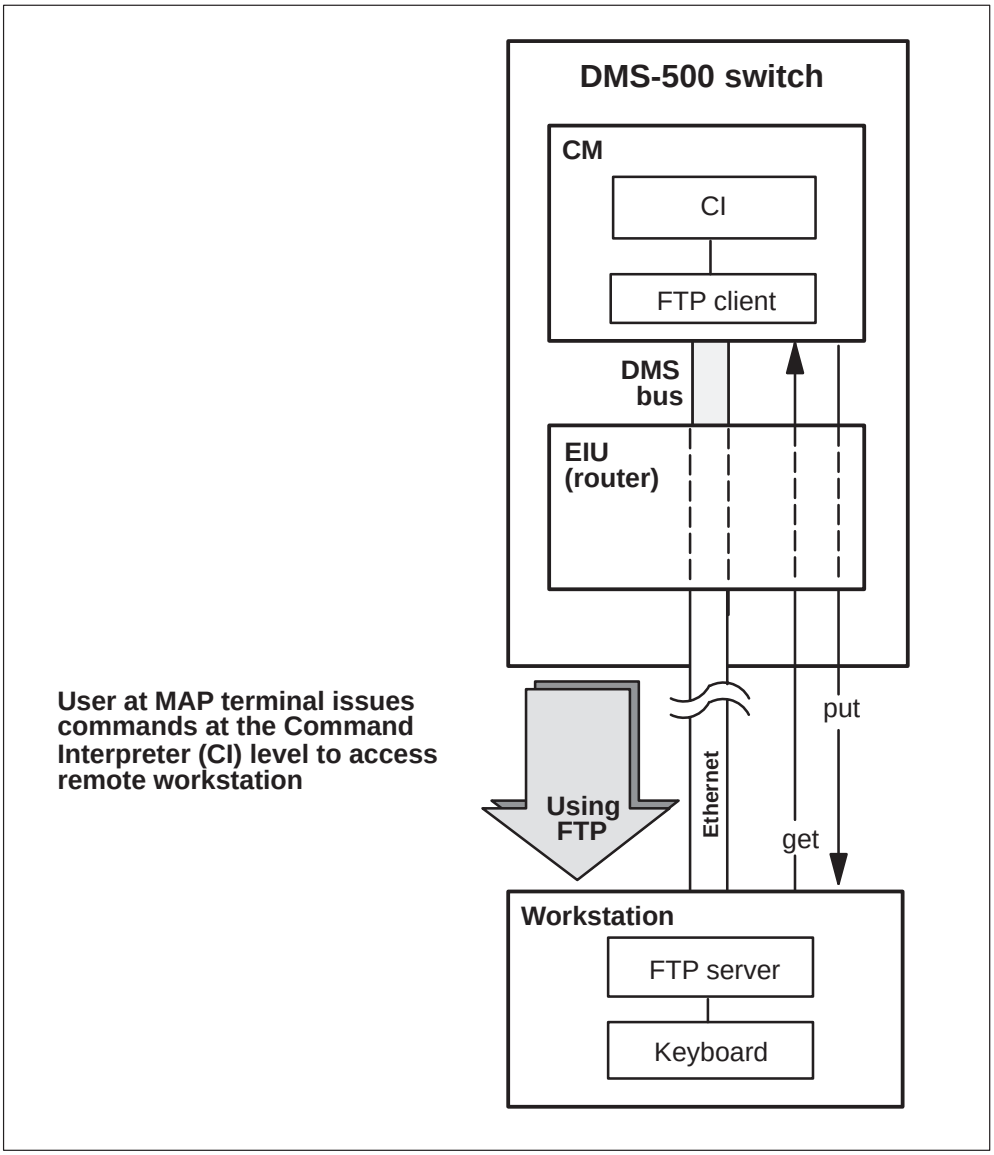
The FTP server is a passive logical entity located at the workstation that provides some type of specified service based upon the requirements of the

application. It does not initiate any request or service; instead it waits (listens) for a request from a client.

The FTP client is an active logical entity located at the DMS-500 switch that initiates requests to the server. The client could be viewed as a command that the user issues, and the server could be viewed as the object that responds to the client command.

Figure 4-1 illustrates using FTP to transfer files to and from the remote host workstation.

Figure 4-1
Using FTP to transfer files to/from remote host workstation



Filename conventions

Filenames must adhere to the following conventions when using FTP on the DMS-500 switch:

- Full pathnames must start with the ":" character.
- Destination and source file names on the remote host can be in lowercase or uppercase. But, because the switch CI will try to convert every letter on the command line to uppercase, single quotes must be placed around lowercase pathnames.

DMS-500 switch supported FTP commands

The SuperNode FTP feature provides full file transfer capabilities between DMS-500 nodes, as well as nodes external to the DMS-500 switch. The number of FTP connections is configurable for each node and provides a user interface plus CI for FTP client sessions.

Table 4-1 lists the commands that the DMS-500 FTP client implementation supports. The commands are listed in alphabetical order.

Note: FTP clients are slightly different from one implementation to another. Some clients have more commands than others. The DMS-500 switch's client has a small command list, but it has the quote command feature that allows it to send any command "as is."

Table 4-1
FTP commands

Command	Brief description
ascii	Changes the transfer to ASCII type
binary	Changes the transfer to binary type
cd	Changes the working directory
delete	Deletes the file specified in the pathname
dir	Lists the directory
ftpclose	Closes the connections with the remote host
ftpdebug	Sets debug messages on or off
ftpopen	Establishes connection to remote host
ftpquery	Prints file attributes
ftpquit	Closes the connection

—continued—

Table 4-1
FTP commands (continued)

Command	Brief description
get	Gets a file from the remote server
help	Provides information on commands
lcd	Changes the local working directory
lrecl	Sends the SITE LRECL command
ls	Lists the directory
mkdir	Makes (creates) a new directory
noop	This is a NO-OP (no operation) command
pass	Sends the password to remote host
put	Sends the file to remote host
pwd	Prints the working directory
quit	Closes the connection and quits CI
quote	Sends arguments as typed to the remote host
rename	Renames a file
rmdir	Removes (deletes) a directory
status	Provides the remote status
user	Sends the username to remote host
—end—	

Using basic DMS-500 FTP client functionality

At the DMS-500 switch CI level, you can use the FTP client to establish a session with a workstation attached to another host. After a session is established, you can use the *get* and *put* commands to transfer files between the DMS-500 switch and the remote host. The commands to perform this basic functionality are described next.

Establishing an FTP session from the DMS-500 switch

At the > prompt, enter FTP giving the CM IP address. An example is given in Figure 4-2.

Figure 4-2
Establishing FTP session from the switch

```
>ftp '47.12.0.2'
Allocated a Session ID Successfully
220 crchh93f FTP server (Version $Revision: 1.21 $ $Date:
93/12/21 10:19:25 $)
```

Entering the host's userid and password

Enter the host's userid when prompted for it. In the example shown in Figure 4-3, the user id is "johnqdoe." When you are prompted for the password, enter it. The password will not be displayed on your screen.

Figure 4-3
Entering userid and password on the host

```
USERNAME:
>johnqdoe
331 Password required.
PASSWORD:
>
230 User johnqdoe logged in.
```

At this point, you have logged into the host with IP address 47.12.0.2. You are placed in a default directory; in this case, the default directory is the HOME directory of the host.

Finding out where you are

To determine your current working directory, issue the command *pwd* (print working directory). In the example shown in Figure 4-4, user johnqdoe is shown to be working in the directory /bnr/users/u2/johnqdoe.

