HEWLETT PACKARD

HP 12076A LAN/1000 Link

Node Manager's Manual

Software Services and Technology Division
11000 Wolfe Road
Cupertino, CA 95014-9804

Manual Part No.12076-90002
E0394

Printed in U.S.A. March, 1994
Second Edition

NOTICE

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARs 252.227.7013.

Printing History

The Printing History below identifies the edition of this manual and any updates that are included. Periodically, update packages are distributed that contain replacement pages to be merged into the manual, including an updated copy of this printing history page. Also, the update may contain write-in instructions.

Each reprinting of this manual will incorporate all past updates; however, no new information will be added. Thus, the reprinted copy will be identical in content to prior printings of the same edition with its user-inserted update information. New editions of this manual will contain new information, as well as all updates.

First Edition	Nov 1985
Update 1	Dec 1986
Update 2	Sep 1987
Second Edition	Mar 1994

Preface

Purpose

This manual describes the HP Node Manager software provided with the HP 92077A RTE-A product. The Node Manager software is used with the ID*67 driver and HP 12076A LAN/1000 Link product. It is intended for network and system managers, and system support personnel, who are required to implement and maintain an IEEE 802.2/802.3 Local Area Network (LAN) consisting of HP 1000 A-Series computers.

With the information contained in this manual, the Node Manager software can be installed and used to configure nodes on the LAN, log certain events, gather node statistics for network use, and perform limited diagnostics.

Caution There is no security provided by the Node Manager software other than what is available through the RTE-A Operating System. Users of Node Manager software have access to commands that can cause communication failure between nodes, and can render network services inoperative. Limited and controlled access to Node Manager software is recommended.

Assumptions

This manual is intended for System Managers or Support personnel who will install or maintain HP 1000 A-Series computers on an IEEE 802.3 Local Area Network. A working knowledge of the RTE-A Operating System and the IEEE 802.2/802.3 standards is presumed.

Related Reading

The following documents should be available as a reference when reading this manual (system manuals were provided with your system). Additional copies may be obtained from Hewlett-Packard Software Materials Operation (SMO), or through your nearest HP Sales and Support Office:

RTE-A System Design Manual, part number 92077-90013
RTE-A System Generation and Installation Manual, part number 92077-90034
RTE-A User's Manual, part number 92077-90002

HP 12076A LAN/1000 Link Local Area Network Interface Controller Installation Manual, part number 12076-90001

In addition, a library of data communications publications starting with the latest editions of the IEEE 802.2 and 802.3 Standards will be helpful. For information, contact:

Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, N.Y. 10017 U.S.A.

Organization

This manual is organized as follows:

Section 1	introduces the Node Manager software. Along with system requirements, general features and implementation considerations of the software are provided.
Section 2	positions the Hewlett-Packard offering within the framework of the Open Systems Interconnection Reference model and the IEEE 802.2 and 802.3 standards. Transmission frame (packet) structure under the IEEE standards is reviewed. Much of the terminology here is used throughout this manual.
Section 3	discusses LAN driver and Node Manager software installation.
Section 4	describes the structure and operation of Node Manager software.
Section 5	describes the use of Node Manager software. Each of the Node Manager commands and parameter entries is provided.
Section 6	describes remote LANVCP operations. It discusses the software and procedures for downloading a memory-based system to another computer, and for using the remote VCP over the LAN.
Appendix A	provides error codes and descriptions for errors returned by the Node Manager software, the LAN driver, and the LANVCP software.
Appendix B	provides the screen listing contained in the HELP menu. This listing of the Node Manager software command summary may be used for quick reference.
Appendix C	illustrates the relationship among the IEEE 802 family of standards.
Appendix D	provides a history of changes to this manual in summary format.

Table of Contents

Chapter 1
Introduction

Identification 1-1
Installation 1-1
System Requirements 1-1
    Hardware 1-1
    Software 1-3
        System Memory 1-4
        LANVCP Operation 1-5
Node Manager Software Services 1-5
    Configuration Services 1-6
    Statistical Services 1-6
    Diagnostic Services 1-6
    Event Logging Services 1-6
Implementation Considerations 1-7
    Designating Nodes 1-8

Chapter 2
General Information

Open Systems Interconnection Model 2-1
IEEE 802 Service Types 2-3
Transmission Frames 2-3
    Format 2-4
    Field Definitions 2-5
        Preamble 2-5
        Start Frame Delimiter 2-5
        Destination Address 2-5
        Source Address 2-7
        Length 2-7
        Protocol Data Unit 2-8
            Destination Service Access Point (DSAP) Address 2-8
            Source Service Access Point (SSAP) Address 2-10
            Control 2-11
            Information 2-13
        Pad 2-15
        Frame Check Sequence 2-15
    Invalid Frames 2-15

Chapter 3
Software Installation

Installation Summary 3-2
Modules Provided 3-3
Answer File Entries 3-3
    System Relocation 3-3
    Driver Relocation 3-3
    Table Generation 3-4

Memory Allocation 3-6
Generate the New System 3-6
Linking Node Manager Software 3-6
Security/1000 3-6
Using LAN8023.CMD 3-7
Driver and Node Manager Initialization 3-8
Verifying the System 3-9

Chapter 4
Node Manager Operations

Node Manager Modules 4-1
Command Processing 4-2
NM and NM2 Modules 4-2
Command Entry Errors 4-2
NMGR Module 4-3
Command Execution Errors 4-3
Files and Directories 4-4
Root Directory 4-5
Help Menu 4-5
Link File Directories 4-5
MCAST.TXT 4-5
EL.TXT 4-7
Driver Interface 4-8
Logical Units 4-8
Writing Packets 4-8
Reading Packets 4-8
Driver's Class Table 4-8
Packet Routing 4-9
Saving Orphan Packets 4-10
LANIC Card Configuration Data 4-11
RAM & NOVRAM 4-11
Driver's Copy 4-12
Node Manager Software Initialization 4-13
Posting Its Class Number 4-13
Finding Link File Directories 4-15
Other Initialization Considerations 4-16
Entering User Commands 4-16
Initialization Errors 4-16
Post Initialization 4-17
Packet Filter Addressing Modes 4-18
Multiple LANIC Cards 4-20
Disk Access 4-20
Command Routing 4-20

Chapter 5
Using Node Manager

Parameter Notation 5-1
Getting Started 5-2
Running the Node Manager Software 5-2
Exiting the Node Manager Software 5-3
Using the Help Facility 5-3
Entering Commands 5-4
Using the Command Stack 5-4

Error Messages 5-5
Command Entry 5-5
Timeout Error Messages 5-6
Command Execution 5-6
Node Manager Commands 5-7
Parameter Defaults 5-7
Group I: Commands Not Containing the FileAddress Parameter 5-8
Group II: Commands Containing the FileAddress Parameter 5-9
Retrieving the ADR Parameter 5-10
Configuration Commands 5-10
Read Link Configuration Command (RC) 5-11
Multicast Address Considerations 5-11
RC Command Examples 5-13
Set Link Configuration Command (SC) 5-17
Station Address Considerations 5-19
Download Server Station Address Considerations 5-20
File Server Station Address Considerations 5-20
Packet Filter Mode Considerations 5-20
SC Command Examples 5-21
Update Link Configuration Command (UC) 5-22
UC Command Example 5-24
Insert Multicast Address Command (IM) 5-25
IM Command Examples 5-26
Delete Multicast Address Command (DM) 5-27
DM Command Examples 5-28
Create Link File Directories Command (CD) 5-29
CD Command Example 5-30
Purge Link File Directories Command (PD) 5-31
PD Command Example 5-32
Check Link File Existence Command (CK) 5-32
CK Command Examples 5-33
Diagnostic Commands 5-34
The Rep Parameter 5-34
LANIC Self-Test Command (TC) 5-35
TC Command Examples 5-36
Do External Loopback to MAU Command (EL) 5-38
EL Command Examples 5-39
Issue TEST Loopback Command (TEST) 5-41
DSAP Considerations 5-42
Self-Addressed TEST Packets 5-42
Errors 5-42
TEST Command Examples 5-42
XID Command (XID) 5-44
DSAP Considerations 5-45
Self-Addressed XID Packets 5-45
Errors 5-45
XID Command Examples 5-46
Event Log Commands 5-47
Read Event Log File Command (RE) 5-48
List Facility 5-49
RE Command Examples 5-50
Statistics Commands 5-52
Statistics Description 5-54
Read Link Statistics Counters Command (RS) 5-56
RS Command Example 5-57

Zero Link Statistics Counters Command (ZS) 5-58
ZS Command Example 5-58

Chapter 6
LANVCP Operations

Memory-Based System, LAN, and VCP 6-1
Hardware and Software Requirements 6-1
IPL_BUILD and IPL_EDIT − Configuration Files 6-2
Examples 6-4
Format of IPL_TABLE.TXT 6-5
Selecting the System File to Download 6-6
DISPATCH − Monitoring LAN Packets 6-6
VCPMT Monitor 6-7
RMVCP − Remote VCP 6-8
RMVCP Commands 6-8
/BREAK 6-9
/EXIT 6-9
/HELP 6-9
/READ 6-9
/WAIT 6-10
VCP Messages From the Remote Node/Client 6-10
Examples 6-11
RMVCP Memory Dump Session 6-12
Downloading Over a LAN Link 6-13

Appendix A
Error Codes & Descriptions

NMGR Error Codes A-1
Driver Error Codes A-2
LANVCP Error Codes A-3

Appendix B
NM Command Summary

Appendix C
IEEE 802 Family Relationships

Appendix D
Record of Changes

List of Illustrations

Figure 1-1	HP 1000 A-Series Connected to an IEEE 802.3 LAN	1-2
Figure 1-2	Node Manager Software Relationships	1-4
Figure 1-3	Node Manager Software Services	1-5
Figure 2-1	Layers of the OSI Model	2-1
Figure 2-2	HP 12076A Relationships to Standards	2-2
Figure 2-3	IEEE 802.3 Frame and Location of IEEE 802.2 Sublayer	2-4
Figure 2-4	IEEE 802.2 Sublayer Fields	2-4
Figure 4-1	NM Software Modules	4-1
Figure 4-2	Typical User Command Processing Through Node Manager Modules	4-2
Figure 4-3	Link Files in File Server Node	4-4
Figure 4-4	Node Manager Software Initialization for Posting Class Numbers	4-14
Figure 5-1	Deciphering the Packet Error Byte, ERR#	5-49
Figure C-1	IEEE 802 Family Relationships	C-1

Tables

Table 4-1	Initial Factory Settings Contained in NOVRAM	4-12
Table 4-2	Receive Packet Filter Modes	4-19
Table 5-1	ADR and LU# Defaults for Group I Commands	5-8
Table 5-2	ADR, FileAddress, and LU# Defaults for Group II Commands	5-9
Table 5-3	Definitions of the RC Command Parameter, PAR#	5-12
Table 5-4	Receive Packet Filter Mode Settings	5-12
Table 5-5	LANIC Card Status Bit Definitions	5-15
Table 5-6	SC PAR# Definitions	5-18
Table 5-7	PAR-Value Range	5-19
Table 5-8	Interpretation of TC Command Self-Test Failed Bits	5-36
Table 5-9	Interpretation of EL Loopback Test Bits	5-39
Table 5-10	IEEE 802.2 Control Field Designations	5-49
Table 5-11	Statistics Information Summary	5-53
Table A-1	Command Execution Errors Returned by the NMGR Module	A-1
Table A-2	Driver Error Codes	A-2

1

Introduction

The HP Node Manager software is a utility for administering HP 1000 A-Series computers as nodes (or “links”) on an IEEE 802.2/802.3 Local Area Network (LAN). Because it contains a subset of Network Link Management services, the Node Manager software provides for the testing, monitoring, and management of both local and remote nodes on the LAN. This manual will provide you with the information to install and use the Node Manager software.

Identification

The Node Manager and LAN driver software associated with the LAN/1000 Link product are provided with the RTE-A Operating System, product number HP 92077A. Modules associated with the software have part numbers with prefix 91830 (that is, 91830-xxxxx).

Installation

Node Manager software is normally installed with the interface driver (ID*67) on each A-Series computer attached to the LAN. For LAN driver (ID*67) and Node Manager software installation information, refer to Chapter 3.

System Requirements

Hardware

Node Manager software operates on HP 1000 A-Series computers that are connected to an IEEE 802.3 Local Area Network (LAN). Figure 1-1 illustrates this connection.

Although Figure 1-1 shows only one card per host computer, the Node Manager software can manage or will work with up to eight *Local Area Network Interface Controller* (LANIC) cards.

As Figure 1-1 illustrates, a LANIC card connects to the IEEE 802 LAN through an IEEE 802.3 card edge connector cable, an Attachment Unit Interface (AUI) cable, and a Medium Attachment Unit (MAU).

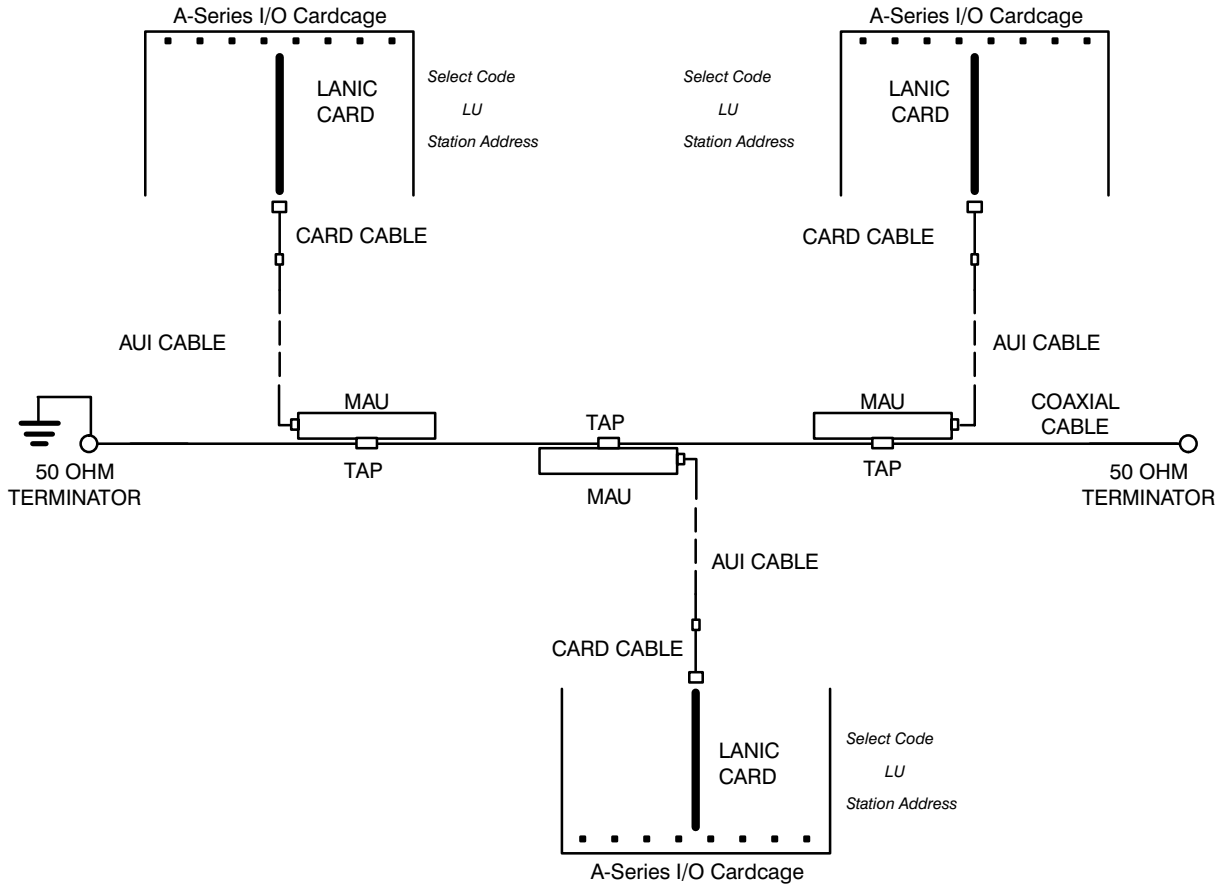


Figure 1-1. HP 1000 A-Series Connected to an IEEE 802.3 LAN

There are several system requirements associated with each LANIC:

Select Code — The select code is an octal number that is set by switches located on the LANIC. Each LANIC card (or any I/O card for that matter) installed in a host computer must have a unique select code (see the *HP 12076A LAN/1000 Link Local Area Network Interface Controller Installation Manual*, part number 12076-90001, for switch location and setting information).

Logical Unit Numbers — Each LANIC card installed in a host computer requires one logical unit (LU) number. This number is unique in the host system and is set during system generation where it is mapped to the card's select code (see the *HP 12076A LAN/1000 Link Local Area Network Interface Controller Installation Manual*, part number 12076-90001, for additional information).

Station Address

Each LANIC card in the network is identified by a unique number called a Station Address. This is a 12-digit hexadecimal number. When shipped from the factory, each LANIC contains a globally administered Station Address stored in (and labeled on) nonvolatile static RAM (NOVRAM). Globally administered means that, in addition to Hewlett-Packard, it is unique across manufacturers. This address can be altered from Node Manager software.

Note that a LANIC card's select code and LU number are unique only to its host computer system, while its Station Address is unique to the LAN.

When a single computer system is connected to several separate LANs (that is, it contains multiple LANIC cards), each LANIC card installed must still contain a unique station address for proper Node Manager software operation.

Software

The HP Node Manager software operates under the RTE-A Operating System and accesses interface driver ID*67. This is depicted in Figure 1-2.

In addition, Figure 1-2 positions HP Node Manager software relative to other network related software operating on the system. Generally, this includes applications that utilize network services such as remote file transfer, remote virtual terminal access, or remote process communication. Application and network services software may be supplied by the user or Hewlett-Packard. (Consult your nearest Sales and Support Office for the latest availability of Hewlett-Packard networking products.)

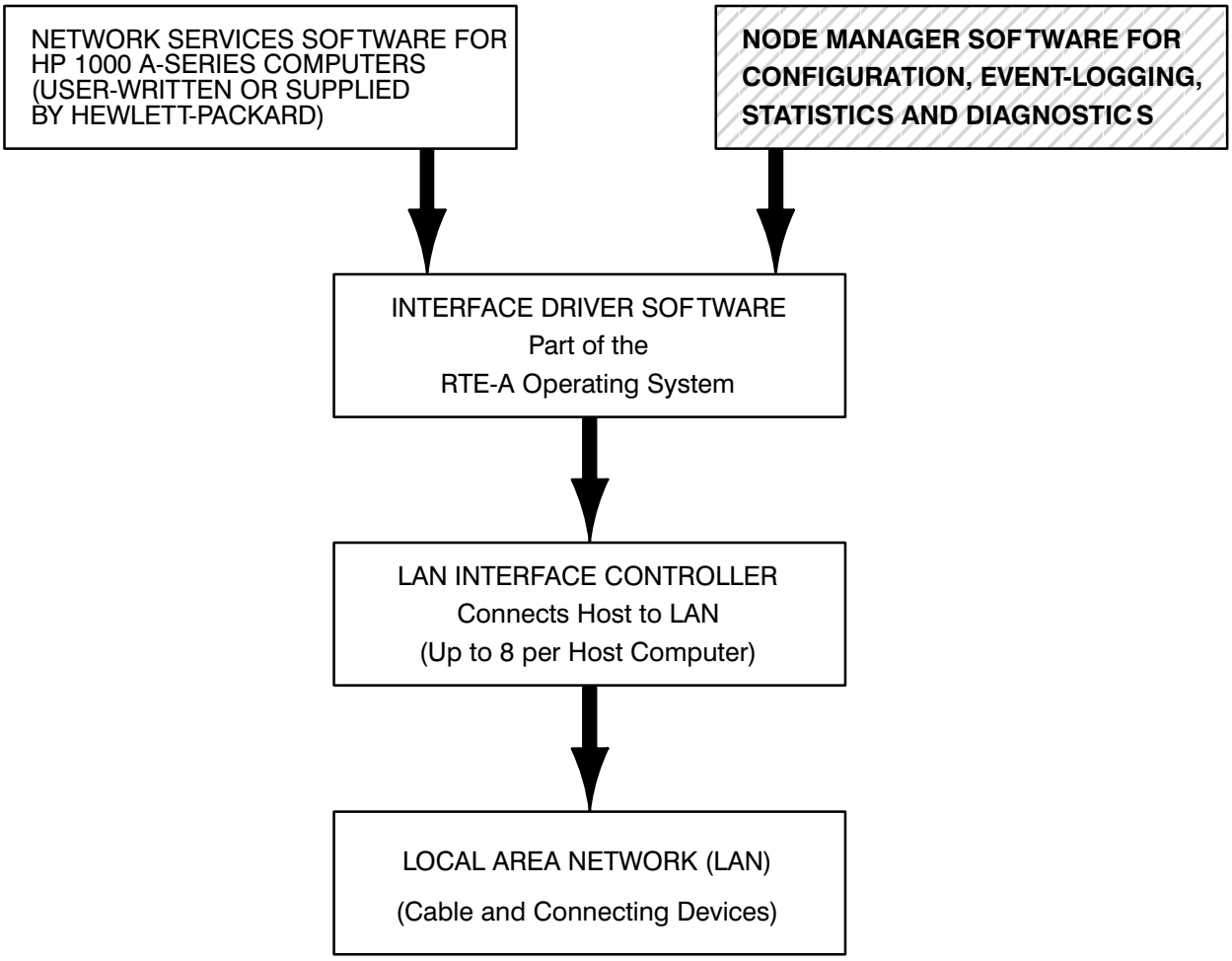


Figure 1-2. Node Manager Software Relationships

System Memory

Node Manager software uses approximately 85 pages (1 Kword per page) of system memory for operation. It consists primarily of three modules with approximate requirements as follows:

NM	: 32 pages
NM2	: 25 pages
NMGR	: 26 pages

During system generation and installation, memory must be allocated for class numbers (refer to Chapter 3). Node Manager software requires two class numbers for proper operation.