Figure 4-4
Determining the current working directory (pwd)

```
>pwd
251 “/bnr/users/u2johnqdoe” is the current working directory
```

Determining which files are in your directory

To determine what files are in the current working directory, you can issue the command *ls* to get the file names (see Figure 4-5) or the command *dir* to get the filenames with file access privileges, file size, and other information (see Figure 4-6).

Figure 4-5
Determining files in the current working directory (ls)

```
>ls
EDMA_Mina_2
TEAM2
WS_FTP_D2
WS_FTP_S1
WS_FTP_S2
al255
```

Figure 4-6
Determining files in the current working directory (dir)

```
>dir
total 2028
drwxr-x---  2 johnqdoe abcdef 1024 Jan 31 20:22 EDMS_Mina_2
-rw-r-----  1 johnqdoe abcdef    0 Jan 29 09:49 TEAM2
-rw-r-----  1 johnqdoe abcdef 1105 Jan 20 13:44 WS_FTP_D2
-rwxr-xr-x  1 johnqdoe abcdef 1142 Feb  6 10:32 WS_FTP_S1
-rwxr-xr-x  2 johnqdoe abcdef 1042 Feb  6 07:48 WS_FTP_S2
drwxr-x---  2 johnqdoe abcdef 1024 Jul 16 1991 al255
```

Changing to another directory at remote host

To go to another directory at the remote host, issue the command *cd* (change directory). Figure 4-7 shows an example of an error that occurs when the quotation marks are not given around the directory pathname.

Figure 4-7
Example of error when using cd command

```
>cd /team/bin
**** error ****
```

The example in Figure 4-7 shows an error condition caused because the DMS-500 CI will translate the command to become ‘CD/TEAM/BIN’ and /TEAM/BIN does not exist on the other host. To correct this error, use single quotation marks around the path name. This is shown in Figure 4-8.

Figure 4-8
Changing the current working directory at remote host (cd)

```
>cd '/team/bin'
200 CWD command okay.
```

Changing to another directory locally

To go to another local directory at the DMS-500 switch, issue the command *lcd* (change local working directory). There are two ways to do this, as shown in Figures 4-9 and 4-10. In these examples, notice the use of single quotes and uppercase letters. The quotes and all uppercase letters are used because disk drive unit (DDU) volumes are not supported in this load.

Figure 4-9
Changing the local working directory at the switch (lcd)

```
>lcd ’/S00DTMCE’
ftp: Local directory changed
```

Figure 4-10
Changing the local working directory (second lcd example)

```
>lcd :/S00DMTCE
ftp: Local directory changed
```

Getting an ASCII text file from the remote host

Figure 4-11 shows an example of transferring an ASCII file (named trahelp.text) from the remote host to the current local directory on the DMS-500 switch. Because the FTP default type is ASCII, specifying the type explicitly, as shown in this example, is optional.

Figure 4-11
Transferring a text file from remote host (get)

```
>ascii
200 Type set to A.
>get ’trahelp.text’ trahelp.text
226 Transfer complete.
12365 bytes transferred in 0hrs.0mins.4secs.110ms (3008 Bps)
```

Putting an ASCII text file onto the remote host

Figure 4-12 shows an example of transferring an ASCII file named RECORDFILE from the volume S00DIMAGEREG on the DMS-500 switch to the current working directory on the remote host, renaming it to jan18.log on the remote host.

Note: Uppercase letters must be used when specifying DMS-500 file and volume names, because DDU volumes are not supported in this load.

Because the FTP default type is ASCII, specifying the type explicitly, as shown in this example, is optional.

Figure 4-12
Transferring a text file to remote host (put)

```
>ascii
200 Type set to A.
>put :/S00DIMAGEREG/RECORDFILE 'jan18.log'
226 Transfer complete.
12365 bytes transferred in 0hrs.0mins.4secs.110ms (3008 Bps)
```

Getting a binary file from the remote host

To get a binary file from the remote host, you must set the type to binary. For some UNIX hosts, you must set the record length (for example, to 256) before transferring the file.

Figure 4-13 shows an example of transferring a binary file named file1.68k in directory /load68k from the remote host to the local directory, S00IMAGE, on the DMS-500 switch. The file is renamed to file1$ld on the switch.

Figure 4-13
Transferring a binary file (second get example)

```
>binary
200 Type set to I.
>lrecl 256
>get '/load68k/file1.68k' :/S00DIMAGE/file1$ld
```

Putting a binary file to the remote host

Figure 4-14 shows an example of transferring an image file named IMAGE1 from the volume S00DMTCE on the DMS-500 switch to the current working directory on the remote host, naming it *image1* on the remote host. This figure also shows an example of transferring a file named FILE1_UNIPL from the volume S00DMTCE on the DMS-500 switch to the current working directory on the remote host, naming it *file1_unipl* on the remote host.

Figure 4-14
Transferring IMAGE and UNIPL files to remote host (put)

```
>binary
>put :/S00DMTCE/IMAGE1 'image1'
>put :/S00DMTCE/FILE1_UNIPL 'file1_unipl'
```

Using Telnet at the workstation

Who uses Telnet?

Telecommunications Network (Telnet) is a standard protocol used by a user at a UNIX host workstation who wants to log in from that host workstation to a remote DMS-500 switch.

Note: A user at a MAP terminal on a DMS-500 switch who wants high-speed file transfer capabilities between that switch and a remote workstation must use FTP (described in Section 4, "Using FTP at the switch").

Definition of Telnet

Telnet can be defined as an application-level service tool of the TCP/IP suite of protocols for communicating between remote computers. This service allows users to log onto a remote system without any knowledge of the lower-level network protocols. Your node is treated as if it were a local terminal on the switch.

Client and server programs

The Telnet software consists of two parts:

- a client program that resides on the accessing computer (workstation)
- a server program that resides on the accessed computer (switch)

The server program at the switch listens at a known port for connections from clients at workstations. After a connection is established, the client redirects all user keyboard input to the server. The server then passes it through to the accessed program (for example, a login, CI, or some other program). The server intercepts all program output and redirects it to the client. The client then prints it on the client machine's screen for the user.

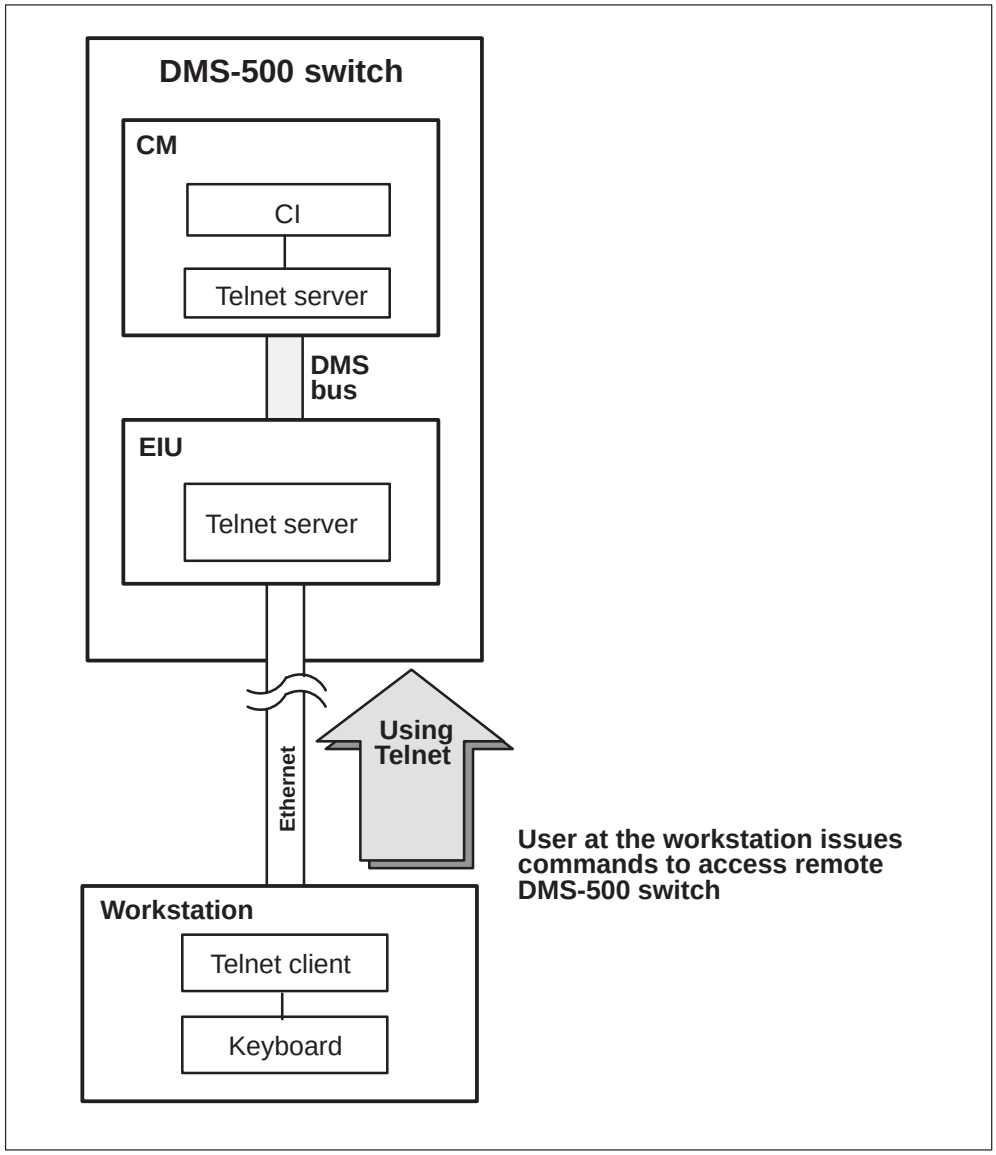
In the DMS-500 switch, the main purpose of the Telnet server is to provide access to MAPCI from a workstation. MAPCI supports asynchronous output to both a scroll area and a "full screen" area. MAPCI input, however, is buffered in a line-by-line mode. The Telnet server performs remote echoing of the input characters back to the Telnet client and ultimately to the workstation.

Telnet architecture

The software moves the Telnet server from the EIU to the CM. Telnet servers may reside on the CM, or EIU. By moving the Telnet server to the CM, you can Telnet directly to the CM and other SOS–based host processors, such as EIU (see Figure 5-1).

When you Telnet directly to the CM, the EIU acts as an IP router. If you Telnet directly to the EIU, the EIU acts as a Telnet host.

Figure 5-1
Using Telnet to access remote DMS-500 switch



Telnet features

The RMAP access and EIU/Telnet enhancements features relating to Telnet are described in the following paragraphs.

Remote MAP access

RMAP access is provided through a Telnet server on the DMS-500 switch. This feature implements an RMAP server on the CM that provides

- the RMAP implementation of a Physical File System (PFS)
- the implementation of a process for each Telnet session
- a known address to which an RMAP client sends connection requests
- the management and auditing of processes
- the Telnet server with CI and MAPCI updates

RMAP access is also provided through a Telnet server that resides on an EIU of the DMS-500 switch which

- receives keyboard input from a Telnet client program by way of standard utility routines
- provides Telnet access to the DMS-500 switch from any VT100-compatible device that can access the DMS-500 switch by way of TCP/IP; line-by-line and full screen MAP access are supported

Enhancements to Telnet allow

- support of a subset of the <BREAK> commands that include
  - — HELP, which outlines differences between Telnet MAP and normal MAP
  - — HT, which halts output to Telnet server, discarding output until next read request is received
  - — HX, which halts execution message to the Telnet server
  - — HXX (same as HX)
  - — LOGIN, which sends a login message to the Telnet server to start a new CI session
  - — LOGOUT, which sends a logout message to the Telnet server to terminate session
  - — MORE {# lines}, which turns on the “MORE...” prompt during scrolling; the number of lines default is 24 with a maximum of 999
  - — NOMORE, which turns off the “MORE...” prompt during scrolling

  - — RT, which sends a continue output message to the RMAP server, restarting output
  - — STOP (same as HX)
- more than one input file to be open at a time
- changes to the RMAP protocol to support new message types and changed message types

EIU/Telnet enhancements

EIU/Telnet enhancements provide

- simultaneous Telnet sessions (limited only by the number of TCP connections available) supported on the DMS-500 switch
- logs for statistical and error tracking information
- a configurable number of Telnet sessions via table control, using table RMCONFIG

Using basic DMS-500 Telnet functionality

At a UNIX host workstation, you can use Telnet to establish a MAP session with the DMS-500 switch. After a session is established, all standard DMS-500 switch MAP commands may then be issued to the remote switch from the host workstation. The commands to perform this basic functionality are described next.

CAUTION

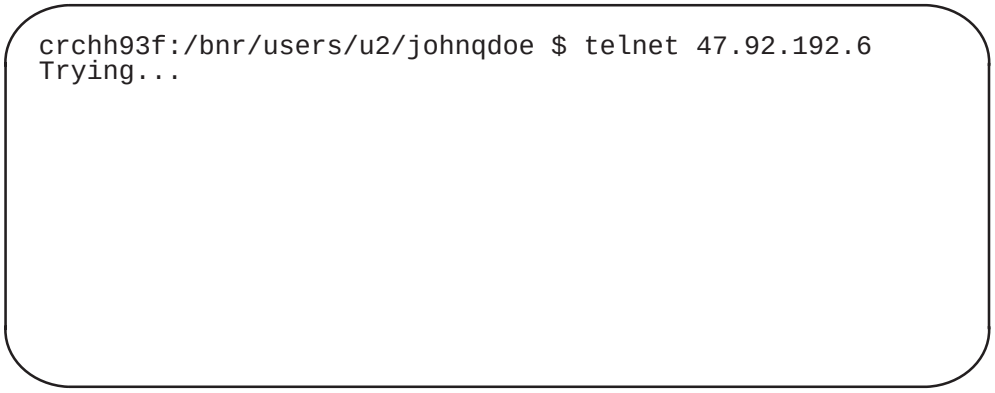
Adhere to filename conventions

Uppercase letters must be used when specifying DMS-500 file and volume names, because DDU volumes are not supported in this load.

Establishing a Telnet session from the workstation

First, at the $ prompt on your UNIX host workstation, enter the Telnet tool. You can do this in one of two ways, as shown in Figures 5-2 and 5-3. The Figure 5-2 example shows how you can type *telnet* with the IP address of the EIU node (destination) to which you want to be connected. The IP address format is ddd.ddd.ddd.ddd, where *d* is a decimal number.