LANVCP Operation

LAN Virtual Control Panel (LANVCP) server software for downloading systems or controlling "front panel" operations of a remote node is provided with VC+ (HP 92078A). For a given LANIC card, the LANVCP server software and the Node Manager software receive packets through the same "channel", which is governed by the design of the driver and other software. An intermediate program, DISPATCH, is provided to inspect and properly route incoming packets to the appropriate program or software module. DISPATCH must be used when both the Node Manager and other LANVCP software access the same LANIC card.

The server software required for LANVCP operation are the following modules: DISPATCH, RMVCP, VCPMT, IPL_BUILD and IPL_EDIT. These modules are shipped in the /VCPLUS/LANVCP directory. LANVCP operation and these required modules are described in more detail in Chapter 6.

Node Manager Software Services

The Node Manager software provides four primary categories of services: Configuration, Statistics, Diagnostics and Event Logging. Since Node Manager software at one node can "talk to" Node Manager software at another node, these services may be accessed locally or remotely. This is illustrated in Figure 1-3.

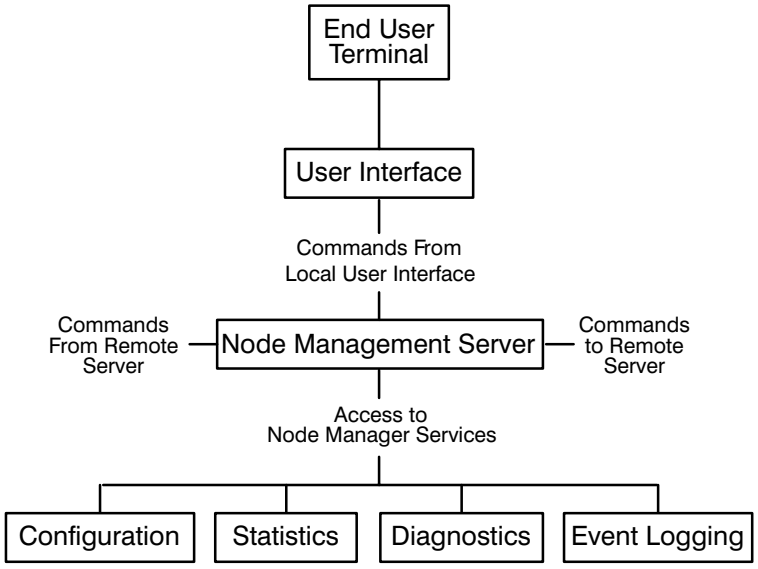


Figure 1-3. Node Manager Software Services

Configuration Services

Node Manager software may be used to configure a node. Configuration refers to the setting of various interface card and driver parameters that govern a node's behavior, as well as maintaining special data in software directories and files.

For example, a node may be configured into one or more modes for receiving and accepting packets from the LAN. These Packet Filter Modes (Individual, Multicast, Broadcast, and Promiscuous) are described later.

In addition, a node's Station Address and Download Server Station Address stored on the LANIC card may be temporarily or permanently altered.

Other items configurable include the node's Retry Limit, and whether or not to save and log "bad" or "trace" packets. These and others will be discussed in detail later in this manual.

Statistical Services

Node Manager software may be used to access and provide a number of useful statistics of node performance. These include, for example, "Good Bytes" transmitted, "Good Packets" transmitted, transmission errors, receiving errors, collisions, and packets discarded. In addition, the statistical counters may be reset. A complete list of statistical data available and how to retrieve it (local and remote nodes) are provided later in this manual.

Diagnostic Services

Node Manager software can be used for limited diagnostics of the local node, and of a remote node if communications to the remote Node Manager software remains intact.

For example, you can initiate an interface card self-test that checks card hardware and firmware operation. For the integrity of the connection between the interface card and LAN coaxial cable, you can initiate an External Loopback test. In addition, special IEEE 802.3 packets (TEST, and XID packets) may be transmitted to remote nodes, where they are processed and returned.

Finally, Node Manager software can check for the existence of applicable files and directories of both local and remote nodes.

Event Logging Services

On occasion, received packets cannot be delivered to an intended program ("orphan" packets), or do not meet IEEE 802.2/802.3 criteria ("bad" packets). Or, it may be desirable to track unsuccessfully transmitted packets ("trace" packets). When a node is properly configured, the Node Manager software will log key information from these packets to an Event Log file saved on disk. This information may be accessed through Node Manager software for examination and analysis. Further details of this feature are provided later.

Implementation Considerations

Depending on a node's function, Node Manager software may be implemented at three basic levels. These are illustrated in Table 1-1.

Table 1-1. Types of Nodes

Type	Description	When Used
Slave Node	Disk- or memory-based nodes that provide Node Manager Server duties from remote nodes only.	Minimum configuration nodes used to execute-only Node Manager commands.
Manager Node	Preferably disk-based, but may be memory-based nodes, that provide Node Manager Server duties from a local User Interface and from remote nodes.	Used to manage local or remote nodes, any of which may be slave nodes. At least one LAN/1000 node must be a Manager Node.
File Server Node	A disk-based Manager Node that stores and maintains special link file data of the local and remote nodes (usually memory-based nodes).	Used to store special link data of nodes being managed (including itself). Managed nodes access this data through Node Manager software.

Slave nodes are those operating with the minimum number of Node Manager software modules. They are execute-only nodes, and report to another system concerning their current status. You cannot directly access Node Manager software from a Slave node because it does not contain the Node Manager User Interface modules needed. Each HP 1000 A-Series computer on the LAN should have this level of Node Manager software installed.

In Manager Nodes, all Node Manager software modules are installed. Each node on the LAN that is running Node Manager software should be accessible to a designated Manager Node. It is recommended that Manager Nodes be disk-based, but this is not required. Also, more than one node on a LAN may be designated as a Manager Node.

A File Server Node also contains all Node Manager software modules, but must be disk-based. It is used to "permanently" save certain link information of designated nodes in files on disk (Event Log, and Multicast Address list). Because of its node-to-node communication capability, Node Manager software can retrieve and update this information over the LAN.

File Server Nodes perform these services for itself, and memory-based or disk-based nodes. They allow a centralized network management approach for the collection of link data from a group of nodes. More than one node on a LAN may serve as a File Server Node when the applicable nodes are properly configured.

Designating Nodes

Designating nodes on a LAN to one or more of the above types is application dependent. The following should be considered:

Economy	If the network considerations dictate that a disk is not needed at a particular node, then a minimum system for execute-only capabilities may be a good choice. If this is the case, a Slave Node containing only the Node Manager software File Server module (NMGR, described later) is configured. This module requires approximately 26-pages of physical memory.
Performance	Software overhead and disk accesses by Node Manager software may impact node performance. Depending on the application, network accesses by Node Manager may add to network traffic, but this should be negligible. Slave Nodes might be considered for high performance, execute-only applications, and are normally configured to update or retrieve file data at a remote disk-based node over the LAN. At least one HP 1000 node on the LAN must be a Manager Node and contain all Node Manager software modules. If file storage for other nodes on the network is required, it may be a File Server node as well.
Security	The Node Manager software is a powerful utility with significant impact on LAN operations. Security will depend upon the user's selective configuration of Node Manager software modules operating on any particular node. The Node Manager "User Interface" modules (NM and NM2, described later) installed on a node will permit users to reconfigure the network virtually without restriction. For this reason, it is recommended that User Interface modules be configured only on nodes where the person designated as the Network Manager exercises direct control.
High Availability	Maximum uptime operation for the network or individual nodes may be important. Individual nodes that fail may lose their link configuration data. File Server Nodes maintaining this information on disk should be located in areas least likely to be disturbed. A distribution of File Server Nodes around the network may help to minimize the number of nodes downed by a failed File Server Node. In continuous process applications, battery backup and spare LANIC cards at Manager and File Server Nodes may be considered.

2

General Information

This section provides the foundation for understanding the underlying operation of the Node Manager software.

If you are already familiar with IEEE 802.2 and 802.3 terminology and concepts, this section may be a review. However, it also contains specific information regarding the Hewlett-Packard implementation of the standards.

Open Systems Interconnection Model

Hewlett-Packard's Local Area Networking implementation was guided by the International Standards Organization (ISO) *Open Systems Interconnection* (OSI) reference model. The model is based on a layered architecture that facilitates a modular approach for network communications development. The seven layers of the model are shown in Figure 2-1.

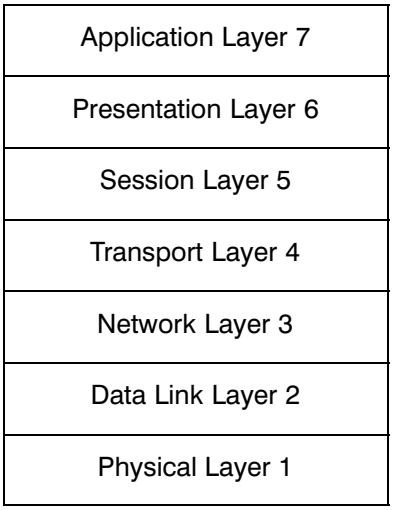


Figure 2-1. Layers of the OSI Model

Along with the LAN coaxial cable, the hardware provided with the HP 12076A LAN/1000 Link product and the driver satisfy the first two layers of the OSI model by conforming to the Institute of Electrical and Electronic Engineers (IEEE) standards 802.2 Type 1 and 802.3. The relationships among the HP 12076A, IEEE standards, and OSI model are shown in Figure 2-2.

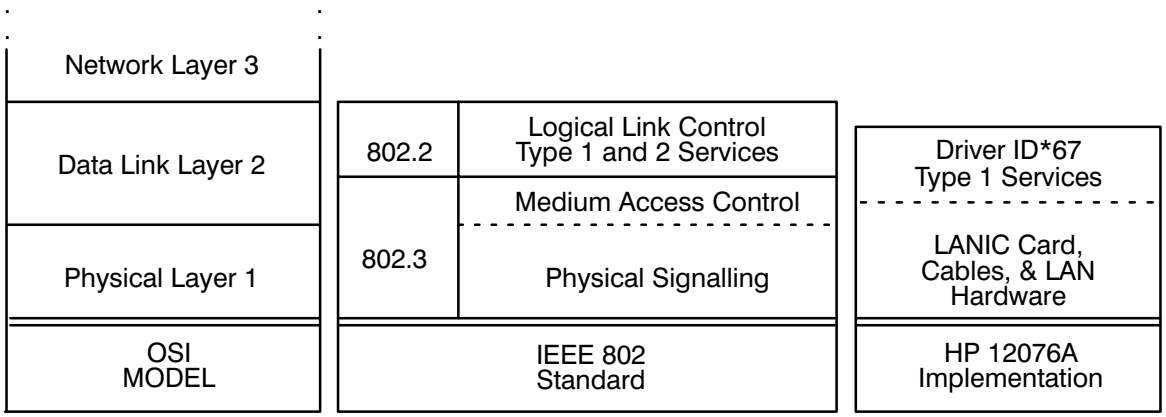


Figure 2-2. HP 12076A Relationships to Standards

Useful communications with other computer nodes, other local area networks, or other general networks may be accomplished by meeting the additional requirements of OSI layers 3 through 7. These layers may be met by software supplied by the user, third parties, and Hewlett-Packard. (Consult your nearest HP Sales and Support Office for the availability of networking software products.)

Note Although it accesses the LANIC card driver, the HP Node Manager software should not be misconstrued as meeting or containing layers 3 through 7 of the OSI model. As a tool for performing various Network Management services on an IEEE 802.3 LAN, it does conform to a Hewlett-Packard *Network Management Architecture* that employs a special HP *Network Management Protocol*.

IEEE 802 Service Types

The IEEE standards allow two types of services that can be provided to the next layer of software:

Type 1	designates unacknowledged connectionless service. A successfully transmitted packet is presumed to be received by a receiving node. There is no requirement at the physical or data link layers for the receiving node to acknowledge packet receipt.
Type 2	designates connection-oriented services. A data link layer connection must be established, and there is flow control and error recovery. A sending node is guaranteed that its successfully transmitted packet was properly received by the receiving node.

Class 1 stations support Type 1 services only, whereas **Class 2** stations support Type 1 *and* Type 2 services at the data link layer.

Note Hewlett-Packard's implementation at the driver and interface card level is for Class 1 stations. Type 2 services, if required, are provided in higher levels of software. For example, some HP Node Manager software transmissions require replies from remote nodes; improper or response failure result in retransmission or error messages to the user.

Transmission Frames

When transmitted or received on the LAN coaxial cable medium, a bit stream that conforms to the IEEE 802.3 Standard is called a *frame*. Communications over the LAN is conducted through the transfer of one or more frames.

Note In this manual, the terms "frames" and "packets" are generally used interchangeably. Although "frame" is more aptly used in physical transmission level discussions, while "packet" applies more to data exchange in higher levels of software, the use of "packet" has grown through common usage. Note, however, that a packet at one level may be quite different from a packet at another, and care should be taken to avoid confusion. It is hoped that usage here is self-evident and clear.

Format

An IEEE 802.3 packet (or more properly, Medium Access Control Frame) consists of eight (8) fields. A packet starts with a Preamble, and ends with a Frame Check Sequence. One of the fields, the Protocol Data Unit, is used to implement the Logical Link Control protocol defined by the IEEE 802.2 Standard. This is illustrated in Figure 2-3. Under the IEEE 802.2 Standard, the Protocol Data Unit field is further divided into additional fields, as illustrated in Figure 2-4.

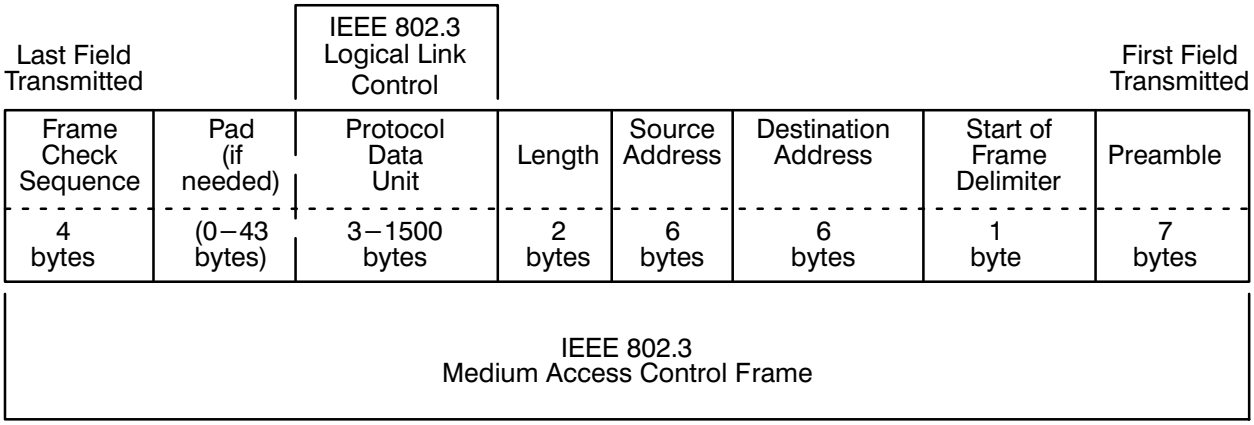


Figure 2-3. IEEE 802.3 Frame and Location of IEEE 802.2 Sublayer

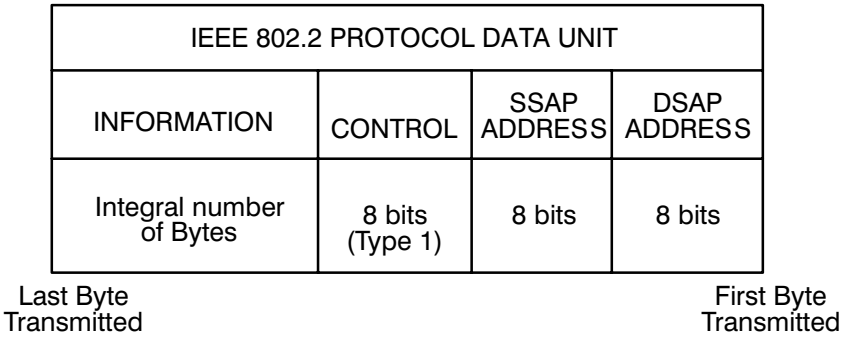


Figure 2-4. IEEE 802.2 Sublayer Fields

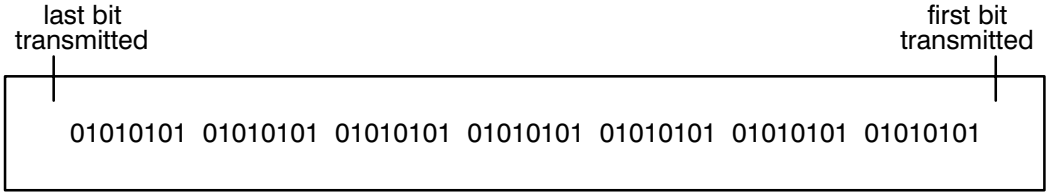
Standard or custom communication protocols between higher layer processes are employed in the Information field of the Protocol Data Unit. For example, Node Manager software communications between a local and remote node is accomplished through a Hewlett-Packard Network Management protocol embedded in the Protocol Data Unit Information field.

Excluding the Preamble and Start Frame Delimiter, a packet must be at least 64 bytes, and can be up to 1518 bytes long.

Field Definitions

Preamble

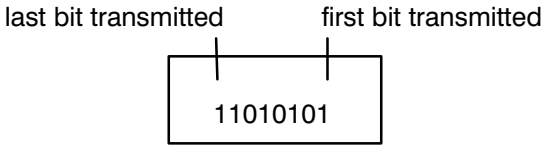
The Preamble consists of seven (7) bytes of alternating “1s” and “0s”, as shown below. It is inserted into a transmitted packet by LANIC card hardware. For received packets, the LANIC card uses the preamble for signal synchronization. The preamble is not incorporated into the Frame Check Sequence algorithm.



Preamble Sequence

Start Frame Delimiter

The Start Frame Delimiter is a single byte that marks the start of the frame. It is also inserted into the packet by the LANIC card hardware. It is not included in the Frame Check Sequence algorithm.



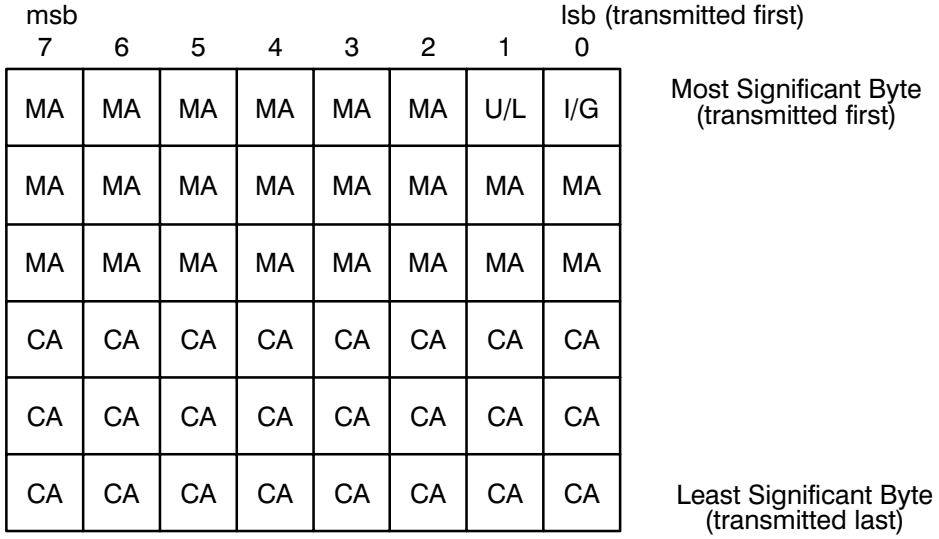
Start Frame Delimiter Byte

Destination Address

The Destination Address field is used to specify the node, or nodes, for which a packet is intended. For an individual node, it is the station address of the LANIC card. For a group of nodes, it is the “Multicast Address” configured in those nodes. For all IEEE 802.3 nodes on the LAN, it is the “Broadcast Address”. These addresses are discussed below.

Note The Node Manager software can be used for configuring the LANIC card’s mode for receiving packets based on the packet’s Destination Address. This is discussed in Chapters 4 and 5.

The Destination Address field is 48 bits (6 bytes) long, as follows: (In this manual, the Destination Address is normally expressed as a 12-digit hexadecimal number.)



where:

CA = Card Address bits comprising the lower six hex digits

MA = Manufacturer's Address bits. Note that the two least significant bits of the most significant byte have the following meanings:

U/L = 0 Globally Administered Address
= 1 Locally Administered Address

I/G = 0 Individual node address
= 1 Group of nodes address

The U/L (Universal/Local) bit determines whether the address is globally administered, or locally administered. A "globally administered address" implies a universally unique address as administered by the IEEE. When shipped from the factory, each Hewlett-Packard LANIC card contains such an address: a unique Manufacturer's Address (08 00 09 hex) assigned to Hewlett-Packard, and the lower six hex digits assigned by Hewlett-Packard. A "locally administered address" is controlled by the user, and is probably not universally unique.

The I/G bit defines the Destination Address as an individual or group address. An "individual" address is associated with a particular station on the network and implies that a single LANIC card is addressed, whereas a "group" address implies more than one station (or card) is addressed.

A group address in the Destination Address Field refers to a "Multicast" or "Broadcast" address. In addition to its individual address, each LANIC card on the LAN can be configured to accept common addresses shared by subgroups of LANIC cards. Such addresses are referred to as "Multicast" addresses; a node's Multicast Address List allows a node to be tied to several different subgroups for receiving common packets.

A "Broadcast" address is a multicast address that denotes the set of all stations on a LAN. It is predefined by the IEEE to consist of all "1s" in the Destination Address Field. By convention and

under firmware control, each LANIC card on the LAN will accept a packet that contains a Broadcast Destination Address.

An example of a Destination Address Field containing the address 08 00 09 00 02 0B (hex) is shown below. Because the first two digits are 08, it is a globally administered, individual station address (U/L and I/G bits are both “0”).

msb 7	6	5	4	3	2	1	lsb (transmitted first) 0	
0	0	0	0	1	0	0=U	0=I	08 (hexadecimal)
0	0	0	0	0	0	0	0	00
0	0	0	0	1	0	0	1	09
0	0	0	0	0	0	0	0	00
0	0	0	0	0	0	1	0	02
0	0	0	0	1	0	1	1	0B

Example of Destination Address Field with address 08 00 09 00 02 0B (hex)

Source Address

The Source Address field contains the Station Address of the LANIC card from which a packet is sent. It is the same length as the Destination Address field.

When the Node Manager software formats a packet for transmission, empty space is allocated for the Source Address. The LANIC card inserts the Station Address stored on the card into this space.

Length

The Length field provides the number of valid data bytes that follow in the Protocol Data Unit field. For an IEEE 802.2 and 802.3 packet, the Length field can be 1500 (decimal) bytes maximum. Note that for short data fields, the Length field should not include the invalid data inserted by the “pad” function discussed later.

Protocol Data Unit

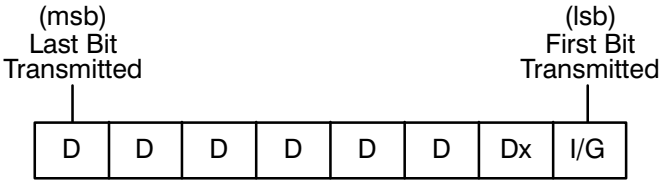
The Protocol Data Unit field contains data to implement the IEEE 802.2 Logical Link Control protocol, and to implement higher layers of software protocol for peer-to-peer communication processes (such as Node Manager-to-Node Manager software residing on separate nodes). The number of bytes of valid data (up to 1500 bytes) is specified by the Length field. If valid data is less than 46 bytes, a Pad field is automatically added by the LANIC card to maintain minimum packet transmission size.

The Protocol Data Unit is comprised of the DSAP, SSAP, and Information fields (as defined by the IEEE 802.2 Standard). Each of these fields is described next.

Destination Service Access Point (DSAP) Address

The Logical Link Control DSAP field contains a single address that identifies one or more service access points (SAPs) to which the information field is directed. (SAP addresses generally provide the logical connections with Network Layer processes of the OSI model.) When it identifies one service access point, or Network Layer process, it is an "Individual DSAP". When it identifies multiple service access points, it is a "Group DSAP". The format of the DSAP address field is described below.

Note Hewlett-Packard software does not support operation with packets containing a Group DSAP. For operation with Group DSAP packets, user-written routines are required. Refer to the *HP 12079A LAN/1000 Link Direct Driver Access Manual* product, part number 12079-90001, for additional information.



DSAP Address Field

where:

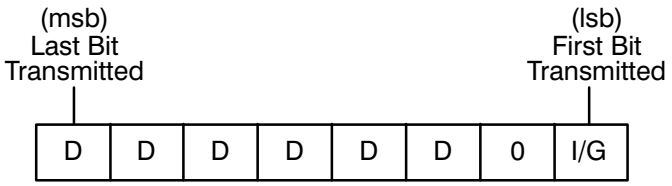
D represents a DSAP address bit.

Dx
0 indicates the DSAP is locally administered (user-defined)
1 indicates it is administered by the IEEE (see below)

I/G is an Individual/Group type designation bit indicating whether the packet data is directed to an individual DSAP or a Group DSAP, as follows:

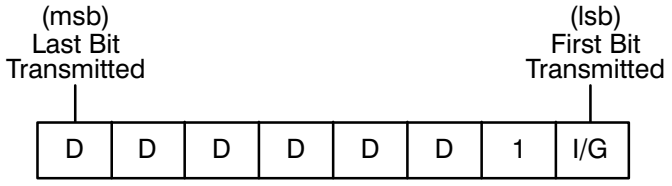
I/G = 0 Individual DSAP, intended for a single process
I/G = 1 Group DSAP, intended for more than one process

A legal (user-defined) DSAP address takes the following form (note the “0” in the second bit):



Legal DSAP Address

Certain DSAPs are defined by the IEEE 802.2 Standard for reserved use, that is, they are administered by the IEEE. They are of the following form (note the “1” in the second bit):



Reserved DSAP Address for IEEE 802 Definition

For example, the IEEE administers the following DSAP values as follows:

DSAP Value	Description
FF (hex)	Global DSAP, consisting of the I/G bit set to “1”, and the seven DSAP address bits set to “1”. The Global DSAP designates the group of all active DSAPs to receive the packet data.
02 (hex)	DSAP for individual Logical Link Control management functions (as defined by the IEEE), consisting of the I/G bit set to “0”, and the seven DSAP address bits set to “0000001”. (Do not associate this DSAP with the Hewlett-Packard Node Manager software.)
03 (hex)	DSAP for group Logical Link Control management functions, consisting of the I/G bit set to “1”, and the seven DSAP address bits set to “0000001”.
06 (hex)	DSAP for Internet Protocol (IP), based upon a Defense Advanced Research Projects Agency (DARPA) standard for an internetwork protocol. The I/G bit is set to “0”, and the seven DSAP address bits are set to “0000011”. (Note: HP networking software uses IP and therefore requires the use of this DSAP. This is in addition to HP reserved SAPs described below.)

A special predefined value is the “Null” DSAP. The Null address neither identifies a Network Layer process nor management function. Instead, it addresses the Medium Access Control sublayer, which in this case is the LANIC card and firmware.

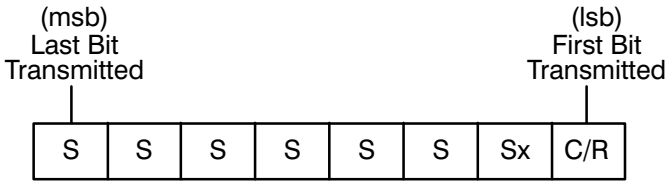
00 (hex)	Null DSAP, consisting of the I/G bit set to “0” and the seven DSAP address bits set to “0”. With the HP 12076A implementation, the card firmware detects a Null DSAP in incoming XID or TEST packets (defined later) and responds appropriately. The driver and upper level software are not accessed.

Hewlett-Packard reserves certain SAPs for operation of HP software. They are:

F0 (hex):	(reserved)
F4 (hex):	HP Link Level LAN Diagnostic Software DSAP
F8 (hex):	HP Network and Node Manager Software DSAP (also may be used for remote VCP and FCL)
FC (hex):	HP Network Services DSAP for PROBE protocol

Source Service Access Point (SSAP) Address

The Logical Link Control SSAP field contains a single address that identifies a service access point (SAP) from which the information field is sent. (Note that Group SSAPs are not defined.) The format of the SSAP address field is as follows:

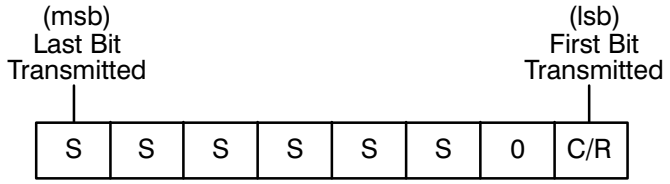


SSAP Address Field

where:

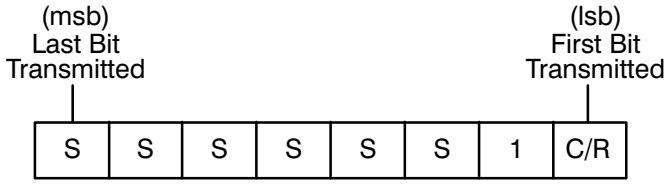
S	indicates SSAP address bits
Sx	0 indicates the SSAP is locally administered (user-defined) 1 indicates it is administered by the IEEE (see below)
C/R	is a Command/Response bit indicating whether the packet data from this SSAP is an initial outgoing command, or a response resulting from some previous incoming command, as follows: C/R = 0 Packet data is a command from this SSAP C/R = 1 Packet data is a response from this SSAP

A legal (user-defined) SSAP address takes the following form (note the "0" in the second bit):



Legal SSAP Address

Similar to DSAPs, certain SSAPs are administered by the IEEE and take the following form (note the second bit is set to "1"):



Reserved SSAP Address for IEEE 802 Definition

For example, the following SSAPs are reserved and defined by the IEEE:

SSAP Value	Description
02 (hex)	Command from an individual Logical Link Control management function SSAP (as defined by the IEEE). (Do not associate this SSAP with HP Node Management software.)
03 (hex)	Response from an individual Logical Link Control management function SSAP.
06 (hex)	Internet Protocol (IP) SAP. IP, which is based on a Defense Advanced Research Projects Agency (DARPA) standard for an internetwork protocol, is used by HP networking software.

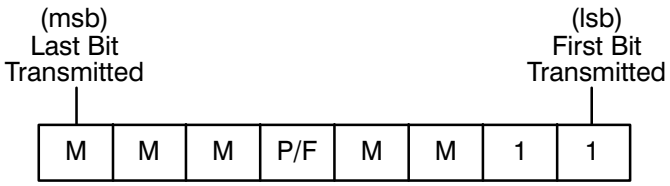
Null SSAPs are also predefined.

00 (hex)	Command Null SSAP. This SSAP originates from the Medium Access Control sublayer (that is, the LANIC card and firmware).
01 (hex)	Response Null SSAP. This SSAP also originates from the Medium Access Control sublayer.

Control

The Control field specifies the interpretation of the data in the Information field. The Control field can assume an 8-bit or 16-bit format as defined by the IEEE 802.2 Standard. The 16-bit format contains additional information to allow flow control and error recovery. Thus, the 16-bit format applies when Type 2 services are provided.

The Hewlett-Packard implementation provides Type 1 services only, where the 8-bit Control field applies. The 8-bit format is referred to as "Unnumbered", or "U-Format", Protocol Data Units. In this case, the Control field structure is as follows:



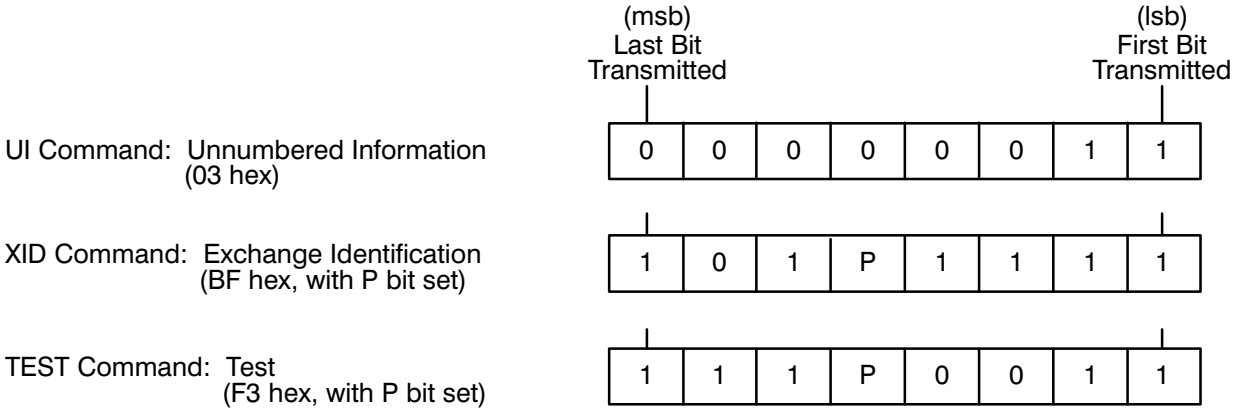
Unnumbered Format for Control Field

where:

M	is a Modifier function bit that depends on the particular command or response
P	is a Poll bit used in commands
F	is a Final bit used in responses

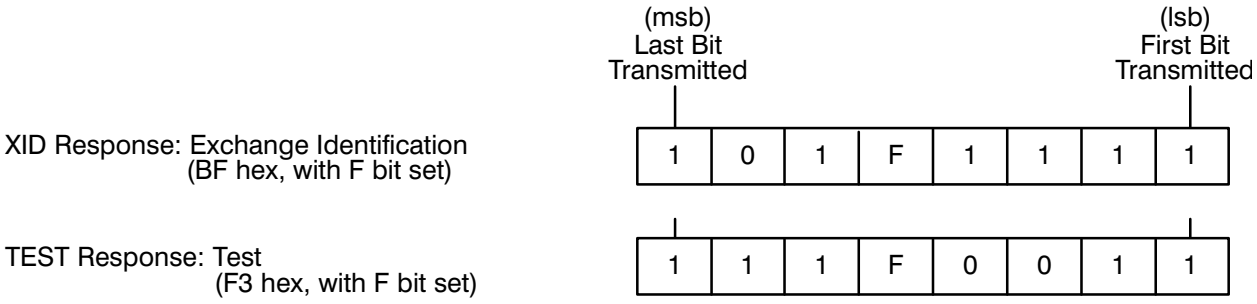
To differentiate between a “command” and a “response”, recall that the C/R bit in the SSAP field (lsb) is used. It is assumed that this bit is appropriately set during the discussions that follow.

Command Set. For Type 1 Service Protocol Data Units, there are three (3) commands possible. The Control field bits for each command are shown below:



Control Field Bit Assignments For Type 1 Service Commands

Response Set. For Type 1 Service Protocol Data Units, there are two responses possible corresponding to the respective command; there is no predefined response to the UI command. The Control field bits for each response are shown below:



Control Field Bit Assignments For Type 1 Service Responses

The P (Poll) and F (Final) bits are used to associate a soliciting command Protocol Data Unit to a corresponding response Protocol Data Unit. For example, if a TEST command Protocol Data

Unit has Control field P-bit set to “1”, the responding Protocol Data Unit must contain the Control field F-bit set to “1”.

Note that the UI command Protocol Data Unit has no predefined response Protocol Data Unit. For Type 1 operation, a UI command Protocol Data Unit is neither acknowledged nor verified for reception; thus, even though it was successfully transmitted, a UI command packet may be discarded or lost. Acknowledgment or packet verification services is implemented in higher layers of software.

Information

Interpretation of data provided in the Information field depends on the Protocol Data Unit command or response type, as indicated by the Control field.

Unnumbered Information (UI) Command. The Information field is not specified by the IEEE 802.2 Standard and is used to transfer information between Logical Link Control units. Higher layer software protocols can be implemented between SAPs (Service Access Points) in a unique manner (for example, HP Node Manager software uses an HP Network Management protocol for Node Manager-to-Node Manager communications between nodes).

Because the Information field is user-specified, the IEEE 802.2 Standard does not define a “UI Response”. In a sense, a user-implemented protocol may employ a “command” that responds to a “command”. The Command/Response (C/R) bit in the SSAP Field may be used by the programmer to ascertain whether a UI command Protocol Data Unit is a command or response.

XID Command and Response. The Exchange Identification (XID) command sent by one Logical Link Control unit to a target unit is used for the following purposes:

- To indicate the type of services (Type 1 or 2) available at the sending SAP; and
- To solicit similar information from the target SAP

The XID Command and Response Information field format is shown below (note that the Control field is also presented):

(Bytes Transmitted Top to Bottom)	(lsb) First Bit Transmitted								
Control Field	1	0	1	P/F	1	1	1	1	XID Command/Response
XID Information Field	X	X	X	X	X	X	X	X	XID Format Identifier
	Z	Z	Z	Y	Y	Y	Y	Y	Y = Logical Link Class Z = Reserved, Set to 0
	W	W	W	W	W	W	W	Z	W = Receive Window Size

General XID Information Field Format

where:

P/F	Poll bit (for commands) or Final bit (for responses) as previously defined.
Y	bit values establish the Logical Link Control services provided, Type 1 and/or Type 2.
Z	bits are reserved and are set to “0”.
W	bits are for Receive Window Size defined for Type 2 services. (For more information, refer to the IEEE 802.2 Standard.)

The Hewlett-Packard implementation provides XID information corresponding to Type 1 services only, but will recognize stations providing Type 2 services. This is illustrated below:

(Bytes Transmitted Top to Bottom)								(lsb) First Bit Transmitted	
Control Field	1	0	1	P/F	1	1	1	1	XID Command/Response
XID Information Field	1	0	0	0	0	0	0	1	IEEE 802 Basic Format
	0	0	0	0	0	0	Y	1	Y = 0 For Class 1 Station (Type 1 Services Only)
	0	0	0	0	0	0	0	0	Y = 1 For Class 2 Station (Type 1 and 2 Services)

HP Recognized XID Information Fields

The XID command may be used in several ways, depending on the capabilities of the software available: *

- To solicit a response from a remote Medium Access Control sublayer (that is, a remote LANIC card), an XID command can be sent to the remote station’s Null DSAP.
- To determine members of a group, an XID command can be sent to a Group Destination Address. Each member of the specified group address could subsequently return an XID response.
- To check for a duplicate address on the LAN, a node can send an XID command to itself.
- To identify services provided by each DSAP, an XID command can be sent to each DSAP.
- To activate a station onto the network, and determine active stations on the network, an XID command can be broadcast (Global Destination Address, all “1s” in the Destination Address field).

* Not necessarily supported by HP Node Manager software. Custom software may be required.

TEST Command and Response. The TEST command Protocol Data Unit sent to a destination Logical Link Control unit solicits a TEST response Protocol Data Unit. It is desirable that data in the Information field of a TEST command be returned in the Information field of the TEST response, but this is not required by the IEEE 802.2 Standard. For example, there may be limitations due to buffer space available.

The TEST command and response are used as a basic test of the transmission path between Logical Link Control stations.

Pad

An IEEE 802.3 Pad field is added by the LANIC card firmware when valid data is less than 46 bytes. In the pad field, invalid data bytes are added until the Protocol Data Unit field contains the required 46 bytes.

Frame Check Sequence

The Frame Check Sequence field contains a 32-bit (4 bytes) Cyclic Redundancy Check (CRC). It is encoded into and decoded from the packet by the LANIC card. The CRC is calculated from the Destination Address, Source Address, Length, and Protocol Data Unit (plus pad) fields.

Invalid Frames

Hewlett-Packard's LAN link implementation is operationally compatible with the IEEE 802.2/802.3 Standards for invalid frames. As will be seen, Node Manager software can be used to configure the link to save and log these "bad packets".

As previously described, a Medium Access Control Frame should consist of a Destination Address, Source Address, Length Field, Protocol Data Unit Field, and Frame Check Sequence. Excluding the Preamble and Start of Frame Delimiter fields, a frame should contain at least 64 bytes, but not exceed 1518 bytes.