Figure 5-2
Establishing a Telnet session from the host (method 1)

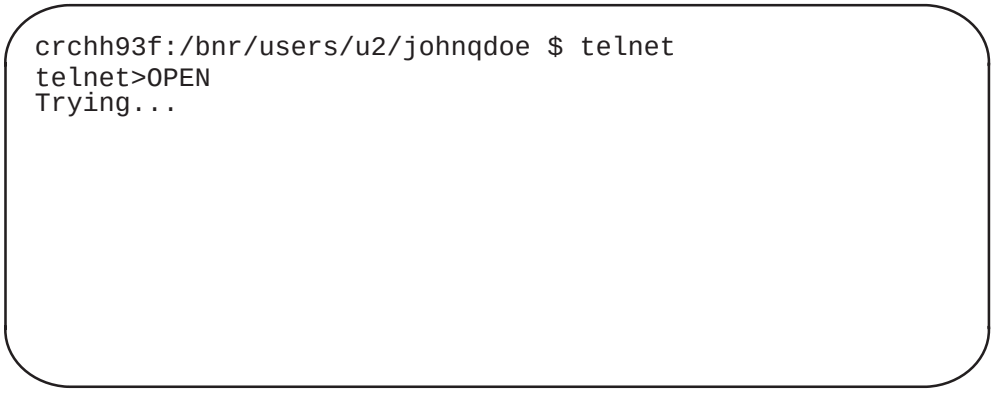


Note: The IP addresses of EIU are datafilled in table IPHOST in field NODEINFO subfield SNADDR and in table IPROUTER in field SNIPADR.

The second way you can establish a Telnet session is to type *Telnet* and omit the IP address of the EIU node (destination) to which you want to be connected. If you omit the IP address destination or if you specify an asterisk (*), you enter the Telnet command level and are prompted for a subcommand. In this case, you issue the subcommand OPEN in response to the *telnet>* prompt.

This is shown in Figure 5-3.

Figure 5-3
Establishing a Telnet session from the host (method 2)

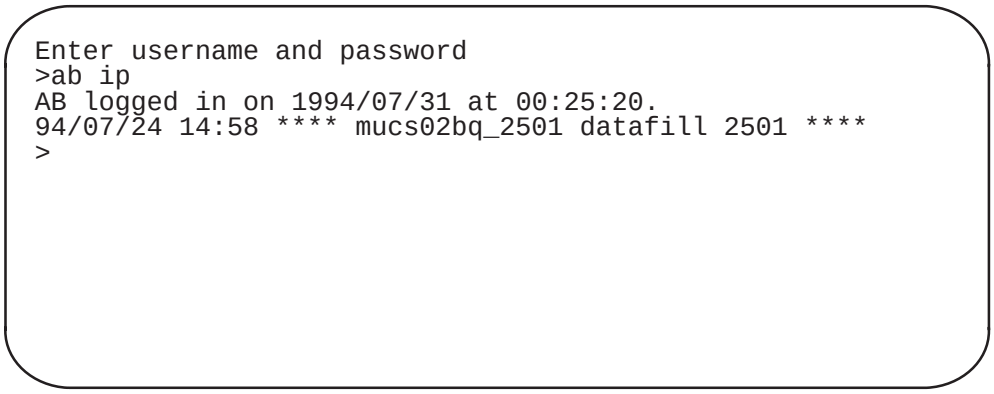


After you have specified a node, Telnet responds with a (“Trying...”) message telling you that it is attempting to make the connection (see Figures 5-2 and 5-3). A second message follows either telling you that the connection has been completed or reporting an error. There may be a pause while the network connection is attempted; this is normal.

Logging into Telnet

After a session is established (a connection to the DMS-500 switch has been made), user login is requested. Log into the switch in the usual manner giving your username and password; you are communicating with the switch just as though you were entering data at a MAP terminal (see Figure 5-4).

Figure 5-4
Logging into a Telnet session



At this point, any standard MAP command and operation may be executed, and output will be a standard MAP response. (For information on standard MAP commands, refer to other NTP documentation.)

Logging out from Telnet

To log out from a Telnet session, enter *logout* at a CI prompt (see Figure 5-5).

Figure 5-5
Logging out from a Telnet session

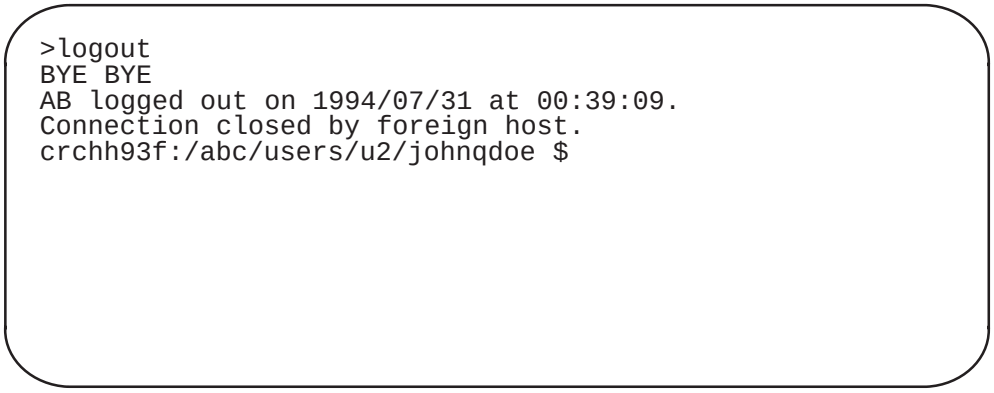


Table datafill

Datafill guidelines

The hardware interacts with the software through the use of the tables described in this section. An interdependence exists between several of these tables. Therefore, the tables must be datafilled in a certain order—as listed and described in this section. Also, consider the restrictions listed in Section 7, “Operations management.”

In preparing software to interact with the hardware, you must

- calculate the number of TCP connections needed and configure the computing module (CM) and Ethernet interface unit (EIU)
- datafill the tables (engineer the switch to do the datafill) which, in turn, activates the software

Calculate TCP connections and configure CM and EIU

Certain criteria must be considered when calculating the number of TCP connections you will need. The following are guidelines for calculating the maximum possible number of TCP connections.