In general, a Medium Access Control Frame is invalid if:

- it does not contain an integral number of bytes
- it contains an invalid Frame Check Sequence value
- its length is not consistent with the value specified in the Length field (that is, improper length)

3

Software Installation

It is normally the System Manager's task to install the LANIC card software driver, as well as the accompanying Node Management software. Installing the LANIC card driver is similar to other driver installation procedures, and it is assumed that the reader is knowledgeable of this process.

This chapter provides supplemental information peculiar to installing the LANIC card driver ID*67. An operational disk-based system is presumed.

Installation Summary

Interface driver ID*67 is a software I/O driver provided by Hewlett-Packard to interface the RTE-A Operating System with a LANIC card. The ID*67 driver manages communications across the host I/O backplane to and from the LANIC card. It formats system I/O requests, and accesses the LANIC to complete each request. For proper node operation, the driver must be installed in the host computer system.

The driver and associated Node Management software can support up to eight (8) LANIC cards per host computer, each card with a unique station address.

The size of the driver allows it to fit into a two-page partition.

To install the driver into the host, a new operating system must be generated and installed. For details on generating and installing a new system, along with general information for incorporating drivers, refer to your RTE-A generation manuals: *RTE-A System Design Manual*, part number 92077-90013, and *RTE-A System Generation and Installation Manual*, part number 92077-90034.

Information relating to the installation of the LANIC driver ID*67 and associated Node Management software is summarized below and discussed further in the remainder of this chapter.

1. Identify the driver and Node Management software modules provided. Transfer them, along with other operating system modules, to a disk-based system used for system generation.

2. To generate a target system, a new “answer” file must be created. This can be done by editing an existing one. Entries for incorporating driver ID*67 into a driver partition, and generating an Interface Table (IFT) and a Device Table (DVT) for each card installed in the host must be made.

   The program RTAGN is run with the new answer file specified in the runstring. This results in the creation of new system and snapshot files for the target system.

3. Link the Node Manager programs using the LAN8023.CMD command file.

4. Initalize the driver and Node Manager software in the Welcome file.

5. Boot the system.

6. Verify successful driver and Node Manager installation.

Modules Provided

The following software is used with the LAN/1000 Link product. These modules can be found in the /RTE_A directory along with other RTE_A files:

%ID*67	Driver
NM.REL	Node Manager user interface routine
NMSTK.LIB	Node Manager user interface library
NM2.REL	Node Manager command parser
NMGR.REL	Node Manager command processor
MENU	Node Manager command menu
LAN8023.CMD	Transfer file to load Node Manager modules
NM.LOD	NM link command file
NM2.LOD	NM2 link command file
NMGR.LOD	NMGR link command file

Transfer these (along with other operating system modules) to your disk-based system to be used for system generation. For instructions, consult your operating system installation and generation manuals.

Answer File Entries

The system generation program RTAGN uses a command file (the answer file) to build an operating system. To generate a system that contains the LANIC card driver, a new answer file must be created, usually by editing an existing one.

Answer file entries must be made for each LANIC card installed in the host. The answer file generally consists of several primary sections: the System Relocation area, the Driver Relocation area, the Table Generation area, and the Memory Allocation area.

System Relocation

There are no additional entries required in the “System Relocation” portion of the answer file.

Driver Relocation

The “Driver Relocation” portion of the answer file must be edited to relocate the LANIC card driver into a driver partition. Since you need to relocate the driver only once, even if there are multiple LANIC cards installed, only one entry needs to be made to the answer file:

```
    .
    .
RE,/RTE_A/%ID*67,,
END
    .
    .
```

The size of the driver is such that it will fit into a two-page partition. It is recommended that the LANIC card driver be the only driver in a partition.

Table Generation

The "Table Generation" portion of the answer file must contain entries that provide one Interface Table (IFT) and one Device Table (DVT) for each card in the system. Example 3-1 shows the entries required for table generation with two LANIC cards in the system. An IFT command is entered for each card in the following form:

```
IFT,/RTE_A/%ID*67,SC:sc
```

where:

`%ID*67`	is the relocatable driver file that also contains IFT default parameters. These defaults include: Entry point = `ID.67` Interface Type = `IT:0`, defaulted to zero IFT extension size = `TX:73`, defaulted to 73
`SC:`*sc*	specifies the octal select code of the LANIC card (set by switch SW1).

The IFT extension, specified by `TX` serves as a table area (driver's class table) for Destination Service Access Points (DSAPs)/Program Codes (PCs)/Ethernet Packet Types (ETs), and associated Class I/O class numbers. In addition, it is used to store a Multicast Address List and other variables used in the driver.

The default IFT extension size is sufficient for use with HP's networking software products. If you will be using other applications that access the LAN driver directly, you may need to modify the IFT extension size. See the *HP 12079A LAN/1000 Link Direct Driver Access Manual*, part number 12079-90001, for more information.

Although there is no device driver associated with the LANIC card, one DVT must be generated for each card. To set up the device table, DVT commands are used. The commands must immediately follow the IFT command for which they apply, and take the following form:

```
DVT,,LU:lu,DT:67b,TO:200
```

where:

`LU:`*lu*	specifies the unique decimal logical unit number to be assigned to the "pseudo device". Because Node Manager Software uses Extended LU EXEC calls (XLUEX), LUs from 2 to 255 may be assigned.
`DT:67b`	specifies the device type as 67 octal.
`TO:200`	specifies timeout for device request completion equal to 2 seconds.

Example 3-1. Sample Table Generation Entries for Two LANIC Cards Installed
(An asterisk "*" denotes a comment line)

```
*
*  BEGIN TABLE GENERATION
*  CONFIGURE LU TABLES
*
         .
         .
         .
*
*  Table Generation for Driver, Card 1
*
*  Interface Table for Card 1
*
IFT,/RTE_A/%ID*67,SC:sc1
*
*  Two Device Tables, Card 1
*
DVT,,,LU:lu1,DT:67b,TO:200
         .
         .
         .
*
*  Table Generation for Driver, Card 2
*
*  Interface Table for Card 2
*
IFT,/RTE_A/%ID*67,SC:sc2
*
*  Two Device Tables, Card 2
*
DVT,,,LU:lu2,DT:67b,TO:200
         .
         .
         .
END
```

where:

*sc*1, *lu*1	are Card 1's select code (in Octal), and logical unit number.
*sc*2, *lu*2	are Card 2's select code (in Octal), and logical unit number.

Memory Allocation

Although the LANIC card driver does not specifically make class I/O calls, the programs with which the driver interacts generally do. Operations that perform class I/O will require class numbers. The "Memory Allocation" portion of the answer file is where memory is allocated for class numbers.

The amount of system memory necessary for class numbers will vary with subsystem and application requirements. Operating without other active processes, the Node Manager software uses two class numbers.

For applications that access the HP LAN/1000 Link subsystem, additional class numbers are needed. Each program that expects to receive messages from the LAN will require at least one class number. Refer to the appropriate applications manual for class number requirements.

Generate the New System

Now that a new system generation answer file has been created, the system generator program, RTAGN, can be run. In the runstring, the answer file is specified along with other optional parameters. The RTAGN program creates a new system file and snapshot file that are used to install the new system.

For details concerning RTAGN, including file naming conventions, refer to the *RTE-A System Generation and Installation Manual*, part number 92077-90034.

Linking Node Manager Software

The various Node Management software modules must be linked, and ultimately placed in the /PROGRAMS directory.

The Node Manager programs can be linked on the target system or on another system by specifying the target system's snap file.

Depending on whether the target system is intended for a disk-based or memory-based computer, installing the new system will vary slightly. Consult the *RTE-A System Generation and Installation Manual*, part number 92077-90034, for complete details.

Security/1000

If the Security/1000 system is installed on the operating system, the Node Manager link command files (indicated by ".LOD") may be altered to provide the level of program capability desired by the system manager. The default Node Manager link command files presume the same level of security as though Security/1000 is not installed. For more information on the Security/1000 system and program security levels, see the *RTE-A System Manager's Manual*, part number 92077-90056.

Using LAN8023.CMD

A transfer file, LAN8023.CMD, is available for loading all of the LAN modules. The following example illustrates the use of this transfer file when in the process of generating a new system:

```
CI> wd,/RTE_A                    Set the working directory.

CI> TR LAN8023.CMD /system/snap.snp /newprogs
```

where:

`/system/snap.snp`	Represents the SNAP file (/directory/file).
`/newprogs`	Identifies the directory in which to put programs. (The `/newprogs` directory is normally renamed to a new `/PROGRAMS` directory later in the system generation process.)

If you use the transfer file with the existing /PROGRAMS directory specified, you may need to off ("CI>OF") the NM, NM2, and NMGR programs first. To illustrate this, the following example loads the LAN/1000 modules when not in the process of generating a new system:

```
CI> wd,/RTE_A                    Set the working directory.

CI> of,NM,ID                     Off any previous programs and ID segments that might
CI> of,NM2,ID                    exist.
CI> of,NMGR,ID

CI> TR LAN8023.CMD,,/PROGRAMS    The /PROGRAMS directory is specified directly.
```

If the transfer file is not used, you can load each of the modules individually using the link command files (.LOD). For example:

```
CI> link NM.LOD                  Link the NM module.
CI> link NM2.LOD                 Link the NM2 module.
CI> link NMGR.LOD                Link the NMGR module.

CI> crdir,/FILES802              Then, the directory for the Node Manager configuration
                                 files, event logs, and Node Manager help file should be
                                 created.

CI> co,MENU,/FILES802/,D         The Node Manager help file (MENU) should be copied
                                 into the directory.
```

Driver and Node Manager Initialization

After the new system is booted, the driver must be initialized for each LANIC card in the host computer, and the Node Manager programs must be restored or executed.

For Node Manager, you must RP the NM2 program and start NMGR to run. For driver initialization, "dummy" control requests (CN commands) are made for each LANIC card configured. The purpose of the control request is to synchronize the driver's copy of card configuration parameters stored in card RAM.

The following Welcome file entries would be made for a system with two LANIC cards:

`rp,/PROGRAMS/NM2.RUN`	Restore program NM2.
`xq,/PROGRAMS/NMGR.RUN`	Run NMGR program in background (execute without wait).
`cn,`*`lu1`*`,30B,20,0`	Dummy DSAP/Class number call (initialize driver for card 1).
`cn,`*`lu2`*`,30B,20,0`	Dummy DSAP/Class number call (initialize driver for card 2).

where:

lu1 and *lu2* are the LUs for the two LANIC cards installed.

With additional cards installed, additional "CN" commands would be required.

Verifying the System

Assuming that all preparations for booting the new system have been made, boot the system in accordance with standard procedures described in the *RTE-A System Generation and Installation Manual*, part number 92077-90034. Consult that manual for the proper boot command and for any error messages that may occur.

There are no formal tests to verify that the target system is operating properly. You should execute a few commands to convince yourself that it is. For example, try the following:

`CI> nm`	Run the Node Manager program. The Node Manager program prompt is `NM>`.
`NM> rs`	Read statistics from the card.

Various card and communication statistics should result. This will give an indication that the driver is installed and operating properly. Consult Chapter 5 for additional Node Manager software commands.

If error messages result during Node Manager commands, consult Appendix A.

To exit the Node Manager software, enter:

```
NM> ex
```

4

Node Manager Operations

This chapter describes the organization of the Node Manager software, and how it operates. An understanding of this chapter is recommended prior to using the Node Manager software.

Node Manager Modules

Node Manager software consists of the following three modules: NM, NM2, and NMGR. As illustrated in Figure 4-1, the modules NM and NM2 provide User Interface services, while the NMGR module provides file services.

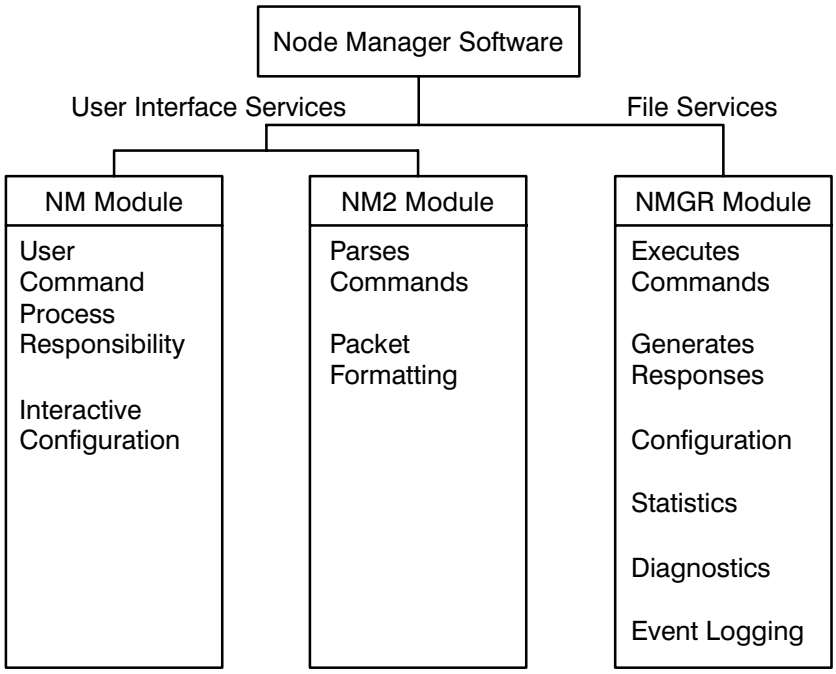


Figure 4-1. NM Software Modules

All nodes designated as Manager Nodes (see Chapter 1) must contain all the modules. On the other hand, Slave Nodes normally contain only the NMGR module for processing and executing commands received over the LAN from Manager Nodes; there is no local means from which to enter Node Manager software commands.

Command Processing

You can access both local or remote Node Manager services through the User Interface modules. Typical user command entry processing is illustrated in Figure 4-2.

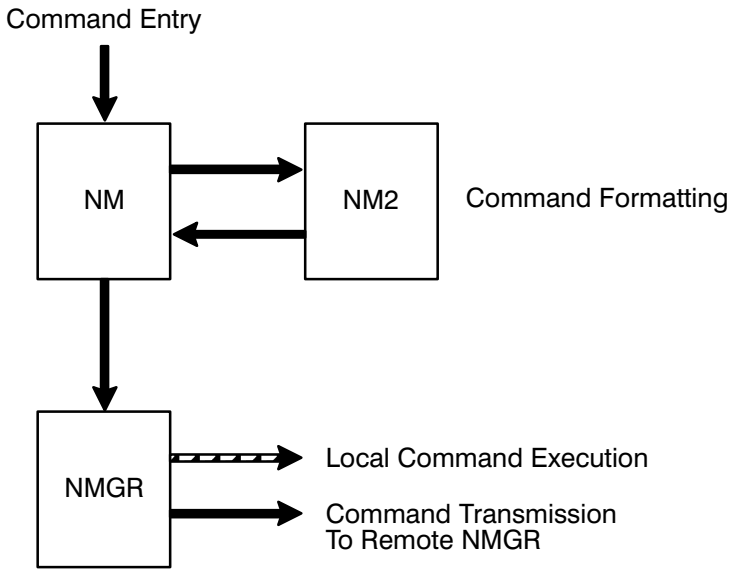


Figure 4-2. Typical User Command Processing Through Node Manager Modules

NM and NM2 Modules

The NM module provides the direct user interface for command entry. It provides the `NM>` prompt on a user terminal, and awaits a user command input.

The NM2 module is scheduled by NM and is primarily used for command parsing. NM2 deciphers a command and verifies that the command is valid. In addition, NM2 provides default values for optional parameters not specified on command entry. If the command is valid, it is mapped into a packet that conforms to the IEEE 802.2 and 802.3 Standards, and the HP Network Management protocol. Subsequently, the packet is returned to NM and is passed to the NMGR module for execution.

For commands that require a response to the user, the local NMGR module (see discussion below) returns an appropriate message to NM where it is formatted and displayed on the user's terminal.

Command Entry Errors

For unrecognized commands, or commands improperly entered, NM2 returns one or more descriptive error messages to the user.

Any system or software error that NM or NM2 cannot handle is returned to the user terminal.

NMGR Module

The NMGR module represents the node to the network from a Network Management perspective. NMGR acts as the focal point for all incoming and outgoing messages related to HP Network Link Management functions.

For packets received from the NM module, the local NMGR module determines whether the command may be processed locally, or requires transmission over the LAN to a remote NMGR module for execution. Packets containing commands from a remote NMGR module are executed only.

Commands or messages from NM or from remote nodes are processed by NMGR sequentially as received.

Command Execution Errors

If an error occurs during NMGR command execution, error messages are generated. A detailed listing of error codes and definitions are listed in Appendix A.

Error messages are returned to the initiator of the failed command:

- If a command was initiated locally, error messages are returned to the local NM module, where they are formatted and displayed on the user's terminal.
- If a command was initiated remotely, error messages are returned to the remote NMGR module.
- If the local NMGR module receives an error message from a remote NMGR module, it is passed to the local NM module and displayed on the user's terminal, presuming other errors did not intervene during this process.

There are four types of errors returned by the NMGR module. In each case, the station address of the node reporting the error, and the Service Access Point (SAP) of the process reporting the error, are returned.

Link Error (LE). Although not rigidly defined, Link Errors are Node Manager software errors that occur primarily during Multicast Address and file processing. The error code returned will be the characters LE followed by three hexadecimal digits that specify the error (for example, LE008 specifies "Multicast Address does not exist").

NM Error (NM). These Node Manager software errors occur primarily when the NMGR module cannot process a particular command even though it was passed by the NM module. In a sense, the NMGR module contains an additional layer of intelligence for screening Node Manager commands. The error code returned will contain NM followed by three hex digits that specify the particular error (for example, NM004 specifies "Illegal function for this parameter").

FMP Error (FM). File Management Package error codes are retrieved by the NMGR module and converted from negative to positive values. The error codes returned will contain FM followed by three hex digits that specify the particular error. (For FMP decimal error code meanings, refer to your *RTE-A Quick Reference Guide*, part number 92077-90020.)

Driver Error (DE). The error codes generated by the LANIC card driver (ID*67) are passed to the NMGR module. The error codes returned to the user will contain DE followed by three hex digits that specify the particular error.

Any error that NMGR cannot handle in the described way is returned to system LU 1 (system console).

Files and Directories

For each LANIC card installed in a host computer, there can be two disk files that are accessed by the local Node Manager software:

- During its initialization, Node Manager software will attempt to retrieve a list of Multicast Addresses contained in the LANIC card's disk file, MCAST.TXT. This list is used to configure the card to receive packets that contain these addresses. (Initialization of Node Manager software is discussed later.)

- During operation, if the local LANIC card is properly configured, Node Manager will log event packets (that is, "bad", "orphan", and/or "trace" packets) to a LANIC card's disk file, EL.TXT.

As discussed in Chapter 1, the disk-based system designated to store these files is called the File Server Node. It may be the local node or a remote node, and may contain the disk files associated with LANIC cards installed in several different remote nodes (typically, memory-based).

A File Server Node's disk files associated with a particular LANIC card are uniquely identified through a hierarchical file structure, as illustrated in Figure 4-3.

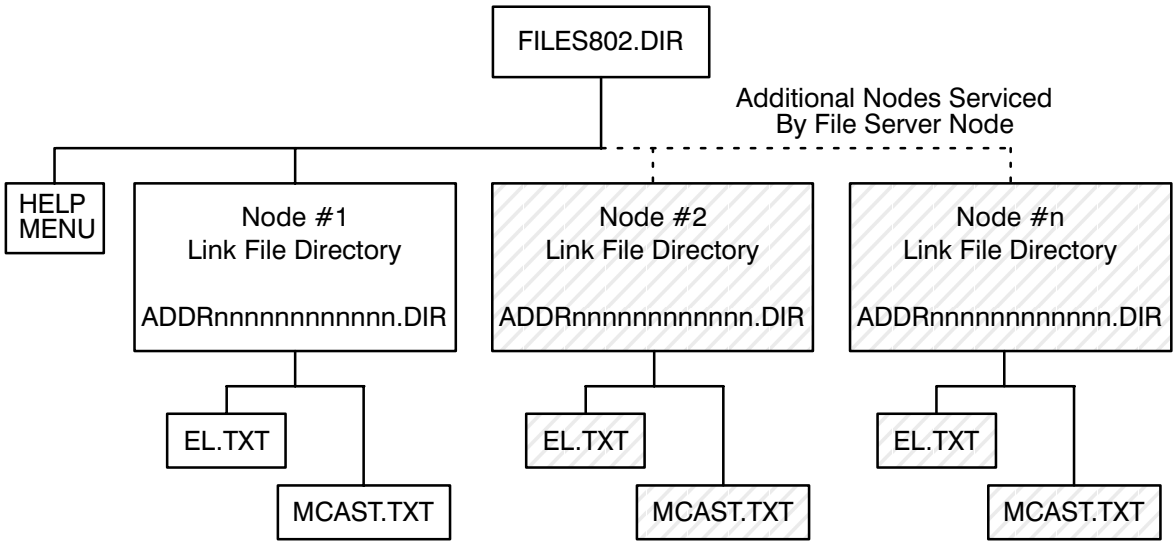


Figure 4-3. Link Files in File Server Node

Root Directory

Each File Server Node on the LAN should contain a root directory file, FILES802. This file is normally created during software installation via the LAN8023.CMD command file (see Chapter 3).

Help Menu

An ASCII file named MENU contains all the Node Manager software commands available to the user. (See Appendix B for the MENU display.) MENU is normally copied to the FILES802 directory during software installation (refer to Chapter 3). The MENU display may be viewed from the Node Manager software prompt `NM>` by entering a "?".

Note The MENU file is displayed only when it is in a FILES802 directory on a local disk-based node. A disk-based system without MENU provides no help.

The MENU file is not remotely accessed; no network traffic results when attempting to display this file.

Memory-based systems are provided a grossly simplified form of this help facility.

Link File Directories

A "Link File" directory is created by the user from Node Manager software (see the CD command described later in this manual) and is uniquely associated with a node's station address (hence, LANIC card).

For example, a link file directory might appear as follows:

```
ADDR08000900020B.DIR
```

where:

```
08 00 09 00 02 0B
```

are hexadecimal digits identifying the station address of the associated LANIC card.

The Node Manager software uses the link file directory name to access the MCAST.TXT and EL.TXT files associated with the applicable LANIC card. These files are automatically created when the link file directory is created, and are initially empty.

MCAST.TXT

Recall that, in addition to its Individual Station Address, a LANIC card may be configured with one or more Multicast Addresses for receiving packets intended for groups of nodes. At power up or boot up, the list of Multicast Addresses is null on the card, and must be loaded.

The MCAST.TXT file is used to "permanently" store a card's Multicast Address list on disk. When Node Manager software initializes, this list is automatically retrieved and configured onto the applicable LANIC card.

The LANIC card's Multicast Address list may be modified through Node Manager commands (see IM and DM commands described later in this manual). However, these commands do not modify the MCAST.TXT file.

Users can make entries to the MCAST.TXT file through the EDIT/1000 program. MCAST.TXT can be accessed from "CI>" by specifying its path, for example:

```
CI> edit /FILES802/ADDR080900020B/MCAST.TXT
```

Each entry made should be of the form:

```
XY-XX-XX-XX-XX-XX
```

where:

`X,Y` are hexadecimal digits, and Y is odd-numbered indicating a group address in accordance with the IEEE 802.3 Standard (see Chapter 2, "Destination Address"). Each entry can be positioned starting at any column of a line (record), but there can only be one entry per line.

Sample entries are illustrated below (note that none are Globally Administered addresses):

```
                    N
              03-00-09-00-02-00
              FF-FF-FF-FF-FF-F1
              07-00-09-08-00-5A
                    .
                    .
            Multicast Address N
               (End Of File)

(Note: N = number of Multicast Addresses in the file)
```

After a file is edited, the information is not configured on the card until the Node Manager software initializes (for example, when rebooting the system, or rerunning the Node Manager software):

```
CI> of,NMGR

CI> xq,NMGR
```

In summary, to make entries to a MCAST.TXT file and to automatically configure a LANIC card with the Multicast Addresses contained in the file, perform the following steps:

1. Run the Node Manager software, and create a link file directory associated with a particular LANIC card. This results in an empty MCAST.TXT file (see Chapter 5 for commands).

2. Edit the MCAST.TXT file, and terminate Node Manager software.

3. Rerun the Node Manager software on the File Server Node that contains the MCAST.TXT file for the LANIC card to be configured. On software initialization, the designated LANIC card will be configured with the Multicast Addresses entered in the MCAST.TXT file.

The Multicast Addresses configured on the card may be displayed using Node Manager software (see the Read Link Configuration, RC, command with PAR# set to "2").

EL.TXT

A node may be configured to receive "bad" or "trace" packets for delivery to Node Manager software (see the Set Link Configuration, SC, command), and it can be configured to save "orphan" packets through a Control Device command from the Command Interpreter (`CI>`) (see "Saving Orphan Packets" later in this chapter).

When the card and driver are configured to save these packets, the Node Manager software logs them to an event log file, EL.TXT, associated with the LANIC card through which the packets were received. (This presumes that the Node Manager software has located the proper file.) After they are logged, the packets are discarded. For each card with an associated EL.TXT file, the most recent 256 entries are maintained.

The EL.TXT file is a standard ASCII file automatically created on disk when a Link File directory is created. The file's contents may be displayed from Node Manager software using the Read Event Log File (RE) command. See Chapter 5, "Event Log Command", for a description of the information returned.

Driver Interface

The Node Manager software programmatically accesses the LANIC card driver, ID*67, to implement its features. Standard I/O (input/output) calls that incorporate special subfunction codes are used.* The following paragraphs provide an overview of the Node Manager software and driver operation.

Logical Units

There is one Logical Unit (LU) associated with each LANIC card generated into the system.

Writing Packets

To transmit packets, Node Manager software will pass the driver packets that conform to the IEEE 802.2 and 802.3 Standards using information entered by the user, or default values. The LANIC card firmware completes the packet by inserting the station address in the Source Address field, and adding a Start of Frame Delimiter field, a Frame Check Sequence field, and a pad (if necessary) to maintain minimum packet size.

Reading Packets

The process through which Node Manager software receives packets is more complex and requires a basic understanding of driver operations.

Driver's Class Table

When installing the driver, an Interface Table (IFT) extension area is created for each card generated into the RTE-A system. The driver uses this area to build a table of class numbers (or "access keys") for identifying various programs that expect to receive packets via the appropriate card. The driver makes an entry to the table when a program makes an appropriate driver request in which a class number and a program identifier are specified.

Program identifiers may be either Service Access Points (SAP), Program Codes (PC), or Ethernet Packet types (ET). A SAP is an even-numbered decimal value from 2 to 254. A PC is similar to a SAP but is limited to certain odd decimal values (1, 3, 5, 7, 9, and 11) and used to identify special programs, as follows:

*For detailed programming information with this driver, refer to the *HP 12079A LAN/1000 Link Direct Driver Access Manual* product, part number 12079-90001.

Program Code	Special Program
1	Network Management dispatching program
3	Orphan/Bad Packet handling routine (normally HP Node Manager software)
5	Transmit Trace Packet handling routine (normally HP Node Manager software)
7	Group DSAP Packet handling routine
9	VCP Server program
11	Ethernet Packet handling routine

The range for Ethernet types is 05DD - FFFF hex.

A new entry is created in the driver's class table when a request is made to post a class number for a new SAP, PC, or ET. If a new class number is posted to an existing SAP, PC, or ET, the previous class number is overwritten. However, note that a program may post its class number to more than one SAP, PC, or ET.

Under normal circumstances (see the "Node Manager Software Initialization" section later in this chapter), Node Manager software will post its class number for receiving packets to SAP F8 hexadecimal (248 decimal), and to Program Code 3 ("bad" and "orphan" packet handling routine) and Program Code 5 (transmit "trace" packet handling routine).

Packet Routing

When the LANIC card receives a packet, the driver is scheduled. Among information the driver obtains from the packet is its Destination Service Access Point (DSAP). (See Chapter 2 for the DSAP location within a packet.)

If the packet's DSAP is F8 hex, the driver searches the class table and retrieves the class number associated with SAP F8 hex (normally the Node Manager software class number for receiving packets). The driver then transfers the packet to System Available Memory (SAM) and queues it on the Node Manager's class number. The Node Manager software retrieves the packet from SAM through a pending Class Get request, and processes the packet data accordingly.

If a bad packet is received and the card is configured to save "bad" packets, the driver will enter the class table and retrieve the class number associated to Program Code 3. The packet will be passed to the program that posted its class number to PC 3 (normally, the Node Manager software).

Suppose an incoming packet contains a DSAP for which there is no class number, or the class number is invalid. If the LANIC card driver is configured to save "orphan" packets, the packet will be passed to the program that posted its class number to Program Code 3 (normally, the Node Manager software).

A transmit "trace" packet is a packet returned to the driver when it fails to transmit due to an error (the LANIC card must be configured to return trace packets). These packets are queued on the class number associated with Program Code 5. The packet will be retrieved from SAM by a trace packet handling program who posted its class number to Program Code 5 (normally, Node Manager software).

When the Node Manager software is posted to PC 3 and PC 5, and when “bad”, “orphan”, and/or “trace” packet processing is properly enabled, they are logged to system LU 1 (system console) and to the event log file (EL.TXT) if it exists.

Note Node Manager software does not process Group DSAP (GDSAP) packets. Recall from Chapter 2, a GDSAP packet contains a “1” in the least significant bit position of the DSAP field (that is, an odd DSAP is interpreted as a Group DSAP). For packets with odd DSAPs, the driver retrieves the class number posted to Program Code 7, and queues the packet on that class number. To process GDSAP packets, a user-written routine is required.

Note On recognition of a “bad”, “orphan”, or “trace” packet, the driver is internally programmed to access class numbers associated with Program Codes 3 and 5 as applicable. However, Program Codes 1 and 9 are used for storing class numbers of a Network Management Dispatcher program and VCP server routine, respectively. These Program Codes may be accessed by the driver only if the driver is externally programmed to do so through the proper driver request. (A Dispatcher program is needed as an intermediate packet router for the simultaneous operation of a user-written VCP server routine and Node Manager software. Incoming VCP server packets and Node Manager packets are routed by the driver to the same SAP, F8 hex.)

Saving Orphan Packets

Orphan packets are those packets received that are not deliverable to a program or process. In other words, an orphan packet contains a DSAP for which there is no, or an invalid, class number in the driver’s class table.

In the default case, the LANIC card and driver will discard orphan packets. When configured to save orphans, the LANIC card and driver will send them to the program whose class number is posted to Program Code 3 in the driver’s class table. If this program is the Node Manager software, orphan packets are logged to system LU 1 (system console) and to the event log file associated with the card.

Although it processes orphans, Node Manager software does not configure the card and driver to save orphans. In addition, it does not detect whether saving orphans is configured.

To configure saving orphans, a Device Control request is made interactively from the Command Interpreter prompt (`CI>`):

```
CI> CN,User_LU,45B,x
```

where:

CN	is the Control Device command to the driver
User_LU	is the logical unit of the specified LANIC card
45B	is the subfunction code for saving/discarding inbound packets
x	if "1" will configure the driver to save orphan packets, if "2" will reset the driver to discard orphan packets (normal mode)

When "saving orphans" is configured, Node Manager software will send orphan packet information to system LU 1 (system console). If not configured, no information is sent. Thus, to detect the configuration for saving orphans on a particular LANIC card, LU 1 (system console) may be checked after sample orphan packets are sent to the card.

LANIC Card Configuration Data

RAM & NOVRAM

The LANIC card contains RAM and NOVRAM (non-volatile static RAM). NOVRAM data is maintained even after power cycling.

Among data stored in NOVRAM include the card's Station Address, and a Download Server Station Address. The Station Address uniquely identifies a node on the LAN (see Chapter 1). A Download Server Station Address is generally used to identify some other node on the LAN from which the local node will receive special information, such as VCP server instructions or Link File directory data, depending on the software running.

Also stored in NOVRAM is the Receive Packet Filter Mode, the Retry Limit, the Save Bad Packet flag, and the Trace Mode flag. Briefly, the Receive Packet Filter Mode is a setting that determines categories of packets that a node can receive; the Retry Limit determines the number of times the card will reattempt a packet transmission if it initially failed (1 or 15 times); the Save Bad Packet flag determines if bad packets are saved or discarded; and the Trace Mode flag configures whether tracing of packets that failed transmission is "on" or "off".

When shipped from the factory, the LANIC card NOVRAM contains initial settings as shown in Table 4-1.

Table 4-1. Initial Factory Settings Contained in NOVRAM

Item	Description of Factory Setting
Station Address	6-byte value, unique to each card. For example, "08-00-09-xx-xx-xx" hex, where "xx xx xx" are labeled on the NOVRAM.
Download Server Station Address	The Broadcast address: FF-FF-FF-FF-FF-FF hex (see "Finding Link File Directories")
Receive Packet Filter	Set to "0", node will receive Individual Station Address packets only. (See Table 4-2)
Retry Limit	Set to "15". On transmission failure, the node will reattempt transmission up to 15 times.
Save Bad Packets Flag	Set to "0". The node will discard bad packets received.
Trace Mode Flag	Set to "0". The node will not trace (echo to driver) packets that failed transmission.

During card initialization, such as after card power-up and reset, information stored in NOVRAM is copied to card RAM where it is subsequently used as required.

Through the driver, Node Manager software can be used to modify RAM or NOVRAM data. For example, it can modify the Station Address and Download Server Station Address in RAM only ("temporary" configuration change), or in RAM and NOVRAM ("permanent" configuration change). Also, it can configure Multicast Addresses in RAM.

See the Read Link Configuration (RC) and Set Link Configuration (SC) commands for more information on node (including card RAM and NOVRAM) configuration.

Driver's Copy

When the driver initializes, it obtains a copy of card RAM data, including the Station Address and Download Server Station Address. If changes are made, such as a new Station Address or Multicast Addresses are written to the card, the driver updates its copy. Thus, at any time, the driver "knows" essential card configuration parameters.

As long as system memory remains intact and there are no failures, the card will maintain its latest configuration. For example, suppose a card's Station Address was altered in RAM only. On card reset and initialization, RAM contents are lost, and the Station Address configured in NOVRAM will be written to RAM. The driver will overwrite the RAM's Station Address with the altered value. (This feature of the driver is especially useful during powerfail for those systems that have battery back-up installed.)

Node Manager Software Initialization

It may be useful to conceptually understand how the Node Manager software initializes when run. Node Manager initialization may be conceptually divided into two basic processes: posting its class number, and finding each card's Link File directory.

Posting Its Class Number

The Node Manager software must be able to receive packets from the LAN. The first part of its initialization process is illustrated in Figure 4-4.

In addition to any other class number, the Node Manager software allocates a class number for retrieving LAN packets. Subsequently, a series of checks is performed to determine what other related LAN programs are configured.

The class number of SAP F8 hex is compared to the class number at Program Code 3, and to zero. This determines what software, if any, was previously configured as the HP Network Management program. If the class numbers are non-zero and match, or if the class number of SAP F8 hex is zero, the Node Manager software automatically assumes that duty by posting its class number to SAP F8 hex.

If the above criteria prove false, then some other program must have its class number at SAP F8 hex. The class number at Program Code 1 is checked. If non-zero, then a Dispatcher program is assumed to have been acting as an HP Network Management program for routing packets between the HP Node Manager software and a VCP server program. The Node Manager software makes its class number available to the Dispatcher program, through which Node Manager software continues to receive packets.

If Program Code 1's class number is zero, it is presumed that a VCP server program was operating as the HP Network Management program and operating without a Dispatcher program available. An error message is written, and the Node Manager software assumes duties of the HP Network Management program by overwriting SAP F8 with its class number (the VCP server will no longer be able to receive packets).

In any event, the Node Manager software posts its class number to Program Codes 3 and 5.

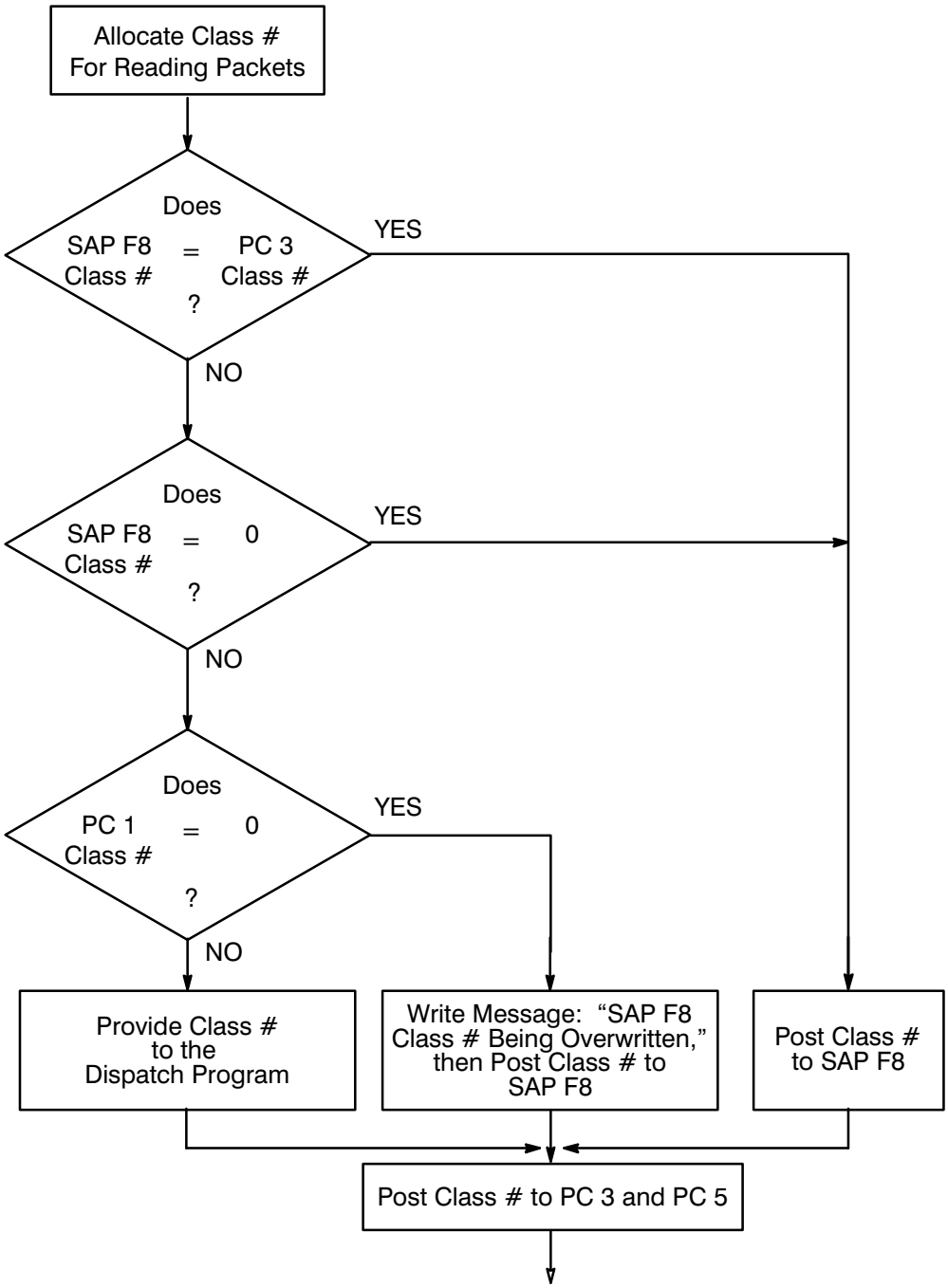


Figure 4-4. Node Manager Software Initialization for Posting Class Numbers

Finding Link File Directories

For each card generated in the system, the Node Manager software attempts to find the applicable Link File directory containing the card's MCAST.TXT and EL.TXT file. Recall that Node Manager software will overwrite the card's Multicast Address list with the data contained in its MCAST.TXT file, and will log "bad", "orphan", or "trace" packets to its EL.TXT file (when the card is properly configured).

The Node Manager software first checks whether or not the local system is disk-based (a system call is used). If the local system is disk-based, a flag is set. For each LANIC card installed, this flag is checked and the FILES802 directory (if it exists) is searched for a Link File directory name that matches the Station Address of the applicable card. A successful match results in the Station Address being stored in a "File Server Station Address" variable maintained by the Node Manager software.

If the local system is not disk-based, or if a Link File directory cannot be found locally for a particular card, the Download Server Station Address stored on the card (in NOVRAM) is inspected:

- If the Download Server Station Address is a valid Individual Station Address, a packet containing the appropriate command is transmitted on the LAN to that address. The remote Node Manager software receives this command and searches its FILES802 directory for the applicable Link File directory. If successful, it notifies the local node through an appropriate response.

  On receiving this response, the local Node Manager software stores the Download Server Station Address in its File Server Station Address variable since it correctly identifies the location of the Link File directory.

- For a zero Download Server Station Address, there is no transmission.

When unable to find a Link File directory for a particular card, the File Server Station Address variable for that card is set to zero. With no MCAST.TXT file, Multicast Addresses will not be configured on the card at boot-up or Node Manager software initialization.

Unless a major error arises, the Node Manager software continues operation.