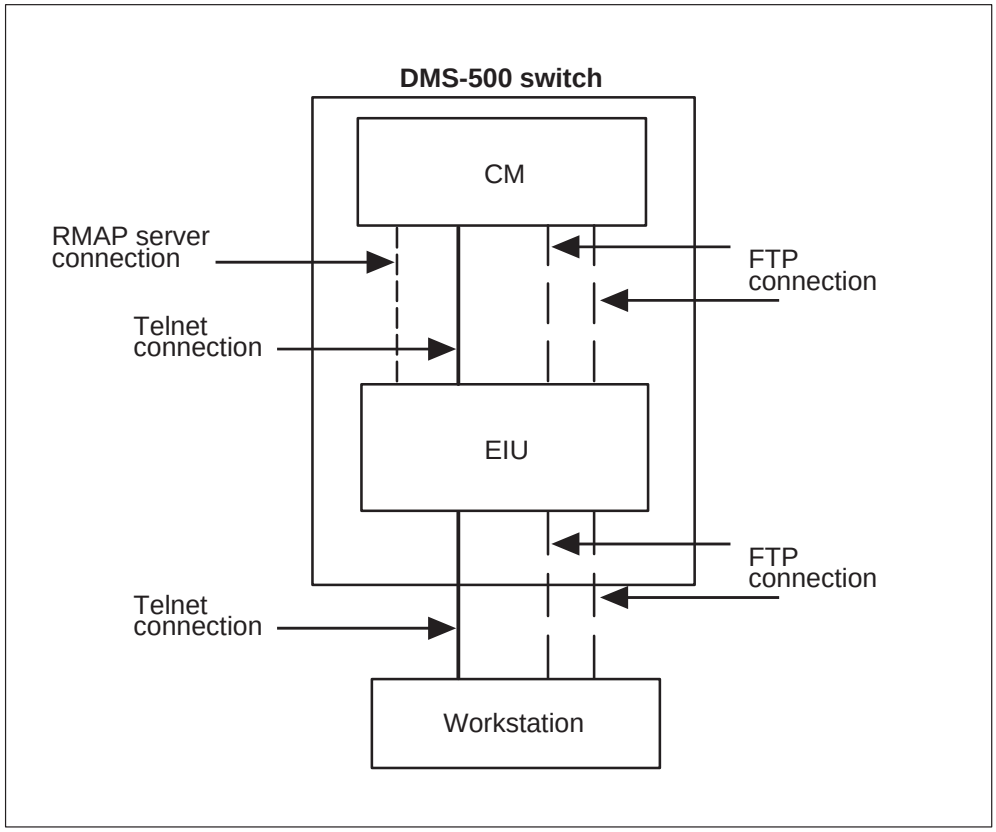
- The maximum number of TCP connections that can be made to a CM or EIU node is 32. The maximum number of Telnet sessions per EIU is 15.
- In table IPHOST, where you datafill TCP endpoints on the CM and EIU, make sure you have enough FTP client and server TCP connections configured for the CM, as well as total TCP connections. You do not need to datafill FTP TCP connections for the EIUs if you won’t be transferring files from the EIU (for example, if you are using the EIU as a router). However, you will need to datafill TCP connections for Telnet connectivity.
  - In addition to current TCP usage, if you want “n” Telnet sessions, you need “n+1” TCP endpoints on the CM and “2n+1” TCP endpoints on the EIU. (The Remote MAP [RMAP] server connection takes up the additional TCP endpoint.) For example, three Telnet sessions require four (3 + 1 = 4) TCP endpoints on the CM and seven ($2 \times 3 = 6 + 1 = 7$) TCP endpoints on the EIU.

— In addition to current TCP usage, if you want “n” FTP client sessions, you must have “n” FTPCLCON connections on the CM and an additional “2n” TCP connections for the CM. These connections are also datafilled in table IPHOST. For example, four FTP sessions require four FTPCLCON connections on the CM. Also, you need eight ($2 \times 4 = 8$) TCP connections for the CM and sixteen ($4 \times 4 = 16$) TCP connections for the EIU.

- In table RMCONFIG, make sure you have enough Telnet TCP connections configured for the CM and EIUs. For example, in table RMCONFIG, make sure you have “n” (3, for example) configured for RMAPCONN on the CM and “n” (3, for example) configured for TELNCONN on the EIU.

Figure 6-1 illustrates one FTP TCP connection and one Telnet TCP connection.

Figure 6-1
One FTP TCP and one Telnet TCP connection



Datafill sequence

To activate the software and provide TCP/IP functionality, the following tables must be datafilled in the order listed:

- table LIUINV
- table IPNETWRK
- table IPHOST
- table IPROUTER
- table IPPROTO
- table IPTHRON
- table RMCONFIG
- table ENSITES
- table ENTYPES
- table EXNDINV

These tables are described on the following pages, with each table beginning at the top of a new page. Table datafill examples are given for each table.

Note: For detailed information on these tables, see the *DMS-500 Data Schema Reference Manual*, 297–2663–851.

Datafilling table LIUINV

Table LIUINV (Link Interface Unit Inventory Table) is datafilled first. This table describes the hardware configuration for all LIUs, including EIUs. Currently, a maximum of four EIUs are allowed per DMS-500 switch. All four EIUs can be on a single link peripheral processor (LPP) or spanned across multiple LPPs.

Table 6-1 describes the fields in table LIUINV.

Table 6-1
Table LIUINV field descriptions

Field Name	Description
LIUNAME	Unique name for the EIU present in the LPP.
LOCATION	Physical location of the EIU by link interface module, shelf, and slot number.
LOAD	Software load name of the load in EIU.
PROCINFO	The Product Engineering Code (PEC) of the particular processor circuit pack.
CARDINFO	The PECs (EIC and EIP) of the EIU circuit packs.
HEARTBEAT	This value (YES or NO) indicates whether or not the EIC is to expect a heartbeat indication from the Media Access Unit (MAU) on the Ethernet LAN. YES is allowed only if the MAU supports heartbeat of Signal Quality Error (SQE). If HEARTBEAT=YES, the SQE dip switch on the MAU must be set to ON. If HEARTBEAT=NO, the MAU SQE dip switch must be set to OFF. If the HEARTBEAT and MAU SQE dip switch do not match as described here, the EIU does not come into service.
MAC_ADDRESS	Media Access Control address for the EIU. This address is represented in hexadecimal format without any spaces. It must be of the form 000075Fxxxxx.

Figure 6-2 provides an example datafill for table LIUINV.

Figure 6-2
Example datafill for table LIUINV

```
TABLE:LIUINV
LIUNAME LOCATION LOAD PROCINFO CARDINFO
----------------------------------------
EIU 102 LIM 0 1 10 ETC02A0 NTEX22BA NT9X84AA NT9X85AA YES 000075F00253
EIU 109 LIM 0 3 10 ETC02A0 NTEX22BA NT9X84AA NT9X85AA YES 000075F00257
EIU 208 LIM 0 2 22 ETC02A0 NTEX22BA NT9X84AA NT9X85AA YES 000075F00254
```

Datafilling table IPNETWRK

Table IPNETWRK (Internet Protocol Network Table) describes the CM node and default EIU and indicates whether or not messages should be screened out so they will not be accepted from certain nodes, based on table EXNDINV.

Table LIUINV must be datafilled before table IPNETWRK. Changes made to the IP address component in table IPNETWRK force automatic reconfiguration of the IP address components of all nodes listed in tables IPHOST and IPROUTER.

Table 6-2 describes the fields in table IPNETWRK.

Table 6-2
Table IPNETWRK field descriptions

Field Name	Description
KEYREF	Unique number entry for CM. Currently, only 0 is allowed.
CMIPADDR	IP address of the DMS-500 CM.
SUBNET	Subnet bitsize of the DMS-500 subnet.
OPTION	Name and number of default EIU to handle messaging.
PARMAREA	Screen Flag. If the flag is set to NO, accept messages without checking table EXNDINV. If the flag is set to YES, accept messages only from nodes datafilled in EXNDINV; otherwise, discard.

Figure 6-3 provides an example datafill for table IPNETWRK.

Figure 6-3
Example datafill for table IPNETWRK

```
TABLE:IPNWETWRK
KEYREF CMIPADDR SUBNET OPTION PARMAREA
---------------------------------------
0 47 96 192 66 19 (EIU 208) (EIU 102) $ (SCRNFLAG N) $
```

Datafilling table IPHOST

Table IPHOST (Internet Protocol SuperNode End Hosts Table) is responsible for configuring DMS nodes as Internet hosts. It activates the TCP layer and its applications on those nodes.

Table IPNETWRK must be datafilled before table IPHOST. IPHOST and IPROUTER are interdependent on each other, as well as on table IPNETWRK. Whenever a tuple in IPHOST is modified, the corresponding tuple, if any, for the same EIU is also modified and automatically configured in table IPROUTER. The changes to both tables are propagated immediately to all in-service nodes. Similarly, changes made to the IP address component in table IPNETWRK force automatic reconfiguration of the IP address components of all nodes listed in tables IPHOST and IPROUTER.