Note If the local system is to contain the local card's Link File directory, the Download Server Station Address on the card should be changed either to zero, or to the Station Address of the card (see Chapter 5 for the appropriate command). Either will prevent Node Manager from transmitting onto the LAN when searching for the node's Link File directory.

Other Initialization Considerations

Entering User Commands

Node Manager commands cannot be processed during initialization, and command entries will time out.

Initialization Errors

Node Manager software initialization errors that occur are returned to the terminal from which initialization originated.

In some cases, an error type and error number (in decimal) are returned. These will correspond to the Node Manager software errors provided in Appendix A. For example, the following message specifies a driver error (type 4) with a "powerfail" error code (1).

```
NMGR INITIALIZATION ERROR
Error Type =  4      Error Number =   1
```

Other error messages may also be returned. These messages are generally clear and self-explanatory. For example, when Node Manager software retrieves the MCAST.TXT file for initializing a LANIC card with Multicast Addresses, the following error indicates a corrupt file.

```
NMGR INITIALIZATION ERROR
Corrupt file:  /FILES802/ADDRxxxxxxxxxxxx/MCAST.TXT:::4:2
```

where:

`xxxxxxxxxxxx` is the Station Address that identifies the applicable LANIC card.

Finally, some messages such as the following should occur only rarely:

```
NMGR ABORTED--NO LUs ARE AVAILABLE
NMGR ABORTED--NO AVAILABLE CLASS NUMBER
NM ABORTED--NO AVAILABLE CLASS NUMBER
NO AVAILABLE 802.3 LU                  (Note:  this message pertains to the NM2 Module)
```

Post Initialization

After initialization, the NMGR module must be operating in the system session prior to receiving packets. When initiated from a "Welcome File" during the boot-process (for example, `XQ,NMGR::PROGRAMS`), NMGR is in the system session. When initiated from a user session, it detaches to the system session and remains there even after the user session terminates.

This can be verified through the System Status Reporting program WH, run with the PL option:

```
CI> WH,PL,NMGR
```

The NMGR module will be in the system session, and will normally be "class suspended" on a class number due to its pending Class Get request.

As a system session module, NMGR may be accessed by any user, including access from a remote node. However, it may be terminated only by a "Superuser".

Once NMGR is detached to the system session, the following information is output to system LU 1 (system console):

- Occurrences of bad, orphan, and trace packets (when the LANIC card and driver are properly configured to process such packets).
- Any error that NMGR cannot process. (To interpret such errors, consult Appendix A or your system manuals.)

Note Because Node Manager software writes to LU 1 (normally the system console), the system console should not be left with a pending read (awaiting input) which would prevent such messages from reaching the console.

The NM module is installed as a system utility. This implies a sequential "one-at-a-time" access; another user is queue suspended while waiting for its completion. To become "unsuspended" may require "offing" the user session, or "offing" NM (by a Superuser) if the current NM user does not exit NM.

Errors that cannot be handled by the NM and NM2 modules are returned to the user's terminal. (To interpret such errors, consult Appendix A or your system manuals.)

Packet Filter Addressing Modes

An IEEE 802.3 LAN is essentially a broadcast network. Any packet transmitted is available for reception by all nodes. Whether or not a node receives and accepts a packet depends on a particular level of address filtering configured.

There are four basic address filtering categories: Individual, Multicast, Broadcast, and Promiscuous. Each category can be characterized as follows:

Individual — This category refers to the use of an Individual address to address one particular node on the network for one-on-one communications. A packet containing an Individual address will always be accepted by the node with matching Station Address. (Although shipped from the factory with a unique Station address, each LANIC card's address may be temporarily or permanently changed through Node Manager software. See Chapter 5.)

Multicast — Here, a Multicast address is used to send a single packet to two or more network nodes simultaneously, that is, a group of nodes. Each member node of a group of nodes may be configured with one or more Multicast addresses. If a packet's Destination Address field contains a Multicast Address that matches one configured on a node, the packet may be accepted (depending on the Packet Filter Mode set).

For example, Multicast Addresses might be used when a supervisory computer transmits instructions to a number of workcell controllers.

Broadcast — A Broadcast address is a special Multicast Address. A Broadcast address in a packet's Destination Address field is intended for all network nodes. When configured to do so, each node on the LAN may receive and accept a packet containing a Broadcast address.

For example, Broadcast address packets might be used to configure a new node on the LAN.

Promiscuous — When a node is configured for Promiscuous operation, it attempts to receive and accept all packets transmitted on the LAN, provided that resources are available to buffer the packets.

Caution It is recommended that a node configured for Promiscuous operation be used only as an online monitor with no network services running. When in Promiscuous mode, the node will process packets as if they were addressed to the node. If a received packet contains a DSAP that matches a valid SAP on the node, the packet will be routed to the program or process associated with that SAP. Such a packet may not be expected by the program or process, and improper operation or failure may result.

Also, if Node Manager software is used to log "bad" or "orphan" packets, such packets will be logged to an event log file on disk. This can consume considerable overhead.

Through Node Manager software, a node may be configured with one or more of these packet filter categories for receiving packets. Table 4-2 shows the possible combinations a node may assume. (See the Read Link Configuration, RC, and the Set Link Configuration, SC, commands in Chapter 5.)

Table 4-2. Receive Packet Filter Modes

Setting	Categories of Packet Addresses a Node Will Accept
0	Individual only (default setting)
1	Individual + Promiscuous
2	Individual + Broadcast
3	Individual + Broadcast + Promiscuous
4	Individual + Multicast
5	Individual + Multicast + Promiscuous
6	Individual + Multicast + Broadcast
7	Individual + Multicast + Broadcast + Promiscuous

Multiple LANIC Cards

The Node Manager software can operate with up to eight LANIC cards installed in a single system.

Disk Access

Node Manager software provides for storing various LANIC card information on a disk-based system (File Server Node). Because disk access is relatively slow, performance may be incrementally degraded with multiple cards if they result in additional events to be logged.

During the initialization process, Node Manager software attempts to locate and access a Link File directory on disk for each LANIC card installed. If found, relevant information is retrieved from disk and written to the card.

During operation, Node Manager software may log “bad”, “orphan”, or “trace” packets to a file on disk for each LANIC card installed and appropriately configured.

Command Routing

If a system contains multiple LANIC cards (nodes) attached to the same LAN, the card through which a local Node Manager command and response are routed depends on the command parameters specified. Even for local Node Manager commands directed to local cards, the command parameters will determine whether:

- a local card is accessed directly, or
- a local card is accessed over the LAN via another local card.

If particular command parameters are defaulted, the routing of commands will depend on the parameter default values implemented by the Node Manager software. These parameters are interdependent; one parameter default value may vary depending on whether another is specified.

In general, command parameter defaults were designed to minimize network access. The applicable parameter defaults are described in Chapter 5.

5

Using Node Manager

This chapter describes the use of Node Manager software. Each of the available commands is described, and examples of command entry and responses are provided.

Caution There is no security provided by the Node Manager software other than what is available through the RTE-A Operating System. Users of Node Manager software have access to commands that can cause communication failure between nodes, and can render network services inoperative. Limited and controlled access to Node Manager software is recommended.

Parameter Notation

The various parameters used in Node Manager software command runstrings are described in the discussions following each command. Node Manager software does not differentiate between lowercase and uppercase characters.

Brackets ("[ ]") are used to indicate optional parameters. Optional parameters may be omitted, and default values will be used. In many cases, brackets are embedded within other brackets to indicate that placeholders (commas) are needed.

For example,

```
[,[option][,LU#]]
```

indicates that if LU# is omitted, the comma preceding it is not needed. If LU# is included while option is omitted, LU# must be preceded by two commas („LU#) to hold the place of option. In this case, option may be referred to as a NULL parameter.

Note that user entries are typically indicated after the `CI>` or `NM>` prompts. `<RETURN>` indicates a carriage return after the user entry. For example:

```
CI> NM<RETURN>
```

Getting Started

It is presumed that the Node Manager software, driver, and related modules have been installed on each HP 1000 A-Series computer node, and the systems have been properly booted. Installation information is contained in Chapter 3.

Running the Node Manager Software

Log onto your system and wait for the Command Interpreter system prompt, `CI>`, to appear. To use the Node Manager software, just type `NM`. The system will respond with the welcome message shown:

```
CI> NM<RETURN>
----- NETWORK LINK MANAGEMENT USER INTERFACE -----
     < for help on NM commands use "?" >
     < to exit from NM use "EX"       >

NM>
```

You will know you are in the Node Manager software utility when the prompt, `NM>`, appears. All Node Manager software commands are executed from this prompt.

When you run the Node Manager software, you may want to configure two parameters in the runstring: `NMtimeout` and `NMretry`. These parameters are described below.

Note These parameters influence the relationship between the NM and NMGR modules only. Do not confuse these with various driver or card firmware timeouts (not configurable), or retry settings for packet transmission onto the LAN (configurable).

The Node Manager software runstring would be modified as follows. Note that parameters 1 and 2 are reserved and require placeholder commas.

```
CI> NM[,,,[NMtimeout][,NMretry]]<RETURN>
```

where:

`NMtimeout` This is the time (in seconds) the NM module waits to receive a response from the NMGR module before trying to send a command again. Each time a command is entered by the user, the command times out after the specified number of seconds if no response is received. The value entered must be an integer from 1 to 600. The default is 5.

`NMretry` This reflects the number of times that the NM module attempts to send a command to the NMGR module before reporting an error. The value entered must be an integer from 1 to 100. The default is 0 (that is, 1 try with 0 retries)..

Setting these parameters may depend on network activity or congestion. If the NMGR module is heavily occupied, the NM runstring parameter values may need to be increased.

Exiting the Node Manager Software

If EX is entered in response to the NM> prompt, Node Manager is exited with an accompanying remark, and the CI> system prompt appears:

```
NM> EX<RETURN>
--- END NM ---

CI>
```

Using the Help Facility

On a disk-based system containing the MENU file (/FILES802/MENU), entering a question mark (?) in response to the NM> prompt will display help screens. First, the available Node Manager commands are listed, part of which is shown below. Subsequent screens explain the various parameters used in the commands. (On memory-based systems, only a command list is displayed.)

```
NM> ?<RETURN>

NM Command Summary:

CONFIGURATION:

1. Read Link Configuration          RC[,[ADR][,[PAR#][,[option][,LU#]]]]
2. Set Link Configuration           SC,[ADR],PAR#[,[PAR-value][,[option][,LU#]]]
3. Update Link Configuration        UC[,[ADR][,[option][,LU#]]]
4. Insert Multicast Address         IM,[ADR],MulticastAddress[,LU#]
5. Delete Multicast Address         DM,[ADR],MulticastAddress[,LU#]
6. Create Link File Directories     CD[,[ADR][,[FileAddress][,LU#]]]
7. Purge Link File Directories      PD[,[ADR][,[FileAddress][,LU#]]]
8. Check Link File Existence        CK[,[ADR][,[FileAddress][,LU#]]]

DIAGNOSTICS

1. Initiate Card Self Test          TC[,[ADR][,[LU#][,Rep]]]
2. Do External Loopback to MAU      EL[,[ADR][,[LU#][,Rep]]]
3. Issue Test Loopback Command      TEST,[ADR],DSAP[,[MSGLEN][,[LU#][,Rep]]]
4. Issue XID  Loopback Command      XID,[ADR],DSAP[,[LU#][,Rep]]

EVENT LOGGING:

 More...('a' to abort)
```

After the first screen, the next screen is displayed by pressing the space bar. To scroll through the entire help file, press the <RETURN> key. To go back to the NM> prompt, press the <A> key (that is, abort the help menu display).

Note that pressing any other alphanumeric key while the display is scrolling causes the system to pause and the More... prompt appears. Just press the <RETURN> key to continue the scrolling.

For a complete listing of the help file, see Appendix B.

Entering Commands

Node Manager software commands are entered from the NM> prompt, followed by pressing the <RETURN> key.

When entering a command, do not use the arrow keys to move the cursor back for error correction; instead, use the <BACKSPACE> key.

Using the Command Stack

As command lines are entered at the terminal keyboard, they are saved in a stack for reference or reuse. Command lines in the stack can be edited and reentered, or simply reentered without retyping.

A maximum of 10 command entries will be saved. If the stack is full, the oldest commands in the stack are removed to make room for new commands. Duplicate commands are not saved in the stack.

To display the command stack, enter a slash (/). As illustrated below, a screenful of commands (up to a maximum of 10) is displayed:

```
NM> /
---Commands---
rc
tc
el
rs
xid,08-00-09-00-8e-e9,00
re
uc
zs
?
ck
```

Note that the cursor is at the bottom of the stack. Simply pressing the return key will return to NM>, where a new command can be entered.

However, the cursor can be moved to any line using the terminal cursor control keys, and the line can be edited using the terminal editing keys. Whether or not the line was edited, pressing the carriage return key will enter the line as if it were retyped and entered at the NM> prompt.

You can recall just the last command with the cursor positioned on the command line. This is done with two slashes:

```
NM> //
---Commands---
ck
```

The number of lines backward from the last line can be specified with the corresponding number of slashes after the command stack command (that is, the first slash). For example, to display the stack with the cursor positioned on the second to the last line, enter three slashes.

A slash followed by a number can be entered. In this case, only the latest command entries are displayed starting with the command corresponding to the line number specified (counting backward from the last line). The cursor is positioned on the line specified.

Whenever the cursor is positioned at a command line, either by slashes or a number, that line may be edited. Pressing the carriage return key will enter the command. If you do not wish to enter this line, you can enter a slash to repeat the whole command stack, or move the cursor to a blank line (and press the return key) to return to the NM> prompt.

The NM command stack is not saved between NM sessions.

Error Messages

Command Entry

If an illegal or unrecognized Node Manager command is entered, the User Interface modules (NM, NM2) return command entry errors. Errors found are returned in sequential order (there may be errors not found). An up-arrow cursor mark or circumflex is displayed at the position of an error with an explanation of the problem.

```
NM> RC,0P-00-09-00-02-0B,0A<RETURN>
       ^1               ^2

error  1 ---> Address must be XX-XX-XX-XX-XX-XX, where X is a hex digit
error  2 ---> PAR# must be an integer in the range 1 to 11 or 'A'

NM>
```

These are typical command entry error messages (for reference, see the Read Link Configuration command, RC, described later in this manual). In error 1, the Station Address contains an improper hexadecimal digit. In error 2, a hexadecimal number instead of a decimal value has been entered. The Node Manager software points out the source of the problem and provides a short description of how to correct it. The command must then be reentered.

Timeout Error Messages

Recall that a timeout for Node Manager commands can be configured in the Node Manager software runstring using the `NMtimeout` parameter (default is 5 seconds). If a command is entered and accepted, but for some reason the NMGR module does not respond to the NM module within the designated timeout period, the NM module will return the following error message:

```
NM> RC,08-00-09-00-02-0B,2<RETURN>
Read 802.3 Link Config from node      08-00-09-00-02-0B... [failed]
-- > times out - no response from target node

NM>
```

Typical causes of command timeouts include:

- transmission to an unknown Station Address,
- excessive NMGR module loading, or
- excessive network traffic.

Command Execution

Command execution errors are returned by the NMGR module. They can result even though command entries were accepted and passed by the User Interface modules. An example of a command execution error message returned to the user is shown below:

```
NM> SC,08-00-09-00-02-5A,3<RETURN>
Set 802.3 Link Config on node       08-00-09-00-02-5A....  [failed]
ERROR:  NM003 REPORTING NODE ADR:08000900025A SAP: F8
Parameter not supported

NM>
```

Note the error contains an “error code”, and the Station Address and program SAP of the node from which the error is generated.

The error codes are described in Chapter 4 (see “NMGR Module”), and provided in Appendix A. These codes consist of two letters reflecting the type of error, followed by three hexadecimal digits that specify the particular error (see Appendix A). In the example above, NM003 indicates a Node Manager error resulting from an unsupported parameter specified in the command. The unsupported parameter, in this case, is the “3” immediately before the `<RETURN>` key.

From the same example above, the Station Address of the node reporting the error is 08000900025A hexadecimal. The program at that node reporting the failure has its class number posted to SAP F8 (hex).

Note In most cases, the SAP indicated will be F8 hex because these commands are generally between Node Manager software operating on different nodes. (Recall that Node Manager software posts its class number on SAP F8.) However, there are special cases where the LANIC card firmware responds (Medium Access Control sublayer) corresponding to SAP 00, or there may be special user software developed on other SAPs.

Node Manager Commands

In the remainder of this section, the available Node Manager commands are described. The commands are categorized by the type of service provided (Configuration, Diagnostics, Event Logging, and Statistics) and discussed in the sequence that they appear in the MENU file (the Help Facility) as shown in Appendix B.

Caution Before issuing Node Manager commands on an active network, the impact on various hardware and software operations should be well understood. This will help to prevent unexpected node or network failure. Although command results are normally reversible, it is recommended that offline systems be used during the Node Manager software familiarization process.

Note Node Manager commands are directed to a target node specified by its Station Address as a command parameter (`ADR`). Node Manager commands cannot be sent to target nodes using Multicast or Broadcast addresses. Such attempts will result in a command entry error.

Parameter Defaults

When commands are entered, various parameters may be defaulted. Where convenient, parameter defaults are specified in the discussion of each command.

However, there are three command parameters that warrant special consideration here. They are common to several commands and their defaults are interdependent. These parameters are:

`ADR` The Station Address of the "target" node for which the command is intended. This address may apply to a local or remote node. When specified, it is a 6-byte value and entered as 6 pairs of hexadecimal digits separated by hyphens.

`FileAddress` The File Server node's station address. This address may apply to a local or remote node. When specified, it is a 6-byte value and entered as 6 pairs of hexadecimal digits separated by hyphens.

`LU#` The Logical Unit number of the card through which a command is delivered to the target node (specified by `ADR`). `LU#` is always an LU in the local system from which the command originates.

When you start NMGR (typically done in the Welcome file), it searches the system I/O tables and builds a table of LAN LUs found on the system. Thereafter, when you enter a Node Manager command without specifying an LU, the lowest LU found in the LAN LU table is used as the default value.

Each parameter applies to a particular LANIC card. In a given command, each parameter may, or may not be specified. The complexities arise because, for multiple LANIC cards installed, the default of one may depend on the value specified for another. Also, it may depend on whether the specified value applies to a local or remote node.

The defaults were designed to minimize network access or to make some logical sense. Note that most systems will contain a single LANIC card where command defaults are greatly simplified.

Group I: Commands Not Containing the FileAddress Parameter

One group of commands, referred to as Group I commands for discussion purposes, utilize the `ADR` and `LU#` parameters only (`FileAddress` is not a parameter in these commands). These commands are: RC, SC, UC, IM, DM, TC, EL, TEST, XID, RS, and ZS (for quick reference, see Appendix B).

Table 5-1 provides the `ADR` and `LU#` parameter defaults for this group of commands.

Table 5-1. ADR and LU# Defaults for Group I Commands

ADR	LU#	Parameter Default Description
---	---	ADR: Station Address of local card with lowest LU LU#: Lowest local LANIC card LU
---	specified	ADR: Station Address of local card with LU specified
specified, local	---	LU#: LU of the local LANIC card specified by ADR
specified, remote	---	LU#: Lowest local LANIC card LU
specified	specified	(Parameters assume specified values)

Group II: Commands Containing the FileAddress Parameter

Another group of commands, referred to as Group II commands here, utilize all three parameters ADR, FileAddress, and LU#. These commands are: CD, PD, and CK.

Table 5-2 provides the parameter defaults for Group II commands.

Table 5-2. ADR, FileAddress, and LU# Defaults for Group II Commands

ADR	FileAddress	LU#	Parameter Default Description
---	---	---	ADR: Station Address of local card with lowest LANIC card LU FileAddress: Same as ADR LU#: Lowest local LANIC card LU
---	---	specified	ADR: Station Address of local card with LU specified FileAddress: Same as ADR
---	specified and local	---	ADR: Station Address of local card with specified FileAddress LU#: LU of LANIC card specified by ADR and FileAddress
---	specified and remote	---	ADR: Station Address of local card with lowest LANIC card LU LU#: Lowest local LANIC card LU
---	specified local/remote	specified	ADR: Station Address of card with LU specified
specified and local	---	---	FileAddress: Station Address of card with specified ADR LU#: LU of card specified by ADR
specified and remote	---	---	FileAddress: Station Address of card with specified ADR LU#: Lowest local LANIC card LU
specified local/remote	---	specified	FileAddress: Station Address of card with specified ADR
specified, local	specified local/remote	---	LU#: LU of the local card specified by ADR
specified, remote	specified, remote	---	LU#: Lowest local LANIC card LU
specified, remote	specified, local	---	LU#: LU of the local Station Address specified by FileAddress
specified	specified	specified	(Parameters assume values specified)

Retrieving the ADR Parameter

When the command parameters are defaulted, Node Manager software (specifically, the NM2 module) will insert the necessary values into the command string. Following the default rules of Table 5-1 and Table 5-2, an attempt is made to read the Station Address from the applicable LANIC card for use as the ADR parameter.

However, in some cases this address may not be accessible (for example, the card may not respond). If a value cannot be retrieved, the NM2 module will enter the address

```
00-00-00-00-00-00
```

(the "default" of ADR defaults), and in a normal manner, pass the command to the NMGR module for processing.

In such cases, the message:

```
The card address could not be acquired.  Try card self-test with TC,,LU#.
```

is returned, along with other information pertinent to the particular command. The TC command is used to initiate card self-test. Since it is a local card, its LU# parameter may be specified and an indication of the problem may be returned (see the TC command description later in this chapter).

Configuration Commands

For both local and remote nodes, certain Node Manager commands can be used to determine the present settings of various node parameters, or to modify these settings as required. Commands are interactively entered; for parameters to be modified, changes are made without stopping system operation.

Node Manager configuration commands are listed below. Command parameters are specified in the command descriptions that follow.

- Read Link Configuration, RC
- Set Link Configuration, SC
- Update Link Configuration, UC
- Insert Multicast Address, IM
- Delete Multicast Address, DM
- Create Link File Directories, CD
- Purge Link File Directories, PD
- Check Link File Existence, CK

Read Link Configuration Command (RC)

The Read Link Configuration command provides the user with information regarding the present configuration of a node. This includes the node's Station Address, File Server station address, Download Server station address, Multicast Address list, Packet Filter mode, and Retry limit. In addition, the node's configuration for receiving bad transmit-trace packets may be determined.

The syntax for the Read Link Configuration command is:

```
RC[,[ADR][,[PAR#][,[option][,LU#]]]]
```

where:

ADR	is the "target" Station Address; that is, the node whose configuration parameters are to be returned. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default values.
PAR#	is an integer 1 through 11, or the letter "A". When omitted, this parameter defaults to "A". The definition of each PAR# entry is described in Table 5-3.
option	"P" or "T" may be entered. If P (for "permanent") is entered, NOVRAM values specified by PAR# are returned. Thus, the P option applies to the following PAR# selections: 1, 4, 5, 6, 7, and 9. If PAR# specifies values not in NOVRAM, P is ignored and T is presumed. If T (for "temporary") is entered, the values specified by PAR# are returned from RAM or Node Manager as appropriate. T is the default entry.
LU#	is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. LU# is a value in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

Multicast Address Considerations

This command can be used to determine the Multicast Addresses configured on a node. However, it is the Packet Filter Mode that determines whether or not a Multicast Address packet is received and accepted (see Table 5-4).

The driver stores a copy of a card's Multicast Address List in an IFT (Interface Table) extension area created during system generation. If there is not enough space in the IFT extension area for Multicast Addresses, this command will fail with a driver error (DE007, see Appendix A). The default IFT extension size is sufficient for use with HP's networking software products. If your application accesses the LAN driver directly, you may need to modify the IFT extension size. (See the *HP 12079A LAN/1000 Link Direct Driver Access Manual* product, part number 12079-90001.)

Table 5-3. Definitions of the RC Command Parameter, PAR#

PAR#	DEFINITION
1	Display the Station Address of the node whose Station Address is ADR (specified or defaulted, see Table 5-1).
2	Display the list of Multicast Addresses configured on the node with Station Address ADR (see Table 5-1).
3	(reserved)
4	Display the Receive Packet Filter mode configured on the node whose Station Address is ADR (see Table 5-1). The initial Receive Packet Filter mode is “0”. See Table 5-4.
5	Display the Retry Limit configured on the node whose Station Address is ADR (see Table 5-1). If a packet initially fails to transmit, the Retry Limit is the number of times the card reattempts transmission. Possible settings are “1” or “15”. The initial Retry Limit is “15”.
6	Display the Save Bad Packet flag setting on the node whose Station Address is ADR (see Table 5-1). If “1” is set, invalid (bad) IEEE 802.3 packets are saved and passed to Node Manager software for logging. If “0” is set, bad packets are discarded. The initial setting is “0”.
7	Display the Trace Mode flag setting on the node whose Station Address is ADR (see Table 5-1). If “1” is set, packets unsuccessfully transmitted are echoed to Node Manager software for logging. If “0” is set, tracing is disabled. The initial setting is “0”.
8	Display a table of “DSAPs versus Class Numbers” maintained by the driver for the LANIC card whose Station Address is ADR (see Table 5-1).
9	Display the Downloading Server Station Address stored on the LANIC card whose Station Address is ADR (see Table 5-1).
10	Display the File Server Station Address associated with the LANIC card whose Station Address is ADR (see Table 5-1). The File Server Station Address is stored by Node Manager in a software variable; *IT IS NOT STORED IN NOVRAM ON THE CARD*.
11	Display LANIC card status information for the card whose Station Address is ADR (see Table 5-1). A status word is returned. See Table 5-5 for bit definitions.
A	This invokes PAR# values 1, 4, 5, 6, 7, 9, and 10, and is the default value if PAR# is not specified.

Table 5-4. Receive Packet Filter Mode Settings

Setting	Categories of Packet Addresses a Node Will Accept
0	Individual only (default setting)
1	Individual + Promiscuous
2	Individual + Broadcast
3	Individual + Broadcast + Promiscuous
4	Individual + Multicast
5	Individual + Multicast + Promiscuous
6	Individual + Multicast + Broadcast
7	Individual + Multicast + Broadcast + Promiscuous

RC Command Examples

Here are examples of using the Read Link Configuration (RC) command.

Example 1. Using RC Command Defaults

```
NM> RC<RETURN>
Read 802.3 Link Config from node        08-00-09-00-02-5A....

Station Address               08-00-09-00-02-5A
Downloading Server Address    08-00-09-00-03-85
File Server Station Address   08-00-09-00-03-85
Receive Packet Filter         06
Retry Limit                   0F
Save Bad Packet Flag          01
Extended Trace Mode Flag      00

NM>
```

Example 1 shows a listing returned when all command parameters are defaulted. (The same listing would be returned if RC,,A<RETURN> was entered).

In this case ADR defaulted to 08-00-09-00-02-5A hex, which is the Station Address of the LANIC card with the lowest LU. Because the PAR# parameter defaults to "A", the values associated with PAR# entries 1, 4, 5, 6, 7, 9, and 10 are returned.

Because the parameters ADR and LU# refer to the same card, the Station Address indicated is the same as that of the target node. The Downloading Server Address is the Download Server Station Address stored on the card (RAM). The File Server Station Address represents the node where the Link File directory for the target node is maintained.

Since the Receive Packet Filter setting is 06, this node receives Individual Multicast, and Broadcast messages (see Table 5-4). Since the Retry Limit is 0F hex (decimal 15), this node will try to transmit a packet up to 16 times (initial attempt plus 15 Retries) until successful.

The Save Bad Packet Flag is set, so this node will save invalid IEEE 802.3 packets for passing to Node Manager software. The Trace Mode Flag has not been set, so unsuccessful packet transmissions are not returned to Node Manager software.

Example 2. Displaying a Node's Multicast Address List

```
NM> RC,08-00-09-00-02-5A,2<RETURN>
Read 802.3 Link Config from node        08-00-09-00-02-5A....

Multicast Address List
09-00-09-10-0A-5C       FF-FF-FF-FF-FF-09       FF-FF-FF-FF-FF-0E
FF-FF-FF-FF-FF-10       FF-FF-FF-FF-FF-12

NM>
```

In Example 2, an ADR parameter is specified and represents the target node's Station Address. Note that hyphens (−) are required between each pair of hexadecimal digits of the address when entering the command. Also, PAR# is specified as 2 to display the node's Multicast Address List configured on the card.

The default LU# parameter depends on whether the target node is local or remote. See Table 5-1.

The Multicast Addresses configured on this node may have been written from the node's File Server node containing the Link File directory (and MCAST.TXT file), or may have been inserted using the Insert Multicast Address command, described later. Note that the listing is in hexadecimal.

Example 3. Displaying LANIC Card Status

```
NM> RC,,11<RETURN>
Read 802.3 Link Config from node         08-00-09-00-02-5A....

Card Status

          DMA DME NVF LWS     UIP WTB RPA NRB MPF MME BME PME NV2
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

NM>
```

Example 3 provides a display of the LANIC status word that can be obtained from an RC Command.

If PAR# is specified as 11, then a status word of the target node is returned. The two leftmost bits are always "0" and reserved for future use. The remaining 14 bits are returned with an acronym representing a status condition. If a bit is set ("1"), that condition exists.

Table 5-5 provides the meanings of the various bits. Note that the above bit pattern returned indicates that the node with Station Address 08-00-09-00-02-5A has Promiscuous Mode and Broadcast Mode enabled. In addition, the last write to the card was successful.

Table 5-5. LANIC Card Status Bit Definitions

Status Code	Status Definition
NV2	NOVRAM Bank #2 is in use. Nonvolatile memory is broken into two redundant banks. If this bit is set to "1", Bank #1 has failed and the back-up memory bank is in use. The LANIC card (or NOVRAM) should be replaced at the next opportunity.
PME	Promiscuous Mode is enabled. The node will accept every packet transmitted on the LAN. (Refer to Chapter 4.)
BME	Broadcast Mode is enabled. The node will accept packets containing Broadcast addresses.
MME	Multicast Address Mode is enabled. The node will accept packets containing Multicast addresses.
MPF	MAU power failure. The MAU draws its power through the LANIC card and cannot operate when power is lost. A likely cause is a blown fuse. Refer to the *HP 12076A LAN/1000 Link Local Area Network Interface Controller (LANIC) Installation Manual* (part number 12076-90001) for fuse replacement instructions.
NRB	No receive buffers. Receive Transmission (RX) buffers on the card are full and cannot accept additional packets.
RPA	Receive packet available. A packet is in a Receive Transmission (RX) buffer waiting to be read by the system.
WTB	Waiting for a transmit buffer. The driver is currently waiting for transmission buffer space on the card.
UIP	Unsolicited interrupt pending. The card has attempted to interrupt the driver (for example, because of a received packet is available), but the driver has not yet responded.
LWS	Last write status. This bit refers to writes to the card and is normally "1". When this bit is "0", the last write was unsuccessful.
NVF	NOVRAM failure. This bit indicates that NOVRAM data has been lost. If repeated failures occur after rewriting to NOVRAM, it may be necessary to replace NOVRAM. Consult the *HP 12076A LAN/1000 Link Local Area Network Interface Controller (LANIC) Installation Manual* (part number 12076-90001) for NOVRAM replacement instructions.
DME	ARP packet filter mode is enabled. If the target IP address in the ARP packet does not match the configured IP address, the packet is discarded.
DMA	The last Direct Memory Access operation aborted abnormally.

Example 4. Displaying LANIC Card's DSAP/Class Number List

```
   NM> RC,,8<RETURN>
   Read 802.3 Link Config from node         08-00-09-00-02-5A....

   DSAP/CLASS NUMBER LIST

-------------------------------------------------------------------------
DSAP range       corresponding   CLASS NUMBERS
                   of the even number SAPs
-------------------------------------------------------------------------

  0 -  14   |     0      0      0      0      0      0      0      0
 16 -  30   |     0      0      0      0      0      0      0      0
 32 -  46   |     0      0      0      0      0      0      0      0
 48 -  62   |     0      0      0      0      0      0      0      0
 64 -  78   |     0      0      0      0      0      0      0      0
 80 -  94   |     0      0      0      0      0      0      0      0
 96 - 110   |     0      0      0      0      0      0      0      0
112 - 126   |     0      0      0      0      0      0      0      0
128 - 142   |     0      0      0      0      0      0      0      0
144 - 158   |     0      0      0      0      0      0      0      0
160 - 174   |     0      0      0      0      0      0      0      0
176 - 190   |     0      0      0      0      0      0      0      0
192 - 206   |     0      0      0      0      0      0      0      0
208 - 222   |     0      0      0      0      0      0      0      0
224 - 238   |     0      0      0      0      0      0      0      0
240 - 254   |     0      0      0      0   3391      0      0      0

NM>
```

In Example 4, the driver's class table associated with a particular LANIC card is displayed. This table shows the system class numbers posted to even-numbered SAPs identifying programs that intend to receive packets from this card.

The table is organized such that the numbers on the left indicate the range of SAPs covered in that row. For example, the second row contains class numbers for SAPs 16, 18, 20, 22, 24, 26, 28, and 30. For this row, there are no class numbers posted to these SAPs.

For this particular node, the table reflects that only one class number is posted. The Node Manager software's class number 3391, assigned by the system, is posted to SAP F8 hex (248 decimal).

By definition, there are no odd-numbered SAPs. A received packet containing an odd DSAP is a Group DSAP packet. The driver routes Group DSAP packets to the program whose class number is posted to a special program code "7" (not reflected in the display above).

Note Node Manager software does not handle Group DSAP packets. For Group DSAP packet handling, a user-written program is required. Refer to the *HP 12079A Direct Driver Access Manual* product, part number 12079-90001, for further information.

Set Link Configuration Command (SC)

The Set Link Configuration command allows the user to modify various local and remote node configuration parameters. This includes the node's Station Address, Download Server Station Address, and File Server Station Address. In addition, the Receive Packet Filter mode, Retry Limit, Save Bad Packet flag, and Trace Mode flag can be set.

Caution Users should consult with a System or Network Manager prior to modifying local or remote configuration parameters.

The syntax for the Set Link Configuration command is:

```
SC,[ADR],PAR#[,[PAR-value][,[option][,LU#]]]
```

where:

`ADR` This is the "target" Station Address; that is, the node whose configuration parameters are to be set. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`PAR#` This parameter is a required entry and must be specified as one of the following integers: 1, 4, 5, 6, 7, 9, or 10. Table 5-6 shows the meaning of each `PAR#` integer.

`PAR-value` For the `PAR#` parameter specified above, the `PAR-value` parameter provides the new value to be set. If not supplied, it is defaulted. See Table 5-7 for the possible `PAR-value` settings available and default values associated with each `PAR#` entry.

`option` "P" or "T" may be entered for NOVRAM-stored parameters (`PAR#` integers 1, 4, 5, 6, 7, or 9).

If P is entered, the parameter specified by `PAR#` is modified in both RAM and NOVRAM. Because the NOVRAM value is modified, the change is "permanent".

If T is entered, the parameter is modified in RAM only. This change is "temporary" because NOVRAM contents are not affected. T is the default entry if option is not specified.

Note that parameters never stored in NOVRAM (for example, File Server Station Address, `PAR#` = 10) *are not permanent regardless of the option specified and will be lost if the Node Manager software is terminated*.

`LU#` This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. `LU#` is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

Note Modification of NOVRAM data (that is, option = P) should be minimized. Due to physical properties of the NOVRAM, there is a finite number of times that its bit cells can undergo a change. This number is on the order of 1000 changes and should not pose a serious limitation. However, it is conceivable that useful NOVRAM life may be exceeded. (For NOVRAM replacement information, refer to the *HP 12076A LAN/1000 Link Local Areal Network Interface Controller (LANIC) Installation Manual*, part number 12076-90001.)

Whenever node or network configuration changes are made, attention to administrative controls is recommended. For example, if the NOVRAM's Station Address is changed, the NOVRAM should be relabeled to indicate the new Station Address. Also, node or network logbooks should be updated to reflect any changes.

When shipped from the factory, a LANIC card NOVRAM contains data that includes initial parameter values as shown in Chapter 4 (see Table 4-1).

Table 5-6. SC PAR# Definitions

PAR#	Definition
1	Set the Station Address of the node whose Station Address is ADR (see Table 5-1 for ADR defaults).
4	Set the Receive Packet Filter mode for the node whose Station Address is ADR (see Table 5-1 for ADR defaults).
5	Set the Retry Limit on the node whose Station Address is ADR (see Table 5-1 for ADR defaults). On a packet transmission failure, the Retry Limit is the number of times the card reattempts transmission.
6	Set the Save Bad Packet Flag on the node whose Station Address is ADR (see Table 5-1 for ADR defaults). Essentially, a bad packet is an invalid IEEE 802.3 packet.
7	Set the Trace Mode Flag for the node whose Station Address is ADR (see Table 5-1 for ADR defaults). Trace packets are unsuccessfully transmitted packets echoed to the driver.
9	Set the Download Server Station Address for the node whose Station Address is ADR (see Table 5-1 for ADR defaults).
10	Set the File Server Station Address for the node whose Station Address is ADR (see Table 5-1 for ADR defaults). The File Server Station Address is stored by Node Manager as a software variable; *IT IS NOT STORED IN NOVRAM* on the card.

Table 5-7. PAR-Value Range

PAR#	Possible PAR-Value Entries
1	Any valid IEEE 802.3 Individual Station Address, entered as 6 pairs of hexadecimal digits, separated by hyphens. Note that Multicast or Broadcast addresses are not allowed. If a PAR-value entry is not supplied, it defaults to ADR.
4	A digit from "0" to "7", that defines categories of packet addresses the node will accept, as follows: 0: Individual only (default if not specified) 1: Individual + Promiscuous 2: Individual + Broadcast 3: Individual + Broadcast + Promiscuous 4: Individual + Multicast 5: Individual + Multicast + Promiscuous 6: Individual + Multicast + Broadcast 7: Individual + Multicast + Broadcast + Promiscuous
5	Either "1" or "15" retries. Since the default is zero,"1" or "15" should be specified.
6	Either "0" or "1", where: 0: bad packets are discarded (default if not specified). 1: bad packets are saved on the card and routed by the driver to a handling program (Node Manager software).
7	Either "0", or "1", where: 0: packet tracing disabled (default if not specified). 1: transmit packet tracing enabled.
9	Any valid IEEE 802.3 Individual Station Address. (Multicast or Broadcast Addresses not allowed.) If not specified, the default is ADR.
10	Any valid IEEE 802.3 Individual Station Address of a disk-based node designated to store the target node's Link File directory. If not supplied, the default is ADR.

Station Address Considerations

The NOVRAM initially contains a globally administered Station Address (12 hexadecimal digits) of which the last six digits are labeled on the NOVRAM. Once altered from its assigned value, there can be no assurance that it is unique within or across manufacturers.

If a NOVRAM is physically replaced on a node, that node's Station Address will now be different. It may be necessary to either notify and update all other nodes on the network with the new address, or reconfigure the old Station Address into the new NOVRAM on the affected node.

Note Addresses placed in NOVRAM by Hewlett-Packard will not be reissued.

Download Server Station Address Considerations

The NOVRAM's initial Download Server Station Address is the Broadcast address (that is, FF-FF-FF-FF-FF-FF hex). This value is assigned to allow for initial boot-up (especially for a memory-based node) where a VCP Server node or File Server node may be acquired over the LAN.

However, except for very special applications, the Download Server Station Address should be changed to an Individual Station Address of the node that will provide VCP and File Server services.

After boot-up, presuming Node Manager software is running, it is recommended that a node's Download Server Station Address be changed to its File Server Station Address. On system reboot or reinitialization of Node Manager software, the Link File directory for the applicable card will be automatically accessed by Node Manager.

File Server Station Address Considerations

Node Manager software uses a node's File Server Station Address as a pointer to the disk-based system (local or remote) designated to maintain the node's Link File directory. Through this directory, event logging for the node is performed.

A node's File Server Station Address is not stored in NOVRAM; instead, it is stored as a variable by the Node Manager software. Note the following:

- Before the software initializes, the File Server Station Address cannot be set by the user. During software initialization, the address is either acquired through the use of the Download Server Station Address (stored in NOVRAM), or set to zero. For more information on this process, refer to the "Node Manager Software Initialization" section in Chapter 4.

- Once the Node Manager software is running, the user can set and change the File Server Station Address for a particular LANIC card. If the software terminates, the address is "lost".

Packet Filter Mode Considerations

Using the SC command, a node is configured to receive and accept packets based on their Destination Addresses. See Chapter 4 for a discussion on Packet Filter Addressing modes.

For example, even if a node contains Multicast Addresses (see the Insert Multicast Address, IM, command), the node will be unable to receive applicable Multicast Address packets unless it is configured with one of the Multicast Address filter settings (see Table 5-7).

It is recommended that only those systems used for dedicated applications, such as online monitoring, be configured with Promiscuous mode settings.

Caution On an active network, a node configured for Promiscuous operation will consume significant system overhead and may render that system inaccessible.

SC Command Examples

The following examples illustrate the use of the Set Link Configuration command.

Example 1. Setting the Trace Mode Filter Flag

```
NM> SC,,7<RETURN>
Set 802.3 Link Config of node            08-00-09-00-02-5A

Extended Trace Mode Flag       00

NM>
```

In Example 1 above, the ADR and LU# parameters are defaulted, so the target node is a local LANIC card with the lowest LU (it happens to be node 08-00-09-00-02-5A). Since PAR-value is defaulted, the trace mode is disabled. This is verified by the value returned "00".