Table 6-3 describes the fields in table IPHOST.

Table 6-3
Table IPHOST field descriptions

Field Name	Description
INDEX	Unique number of table entry.
NODE	Node name and number for EIU or CM. This must match table LIUINV and IPNETWRK.
SNADDR/ SOSADDR	DMS-500 switch side address. Must match table IPROUTER if EIU is datafilled as node and host.
LANADDR	LAN side IP address of EIU.
TCPCONN	Maximum number of TCP connections you plan to use.
FTPSVCON	Maximum number of FTP server sessions allowed.
FTPCLCON	Maximum number of FTP client sessions allowed.
UNXADDR	Optional UNIX side IP address for a file processor.

Figure 6-4 provides an example datafill for table IPHOST.

Figure 6-4
Example datafill for table IPHOST

```
TABLE:IPHOST
INDEX NODENAME NODEINFO
-----------------------
0 CM 0 16 2 2
1 EIU 102 47 96 192 67 47 177 75 4 8 2 2
2 EIU 208 47 96 192 68 47 177 75 5 15 0 0
3 EIU 109 47 96 192 69 47 177 75 6 8 2 2
```

Datafilling table IPROUTER

Table IPROUTER (Internet Protocol Subnet Router Table) contains the list of EIUs and corresponding parameters. This table is required for configuring an EIU as an Internet node.

Table IPNETWRK must be datafilled before table IPROUTER. IPHOST and IPROUTER are interdependent on each other, as well as on table IPNETWRK. Whenever a tuple in IPHOST is modified, the corresponding tuple, if any for the same EIU, is also modified and automatically configured in table IPROUTER. The changes to both tables are propagated immediately to all in-service nodes. Similarly, changes made to the IP address component in table IPNETWRK force automatic reconfiguration of the IP address components of all nodes listed in tables IPHOST and IPROUTER.

Table 6-4 describes the fields in table IPROUTER.

Table 6-4
Table IPROUTER field descriptions

Field Name	Description
ROUTER	Name and number of EIU. This must match table LIUINV and IPNETWRK.
SNIPADR	DMS-500 switch subnet side IP address for EIU. It must match the entry in table IPHOST if EIU is configured as both the node and host.
ETHIPADR	Ethernet LAN subnet side IP address for EIU.
ETHARP	Determines ARP activation/deactivation. ARP implements the Address Resolution Protocol that provides dynamic binding between an IP address and a subnet address.
ETHPARP	Determines Proxy ARP activation/deactivation. This provides for simple IP load balancing between EIUs on the same LAN.

Figure 6-5 provides an example datafill for table IPROUTER.

Figure 6-5
Example datafill for table IPROUTER

```
TABLE:IPROUTER
RKEY ROUTER SNIPADR ETHIPADR ETHARP ETHPARP
-----------------------------------------
0 EIU 102 47 96 192 67 47 177 75 4 YES YES
1 EIU 208 47 96 192 68 47 177 75 5 YES YES
2 EIU 109 47 96 192 69 47 177 75 6 YES YES
```

Datafilling table IPPROTO

Table IPPROTO is rarely used and normally does not need to be datafilled. If there is a serious performance problem, typically on very slow networks, then modification of this table might be considered.

Table 6-5 describes the fields in table IPPROTO.

Table 6-5
Table IPPROTO field descriptions

Field Name	Description
IPRSMTMO	The IP reassembly timeout sets the time when IP reassembly gives up reassembling a message packet. By default, the IP reassembly timeout is 10 seconds. The timeout can be modified to improve performance in extreme network conditions. On extremely slow networks, this may be increased to give reassembly a better chance to reassemble before the timeout occurs.
ARPRFTMO	On slow networks, the ARP cache timeout can be increased from the default of 1. Increasing the timeout too much can cause an excessively large ARP cache, thereby reducing the network performance.

Figure 6-6 provides an example datafill for table IPPROTO.

Figure 6-6
Example datafill for table IPPROTO

```
TABLE:IPPROTO
IPPKEY IPRSMTMO ARPRFTMO
------------------------
0 10 1
```

Datafilling table IPTHRON

Table IPTHRON (Internet Protocol Throttling Numbers Table) contains IP throttling numbers. The IP message flow from DMS-500 hosts requires throttling to control message congestion in the bandwidth-limited shared communication resources between the local message switch (LMS) and message switch (MS). The IP throttling numbers datafilled in this table derive the level of such throttling to and from each of the IP DMS-500 hosts.

An application running on an LPP constitutes a load. Loads must be engineered in such a manner that overloading of shared resources (FBus, TBus, and DS30 links) is prevented. It is especially important to ensure this where CCS7 traffic is present, because an overload of shared resources can currently cause an outage of the LPP and all applications running on it.

Throttling is a control mechanism for TCP/IP traffic across the DS30s between the MS and the LMS of the LPP. The throttling algorithm keeps track of the number of bytes to be transmitted during a 12.5 ms window. There is no credit accumulated from one window to another. This traffic is throttled to values (in kbyte/s) set in table IPTHRON for both the Transmit (Tx) and Receive (Rx) directions. Traffic from one Application Service Unit to another on the same LPP is not throttled. The IPOMSCI OM group indicates when throttling begins.

(See “Restrictions” in Section 7, “Operations management” for additional information.)

The EIU must first be datafilled in table LIUINV before it is allowed in table IPTHRON. This is because as EIUs are automatically datafilled in table LIUINV, a tuple with default values is automatically entered into table IPTHRON.

CAUTION
Throttling capacity fields should not be zeros
The IP throttling numbers default to zero (100% throttling) for all EIUs datafilled in table LIUINV. If the throttling capacity numbers are not datafilled to non-zero values, the EIU cannot communicate to destination nodes across DS30 links.

The default IPTHRON tuple contains zeros for the transmit and receive capacity fields. Features that use the IP protocol via the EIU require correct datafill with non-zero fields. The numbers must be changed to be greater than zero so the EIU can communicate properly.

The EIU is also automatically deleted from table IPTHRON if it is deleted from table LIUINV. The actual values for the fields in this table must be determined carefully with consideration to LPP engineering rules.

Table 6-6 describes the pertinent fields in table IPTHRON.

Table 6-6
Table IPTHRON field descriptions

Field Name	Description
LMSNODE	Key to table entry. The IP capable node located on the LMS; this is the EIU and a valid node index in the range 0 to 750.
TXCAPCT	Total IP transmit capacity in kbyte/s to all DMS hosts across the LMS from the LMSNode. One kbyte is 1024 bytes.
RXCAPCT	Total IP receive capacity in kbyte/s to all DMS hosts across the LMS from the LMSNode. One kbyte is 1024 bytes.

Figure 6-7 provides an example datafill for table IPTHRON.

Figure 6-7
Example datafill for table IPTHRON

```
TABLE:IPTHRON
LMSNODE TXCAPCT RXCAPCT OPTION
----------------------------
EIU 102 32000 32000 $
EIU 109 32000 32000 $
EIU 208 32000 32000 $
```

Datafilling table RMCONFIG

Table RMCONFIG (Remote Access Configuration Table) allows you to configure the number of simultaneous Telnet sessions on the DMS-500 switch by means of table control.

Table 6-7 describes the fields in table RMCONFIG.

Table 6-7
Table RMCONFIG field descriptions

Field Name	Description
INDEX	Unique key.
NODE	CM and/or EIU. One entry for the CM defining the number of RMAP servers on it and a separate entry for each EIU connected to the system defining the number of Telnet servers on it.
SESSIONS	Number of Telnet sessions allowed; maximum 32 for each entry.

Figure 6-8 provides an example datafill for table RMCONFIG.

Figure 6-8
Example datafill for table RMCONFIG

```
TABLE:RMCONFIG
INDEX NODE SESSIONS
------------------
0 CM 30
1 EIU 102 30
2 EIU 109 30
3 EIU 208 30
```

Datafilling table ENSITES

Table ENSITES (Eternal Node Sites Table) contains a complete list of all the sites referenced in table EXNDINV with which a DMS-500 switch is allowed to communicate. If the screening flag in table IPNETWRK is set to NO, this table is disregarded.

Table ENSITES must be datafilled before table EXNDINV.

Table 6-8 describes the fields in table ENSITES.

Table 6-8
Table ENSITES field descriptions

Field Name	Description
ENSITE	Unique key for site. This is a character string, maximum 12 letters, naming the location (usually a building) in which the node is housed.

Figure 6-9 provides an example datafill for table ENSITES.

Figure 6-9
Example datafill for table ENSITES

```
TABLE:ENSITES
ENSITE
------
RICH
```

Datafilling table ENTYPES

Table ENTYPES (External Node Types Table) contains a complete list of all the types referenced in table EXNDINV with which a DMS-500 switch is allowed to communicate. If the screening flag in table IPNETWRK is set to NO, this table is disregarded.

Table ENTYPES must be datafilled before table EXNDINV.

Table 6-9 describes the fields in table ENTYPES.

Table 6-9
Table ENTYPES field descriptions

Field Name	Description
ENTYPE	Unique key. This is a character string, maximum 12 letters, for freeform entry of type of node (such as HP or NCS, for example).

Figure 6-10 provides an example datafill for table ENTYPES.

Figure 6-10
Example datafill for table ENTYPES

```
TABLE:ENTYPES
ENTYPE
------
NCD_WS
```

Datafilling table EXNDINV

Table EXNDINV (External Node Inventory Table) contains information about external nodes connected to the DMS-500 switch by way of an EIU. Each tuple in the table contains node name, address, protocol, and various other information about a node.

This table must be datafilled last.

Table 6-10 describes the fields in table EXNDINV.

Table 6-10
Table EXNDINV field descriptions

Field Name	Description
EXNDKEY	Unique identifier for external node; this is the EXND plus node index in range 0–29.
ENNAME	Unique string name for external node; maximum 12 letters.
ENADDR	Node address type and address. The addrtype may be External IP (ENIP) or External X.25 (ENX25). The IP address is expressed as 4 bytes each ranging from 0 to 255. The X.25 address is a multiple of 4 to 14 digits.
ENFNAME	External Node Filename; maximum 8 characters.
ENSITE	Character string naming the location (usually a building) in which the node is housed. This is the key field of the ENSITES table.
ENLOCN	The location of the node within a building. The three subfields are floor, row, and position.
ENTYPE	A freeform field that contains the type of node (HP, NCD). This is the key of table ENTYPES.
ENINFO	A freeform field that can be used to store any additional information about the node.
ENPROCSR	Set of processor types with which the EXND is allowed to communicate; either CORE, EIU, ALL, or NONE (defaults to CORE).
ENPROTCL	Set of protocols with which the EXND is allowed to communicate with the DMS-500 switch; either ICMP, UDP, TCP, ALL, or NONE (defaults to ICMP).

—continued—

Table 6-10
Table EXNDINV field descriptions (continued)

Field Name	Description
EN0LKALM	Link Alarm for Link 0. Alarm raised if no link available; either NA, MN, MJ, or CR.
EN1LKALM	Link Alarm for Link 1. Alarm raised if no link available; either NA, MN, MJ, or CR.
ENALMSPT	External Node Alarm Scan Point information.
	—end—

Figure 6-11 provides an example datafill for table EXNDINV.

Figure 6-11
Example datafill for table EXNDINV

```
TABLE:EXNDINV
EXNDKEY ENNAME ENADDR ENFNAME ENSITE ENLOCN ENTYPE ENINFO ENPOCSR
ENPROTCL EN0LKALM EN1LKALM ENALMSPT
-------------------------------------
EXND 0 JOHN1 (ENIP 47 122 71 118) $ JOHN2 RICH 2 A 21 NCD_WS
'GREAT' ALLTCP ICMP UDP $ MM NA Y OAU 0 24 0 1 2 DSISIG
```

Operations management

This section lists pertinent operational measurements (OM), logs, and alarms. It also lists some restrictions that should be considered when preparing software to interact with hardware. For more information on OMs and logs, refer to the *DMS-500 Operational Measurements Reference Manual*, 297–2663–814, and the *DMS-500 Logs Reference Manual*, 297–2663–840.

OMs

If failure of any test occurs, the following OM information is collected:

- PM1 group
- NCMCPUST group
- EIUETHER group
- LIUFBUS group

Logs

The following logs may be produced:

- ITN201–206 TCP
- ITN207–208 TCP/PING
- ITN299 TCP
- ITN300–306 IP
- ITN310–313 IP
- ITN399 IP
- ITN400–406 ICMP
- ITN499 ICMP
- ITN501 FTP
- ITN599 FTP
- PM102–106 LAN/EIU
- PM128 EIU

- PM181 LAN/EIU
- RMAP100 Telnet
- TELN100 Telnet
- TELN110 Telnet
- TELN120 Telnet
- TELN130 Telnet
- TELN140 Telnet

Alarms

The following alarm should be investigated if it appears at the External Node (EXND) MAP sublevel:

- EXND

Restrictions

The following restrictions should be considered when preparing software to interact with hardware:

- An External interface unit (EIU) can be datafilled to operate as an IP router, an IP end host, or both. However, an EIU engineered for both functions is not generally desirable for performance reasons.
- In the implementation, EIUs are used only as routers. This means no files can be moved from the EIU to a workstation. Files are only moved from the computing module (CM) to a workstation and from a workstation to the CM.
- An FTP session can only be originated from the DMS-500 switch. It cannot be originated from the workstation.
- The maximum number of TCP connections is 32 per node. Therefore, the maximum number of Telnet sessions per EIU is 15.
- Limited control over EXNDs is provided by way of monitoring and screening. Loading and rebooting of EXND is not provided.
- Screening and subsequent discarding of messaging is done to any EXND not datafilled in table EXNDINV and/or OFFLine when the screen flag is set to YES in table IPNETWRK.
- Screening and subsequent discarding of messaging is done on the basis of protocol and processor class as specified in table EXNDINV.
- All protocol messages required for LAN management will always be delivered regardless of screening. All ICMP messages are delivered to the CM for LAN management maintenance.
- A maximum of 30 EXNDs can be managed from the MAP terminal. This limit was designed for ease of implementation.

- IP expects all other IP implementations on third-party equipment to be able to handle datagrams of 1500 bytes including the IP header.
- The maximum number of DMS-500 end hosts is 64.
- Any one DMS-500 switch cannot be logically partitioned into multiple subnets.
- A DMS-500 end-host can have, at most, two IP addresses.
- The DMS-500 RIP limits destination networks or subnets to 15 hops.
- Certain network topology may take longer than two minutes before traffic is rerouted.
- The DMS-500 PING timing is limited in accuracy depending on which node the user is pinging from: CM (+/–) 1.0 ms, EIU 12.5 ms.
- PING does not give round trip delay time if the packet size is less than 16 bytes.
- An input buffer length restriction of 2048 bytes is imposed by the DMS-500 switch for messages on the DMS bus.
- The Ethernet frame length is limited to 1460 bytes of data and is chosen as the fragment size on the DMS-500 switch to avoid refragmentation by the EIU when sending messages out to Ethernet.
- The Buffer Management System (BMS) buffer limit is 16 kbyte words. This restricts the maximum size of a reassembled message that can be delivered to an upper level protocol.
- Throttle limits are determined from
  - — the smallest message lengths in both Tx and Rx directions for each application
  - — consideration of the impact each application makes to overall traffic

  The smallest message length for Telnet is 1 byte in both directions. FTP sends its messages in 1 kbyte blocks.

  In an example configuration, one EIU is dedicated to FTP. Therefore, throttling is done for FTP apart from Telnet. The other EIU allows Telnet access. Because the Telnet sessions are used for MAP access, a data rate of 2.5 kbyte/s should suffice. For ten Telnet sessions, Rx=25 kbyte/s. Because keyboard input is used for transmitting, Tx=25 kbyte/s. Table IPTHRON will be datafilled with values of Tx=32 kbyte/s and Rx=32 kbyte/s.

- The upper limit on the number of concurrent file transfers for a given node is governed by the number of FTP and TCP connections datafilled.
- The number of FTP connections should not be more than half of the total number of TCP connections.

- Usernames cannot be added via the FTP tool.
- No wild cards are allowed in FTP filenames or paths.
- An FTP user has three attempts in two minutes to successfully login, after which the connection is dropped.

List of abbreviations

ANI
automatic number identification

ARP
Address Resolution Protocol

ARPANET
Advanced Research Projects Agency Network

ASCII
American Standard Code for Information Interchange

AUI
application user interface

BMS
buffer management system

CCS7
Common Channel Signaling 7

CI
command interpreter

CM
computing module

DARPA
Defense Advanced Research Projects Agency

DCP
data communications processor

DDU
disk drive unit

DMOPRO
data modification order process

EIC
Ethernet interface card

EIP
Ethernet interface paddleboard

EIU
Ethernet interface unit

ENSITES
External Node Sites Table

ENTYPES
External Node Types Table

EXND
External Node

EXNDINV
External Node Inventory Table

FBus
Frame Transport Bus

FIT
Fault Insertion Test

FTA
frame transport address

FTP
File Transfer Protocol

GNI
Generic subNet Interface

ICMP
Internet Control Message Protocol

IOC
input/output controller

IP
Internet Protocol

IPF
Integrated Processor and Fbus

IPHOST
Internet Protocol SuperNode End Hosts Table

IPNETWRK
Internet Protocol Network Table

IPROUTER
Internet Protocol Subnet Router Table

IPTHRON
Internet Protocol Throttling Numbers Table

ISO
International Standards Organization

LAN
local area network

LIU
link interface unit

LIUINV
Link Interface Unit Inventory table

LMS
local message switch

LPP
link peripheral processor

MAC
media access control

MAP
maintenance administration position

MAU
media access unit

MS
message switch

OM
operational measurement

OSI
Open Systems Interconnection

PBus
processor bus

PEC
Product Engineering Code

PFS
physical file system

PM
peripheral module

RIP
Routing Information Protocol

RMAP
remote MAP software as implemented in this feature

RMCONFIG
Remote Access Configuration Table

Rx
receive

SNAP
subnetwork access point

SQE
signal quality error

TBus
transactor bus

TCP
Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol (suite of protocols)

Telnet
Telecommunications Network (protocol)

TLI
Transport Layer Interface

Tx

transmit

UDP

User Datagram Protocol

WS

workstation

Appendix A
Frequently asked questions

This appendix contains a group of frequently asked questions and answers. In some cases, the answers are pointers back into the documentation.

What is TCP/IP?

Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of communications protocols including, for example, File Transfer Protocol (FTP) and Telecommunications Network (Telnet). Although the term TCP/IP refers to the entire four-layer stack including applications, TCP and IP are also discrete protocols within the Transport Layer and the Network layer, respectively. See Section 2, “TCP/IP on the DMS-500 switch,” for details on the TCP/IP architecture and for an overview of FTP, Telnet, and other TCP/IP protocols covered in this document.

When do I use FTP and when do I use Telnet?

Use FTP when you need to make a file exchange between hosts. See Section 4, “Using FTP at the switch” for FTP details.

Use Telnet when you want to log in to the switch from a remote location. Telnet allows your workstation to act like a MAP terminal, allowing you to enter MAP commands just as though you were at the switch. See Section 5, “Using Telnet at the workstation” for Telnet details.

Why do I need to have both a MAC address and an IP address?

Each Ethernet interface unit (EIU) has a Media Access Control (MAC) address (also called the Ethernet address) that uniquely identifies it on the Ethernet LAN. The MAC addressing scheme handles addressing at the Link layer while the IP addressing scheme handles addressing at the Network layer. For details on addressing, see Section 3, “Ethernet Interface Unit.”

Who administers the MAC addresses?

The operating company contacts the Northern Telecom (Nortel) Program Manager for MAC address assignment. Although Nortel installs the EIU boards, the operating company provides the AUI cable that connects to it.

Before connecting the cable, the site administrator must know the assigned EIU address (MAC address).

How is the TCP/IP functionality activated?

To activate the software and provide TCP/IP functionality, the following tables must be datafilled in the following order:

- LIUINV
- IPNETWORK
- IPHOST
- IPROUTER
- IPPROTO
- IPTHRON
- RMCONFIG
- ENITES
- ENTYPES
- EXNDINV

For details on table datafill, see Section 6, “Table datafill.”

Can I use FTP to upload table information from a remote workstation? For example, can I upload ANI information to table ANISCUSP?

Yes, provided the FTP session is initiated from the DMS-500 switch. In this application, you use the *get* command. See Section 4, “Using FTP at the switch” for FTP details.

Appendix B
Ordering information

Use the following table for ordering Nortel NTPs (Northern Telecom Publications) and PCLs (Product Content Loads):

Type of product	Source	Phone	Cost
Technical documents (paper or CD-ROM)	Nortel Product Documentation	1-877-662-5669, Option 4 + 1	Yes
Individual NTPs (paper)	Merchandising Order Service	1-800-347-4850	Yes
Marketing documents	Sales and Marketing Information Center (SMIC)	1-800-4NORTEL (1-800-466-7835 * ESN 444-5930)	No
Training documents	Nortel Technical Education Center	1-800-NT-TRAIN (1-800-688-7246)	Yes
PCL software	Nortel	Consult your Nortel sales representative * Employee	Yes

When ordering publications on CD

Please have the CD number and software version available, for example, **HLM-2663-001 02.03**.

When ordering individual paper documents

Please have the document name and number available, for example, **297-2663-900, DMS-500 TOPS User Guide**.

When ordering software

Please have the eight-digit ordering code, for example, **LLT0B005**, as well as the ordering codes for the features you wish to purchase. Contact your Nortel representative for assistance.

Digital Switching Systems

DMS-500

TCP/IP Application Guide

Product Documentation—Dept 3423
Northern Telecom
P.O. Box 13010
RTP, NC 27709–3010
1-877-662-5669, Option 4 + 1

Publication number: 297-2663-340
Product release: LLT00008 and up
Document release: Standard 02.03
Date: August 1998
Printed in the United States of America

NORTEL
NORTHERN TELECOM