Example 2. Setting the Retry Limit

```
NM> SC,,5,15<RETURN>
Set 802.3 Link Config of node            08-00-09-00-02-5A

Retry Limit      15

NM>
```

Example 2 sets the Retry Limit on the node with Station Address 08-00-09-00-02-5A to "15".

Example 3. Setting the Download Server Station Address

```
NM> SC,,9,08-00-09-00-02-20<RETURN>
Set 802.3 Link Config of node            08-00-09-00-02-5A

Downloading Server Address    08-00-09-00-02-20

NM>
```

Example 3 sets the Download Server Station Address on the local node to "08-00-09-00-02-20", as verified by the return.

Example 4. Multicast Address as the Download Server Station Address

```
NM> SC,,9,09-00-09-00-02-20<RETURN>
Set 802.3 Link Config of node            08-00-09-00-02-5A
ERROR:  DE006 REPORTING NODE ADR:08000900025A SAP: F8
Value out of range

NM>
```

Example 4 attempts to set a Multicast Address as the Download Server Station Address on the local node. The driver returns an error indicating that the input address was "out of range" (that is, improper).

Update Link Configuration Command (UC)

The Update Link Configuration command is similar to the SC command except that it allows the user to modify various LANIC card configuration parameters interactively through a single command.

Caution Users should consult with a System or Network Manager prior to modifying local or remote node configuration parameters.

Note During an interactive UC command session, an entry that exceeds 128 characters will abort the Node Manager software interface program. Subsequently, it must be rerun.

The syntax of this command is:

```
UC[,[ADR][,[option][,LU#]]]
```

where:

`ADR` This is the "target" Station Address, that is, the node whose configuration parameters are to be set. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`option` "P" or "T" may be entered for NOVRAM-stored parameters.

If P is entered, parameters corresponding to `PAR#` values 1, 4, 5, 6, 7, or 9 in Table 5-6 are modified in both RAM and NOVRAM with the `PAR-value` entry (see Table 5-7) that you specify. Because NOVRAM values are modified, the change is "permanent".

If T is entered, the applicable parameters are modified in RAM only. This change is "temporary" because NOVRAM contents are not modified. T is the default entry if `option` is not specified.

Note that parameters never stored in NOVRAM (for example, File Server Station Address, `PAR#` = 10) *are not permanent regardless of the option specified and will be lost if the Node Manager software is terminated*.

`LU#` This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. `LU#` is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

Note Modification of NOVRAM data (that is, `option = P`) should be minimized. Due to physical properties of the NOVRAM, there is a finite number of times that its bit cells can undergo a change. This number is on the order of 1000 changes and should not pose a serious limitation. However, it is conceivable that useful NOVRAM life may be exceeded. (For NOVRAM replacement information, refer to the *HP 12076A LAN/1000 Link Local Area Network Interface Controller (LANIC) Installation Manual*, part number 12076-90001.)

Whenever node or network configuration changes are made, attention to administrative controls is recommended. For example, if the NOVRAM's Station Address is changed, the NOVRAM should be relabeled to indicate the new Station Address. Also, node or network logbooks should be updated to reflect any changes.

Because the UC and SC commands serve similar functions, refer to the "Set Link Configuration Command (SC)" paragraphs for a discussion of Station Address, Download Server Station Address, and File Server Station Address considerations.

During an interactive UC command session, an existing configuration parameter value is displayed, and the user is prompted for a new value. (See the SC command description, Table 5-7, for possible parameter values.)

Note The Save Bad Packet configuration requires "Y" or "N" responses instead of "1" or "0", respectively.

If a new value is desired, it is entered; if no change is desired, nothing is entered. On carriage return (pressing the `<RETURN>` key), the next parameter is displayed and the process repeats until all configuration parameters are considered.

New configuration parameters are not actually implemented until the UC command's interactive session ends normally. The session may be aborted by pressing the `<CNTL>` and "`D`" keys simultaneously. Parameters entered during an aborted UC command session are invalid and will not reconfigure the target node.

UC Command Example

The following is a typical session using the Update Link Configuration command.

Example 1. Typical UC Command, Command Parameters Defaulted

```
NM> UC<RETURN>
Read 802.3 Link Config of node          08-00-09-00-02-41....
--- Interactive Configuration ---

to keep the old configuration - hit return key
to abort - type CNTL(D)

old Station Address: 08-00-09-00-02-41
enter New Station Address:08-00-09-00-02-5A<RETURN>

old Downloading Server Station Address: 08-00-09-00-02-10
enter New Downloading Server Station Address:<RETURN>
parameter unchanged

old File Server Station Address: 08-00-09-00-02-10
enter New File Server Station Address:<RETURN>
parameter unchanged

old Receive Packet Filter:  6 ---> I+M+B

I: Individual, P: Promiscuous
B: Broadcast , M: Multicast

0: I         , 1: I+P
2: I+B       , 3: I+B+P
4: I+M       , 5: I+M+P
6: I+M+B     , 7: I+M+B+P

enter New Receive Packet Filter [0~7]:<RETURN>
parameter unchanged

old Retry Limit: 15
enter New Retry Limit [1 or 15]:<RETURN>
parameter unchanged

old Save Bad Packet Flag: NO
enter new Save Bad Packet Flag [Y/N]:<RETURN>
parameter unchanged

old Trace Mode: 0
0: no trace message returned - trace disabled
1: trace message returned - only packet w/ Xmit err
```

```
enter New Trace Mode [0,1]:<RETURN>
parameter unchanged
Read 802.3 Link Config of node          08-00-09-00-02-41

Station Address               08-00-09-00-02-5A
Downloading Server Address    08-00-09-00-02-10
File Server Station Address   08-00-09-00-02-10
Receive Packet Filter         06
Retry Limit                   0F
Save Bad Packet Flag          00
Extended Trace Mode Flag      00

NM>
```

In the example, ADR and LU# were defaulted and refer to the same card (see Table 5-1), that is, the card with Station Address 08-00-09-00-02-41. Because the option parameter was defaulted, the "T" option applies; any configuration values changed are temporary and affect card RAM only, not NOVRAM.

There was only one parameter value modified in the above example, the Station Address. Following any user inputs, the resulting configuration parameter values are listed. Note that it shows the new (temporary) Station Address for the node.

Insert Multicast Address Command (IM)

This command is used to insert a Multicast Address.

Note The LANIC card will accept packets that utilize this address only when the appropriate Packet Filter Mode is configured (see the SC command).

The syntax of the command is:

```
IM,[ADR],MulticastAddress[,LU#]
```

where:

`ADR` This is the "target" Station Address, that is, the node to which a Multicast Address will be added. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`MulticastAddress` This is the 6-byte Multicast Address that is being added to the LANIC card's Multicast Address list. The address specified must conform to the IEEE 802.3 standard for Multicast Addresses. This parameter is required and entered as 6 pairs of hexadecimal digits separated by hyphens.

LU# This is the Logical Unit number of the LANIC card through which the command is transmitted and from which a response is received. It is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

When a Multicast Address is configured in a card (in RAM), the driver stores a copy in its IFT (Interface Table) extension area. The memory allocated for this use is created during system generation. Three words of memory are required for each Multicast Address.

Note If there is not enough space in the IFT extension area for the Multicast Addresses, this command will fail with a driver error (DE007, see Appendix A). The default IFT extension size is sufficient for use with HP's networking software products. If your application accesses the LAN driver directly, you may need to modify the IFT extension size. See the *HP 12079A LAN/1000 Link Direct Driver Access Manual* product, part number 12079-90001.

Should the card lose its Multicast Addresses, such as on a card reset or powerfail, the driver will rewrite its copy to reconfigure the card.

Note that this command does not add entries in the MCAST.TXT file associated with the card. If a node's MCAST.TXT file requires updating, the HP 1000 editor must be used.

IM Command Examples

The following examples illustrate the use of the Insert Multicast Address command:

Example 1. Verifying the Addition of a Multicast Address

```
NM> RC,08-00-09-00-02-5A,2<RETURN>
Read 802.3 Link Config of node          08-00-09-00-02-5A....

Multicast Address Lis
FF-FF-FF-FF-FF-09       FF-FF-FF-FF-FF-0E       FF-FF-FF-FF-FF-10
FF-FF-FF-FF-FF-12

NM> IM,08-00-09-00-02-5A,F3-00-09-00-02-03<RETURN>
Insert Parameter on node                08-00-09-00-02-5A....

Multicast Address Inserted     F3-00-09-00-02-03

NM> RC,08-00-09-00-02-5A,2<RETURN>
Read 802.3 Link Config of node          08-00-09-00-02-5A....

Multicast Address List
F3-00-09-00-02-03       FF-FF-FF-FF-FF-09       FF-FF-FF-FF-FF-0E
FF-FF-FF-FF-FF-10       FF-FF-FF-FF-FF-12
```

```
NM>
```

In Example 1, we first read the Multicast Addresses configured on the LANIC card whose Station Address is 08-00-09-00-02-5A. Initially there are four Multicast Addresses configured.

Next, the Multicast Address F3-00-09-00-02-03 is added using the IM command. A message is returned verifying the added address.

Finally, an RC command is repeated. Note that, with the added address, there are five Multicast Addresses configured.

Example 2. Adding an Invalid Multicast Address

```
NM> IM,,08-00-09-00-02-0B<RETURN>
        ^1

error  1 ---> Address must be a MULTICAST 802.3 address
NM>
```

In Example 2, the least significant bit of the most significant byte is "0" reflecting an even valued byte. This address is not a valid group (that is, Multicast) address, and the Node Manager interface returns the command entry error message. (See Chapter 2 for more information on address field format.)

Delete Multicast Address Command (DM)

This command is used to delete a Multicast Address configured on the LANIC card. In addition, the driver's copy of the Multicast Address stored in the driver's IFT (Interface Table) extension area is also erased.

The syntax of this command is:

```
DM,[ADR],MulticastAddress[,LU#]
```

where:

`ADR`	This is the "target" Station Address, that is, the node from which a Multicast Address will be deleted. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default ADR addresses.
`MulticastAddress`	This is the 6-byte Multicast Address which is being deleted from the LANIC card's Multicast Address list. The address specified must conform to the IEEE 802.3 standard for Multicast Addresses. This parameter is required and entered as 6 pairs of hexadecimal digits separated by hyphens (see examples below).
`LU#`	This is the Logical Unit number of the LANIC card through which the command is transmitted and from which a response is received. It is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

Note that this command does not delete entries in the MCAST.TXT file associated with the target node. If a node's MCAST.TXT file requires updating, the editor must be used.

DM Command Examples

The following examples illustrate the use of the Delete Multicast Address (DM) command.

Example 1. Deleting a Multicast Address

```
NM> DM,08-00-09-00-02-5A,F3-00-09-00-02-03<RETURN>
Delete Parameter on node               08-00-09-00-02-5A....

Multicast Address deleted       F3-00-09-00-02-03

NM> RC,08-00-09-00-02-5A,2<RETURN>
Read 802.3 Link Config of node         08-00-09-00-02-5A....

Multicast Address List
FF-FF-FF-FF-FF-09       FF-FF-FF-FF-FF-0E       FF-FF-FF-FF-FF-10
FF-FF-FF-FF-FF-12
NM>
```

Example 1 deletes the Multicast Address F3-00-09-00-02-03 previously configured on the node, as verified by the returned comment. This is confirmed with an RC command to read the Multicast Addresses now configured.

Example 2. Deleting a Non-existent Multicast Address

```
NM> DM,08-00-09-00-02-5A,F3-00-09-00-02-03<RETURN>
Delete Parameter on node             08-00-09-00-02-5A....[failed]
ERROR:  LE008 REPORTING NODE ADR:08000900025A  SAP: F8
Multicast Address does not exist
NM>
```

Once the Multicast Address was deleted by Example 1, Example 2 shows that attempting to again delete this Multicast Address when it is not configured on the node results in a Link Error (see Appendix A).

Create Link File Directories Command (CD)

This command creates a subdirectory (that is, the Link File directory) and two files under the root directory, FILES802, on a designated File Server (disk-based) node.

The Link File directory's name will identify the node to which it is associated since it contains the node's Station Address (in a compressed form).

A node's Link File directory will contain two files: MCAST.TXT and EL.TXT. On initialization, Node Manager software will write the Multicast Addresses contained in the MCAST.TXT file to the respective node. When the node is properly configured, "bad", "orphan", and "trace" packets will be logged to the EL.TXT file. (See Chapter 4.)

The syntax of this command is:

```
CD[,[ADR][,[FileAddress][,LU#]]]
```

where:

`ADR`	This is the "target" Station Address, that is, the disk-based node on which the Link File directory will be created. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-2 for default addresses.
`FileAddress`	This is a 6-byte Station Address of the node for which a Link File directory is created. Through a mapping process, Node Manager uses this entry to name the Link File directory (see Chapter 4). `FileAddress` is entered using 6 pairs of hexadecimal digits separated by hyphens. See Table 5-2 for default entry values.
`LU#`	This identifies the Logical Unit number of the LANIC card through which the command is transmitted and from which a response is received. It is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-2 for default values.

Note that the `ADR` parameter is the File Server Station Address for the node specified by `FileAddress`. However, neither the local nor remote Node Manager variable for storing the File Server Station Address is updated with this information. In other words, after a CD command is executed, the `FileAddress` node still does not "know" its File Server Station Address.

The SC or UC commands are used to update a node's File Server Station Address variable maintained by the Node Manager software. In addition, these commands may configure the File Server Station Address as the Download Server Station Address (in NOVRAM) to make it more permanent. Refer to the SC and UC command descriptions for additional information.

CD Command Example

The following example utilizes the Create Link File Directories command.

Example 1. Creating a Link File Directory

```
NM> RC,08-00-09-00-02-00,10<RETURN>
Read 802.3 Link Config of node        08-00-09-00-02-00....

File Server Station Address     00-00-00-00-00-00

NM> CD,08-00-09-00-02-5A,08-00-09-00-02-00<RETURN>
Create Link File Directories on node  08-00-09-00-02-5A....  [ok]

NM> RC,08-00-09-00-02-00,10<RETURN>
Read 802.3 Link Config of node        08-00-09-00-02-00....

File Server Station Address     00-00-00-00-00-00

NM> SC,08-00-09-00-02-00,10,08-00-09-00-02-5A<RETURN>
Set 802.3 Link Config of node         08-00-09-00-02-00....

File Server Station Address     08-00-09-00-02-5A

NM> RC,08-00-09-00-02-00,10<RETURN>
Read 802.3 Link Config of node        08-00-09-00-02-00....

File Server Station Address     08-00-09-00-02-5A

NM>
```

In Example 1, the first Read Link Configuration command determines that a File Server Node is not configured for node 08-00-09-00-02-00. This is indicated by the response (all zeros).

The next command, CD, results in the creation of a Link File directory named ADDR080009000200. This directory is contained in the root directory, FILES802, on a File Server Node (08-00-09-00-02-5A).

Note Node Manager software will not allow the creation of a duplicate Link File directory on the same File Server Node. However, a Link File directory for a given node may exist on separate File Server Nodes. The one accessed will depend on the File Server Station Address configured.

Although its Link File directory now exists, another RC command shows that the location of this directory is not configured on the node.

Using the SC command, the File Server Station Address is configured and identifies the node's File Server Node.

Purge Link File Directories Command (PD)

This command allows the user to purge a Link File directory associated with a particular node from the root directory (FILES802) on a File Server Node.

Caution Once purged, a subdirectory and the files it contains may not be recoverable. Be sure you want to delete the directory before doing so.

The syntax of this command is:

```
PD[,[ADR][,[FileAddress][,LU#]]]
```

where:

`ADR` This is the Station Address of the File Server Node from which a particular Link File directory is to be deleted. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-2 for default entries.

`FileAddress` This is the Station Address of the node that identifies the Link File directory to be purged. It is entered as 6 pairs of hexadecimal digits separated by hyphens, and is mapped to the name of the Link File directory. See Table 5-2 for default values.

`LU#` This is the Logical Unit number of the LANIC card through which the command is transmitted and from which a response is received. It is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-2 for default values.

Although a Link File directory associated with a particular node is purged, that node's File Server Node (configured and stored by Node Manager software in a File Server Station Address variable) is not updated. Hence the node will still "think" that its Link File directory is still located at the File Server Node. (See the CK command for checking the existence of a particular Link File directory on a specified node.)

PD Command Example

The following example illustrates the use of the Purge Link File Directories Command.

Example 1. Purging a Link File Directory

```
NM> PD,08-00-09-00-02-5A,08-00-09-00-02-00<RETURN>
Purge Link File Directories on node    08-00-09-00-02-5A....  [ok]

NM> RC,08-00-09-00-02-00,10<RETURN>
Read 802.3 Link Config of node         08-00-09-00-02-00....

File Server Station Address      08-00-09-00-02-5A

NM> SC,08-00-09-00-02-00,10,00-00-00-00-00-00<RETURN>
Set 802.3 Link Config of node          08-00-09-00-02-00....

File Server Station Address      00-00-00-00-00-00

NM>
```

In Example 1, the Link File directory ADDR080009000200 and its files are purged from the File Server Node (File Server Station Address is 08-00-09-00-02-5A).

As shown by the RC command, the File Server Station Address is still configured at the node whose Link File directory was purged. The subsequent SC command reconfigures the File Server Station Address to the null address.

Check Link File Existence Command (CK)

This command allows the user to check whether a particular Link File directory exists on a specified disk-based node that is being used for Node Manager file services.

The syntax of this command is:

```
CK[,[ADR][,[FileAddress][,LU#]]]
```

where:

`ADR`	This is the Station Address of the File Server Node that is being checked for the existence of a Link File directory. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-2 for default entries.
`FileAddress`	This is the Station Address of the node that identifies the Link File directory. It is entered as 6 pairs of hexadecimal digits separated by hyphens, and is mapped to the name of the Link File directory. See Table 5-2 for default entries.
`LU#`	This is the Logical Unit number of the LANIC card through which the command is transmitted and from which a response is received. It is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-2 for default values.

CK Command Examples

The following examples illustrate the use of the Check Link File Existence command.

Example 1. Link File Directory Exists on File Server Node

```
NM> CK,08-00-09-00-02-5A,08-00-09-00-02-0B<RETURN>
Check Link Directory Existence on node       08-00-09-00-02-5A....  [ok]

NM>
```

In Example 1, the node (Station Address 08-00-09-00-02-5A) is checked for the directory /FILES802/ADDR08000900020B. Since it exists, the only confirmation is an "`[ok]`".

Example 2. Link File Directory Does Not Exist on File Server Node

```
NM> CK,08-00-09-00-02-0B,08-00-09-00-02-0B<RETURN>
Check Link Directory Existence on node    08-00-09-00-02-5A....  [failed]
ERROR:  FM0D1 REPORTING NODE ADR:08000900020B SAP: F8
No such directory

NM>
```

In Example 2, the directory /FILES802/ADDR08000900020B does not exist and "`[failed]`" is returned. In addition, an FMP error is returned (see Appendix A) along with confirmation that the directory does not exist on the designated node.

Diagnostic Commands

Communication degradation or failure among nodes on the LAN can occur for many reasons. These include, for example, improper physical connections, hardware failure, configuration errors, excessive network traffic, and environmental factors. To correct node or network communication problems, the cause(s) must be isolated.

For each LAN/1000 node that is running Node Manager software, several commands provide limited diagnostic capability. These "Diagnostic Commands" provide problem isolation to three broad levels of node or network operation:

1. LANIC card operation using the card self-test.

2. Link operation from the LANIC card to the LAN coaxial cable medium (that is, the LANIC card, Attachment Unit Interface (AUI) cabling, Medium Attachment Unit (MAU), and LAN coaxial cable connections) using a LANIC card external loopback test.

3. Network operation from one LAN/1000 Link to another over the coaxial cable medium using IEEE 802.2 TEST and XID packets.

In general, the Node Manager software may be used to sequentially test node communications by issuing an appropriate command first at the card level, then the link level, and finally the network level. (Once isolated to a particular level, a problem may require other tools and resources for further isolation and correction.)

Using the Node Manager diagnostic commands, each node may be accessed locally, or remotely if communications are not completely severed. Diagnostic commands are listed below, and discussed on the following pages.

- LANIC Self-Test Command, TC
- Do External Loopback to MAU Command, EL
- Issue TEST Loopback Command, TEST
- XID Command Loopback Command, XID

The Rep Parameter

In each of the diagnostic commands, an optional parameter, Rep, provides for command repetition. The default value is "1", indicating the command is issued once only. A value up to "9999" is possible. A special value of "0" specifies continuous command repetition until a failure occurs, or the command is aborted.

When Rep is specified other than "1", a command completes and a response is returned to the user's terminal prior to another command cycle. Thus, Rep provides a repetitive loopback mechanism for transmissions to and from remote nodes.

To exit from excessive command repetition, the process may be aborted by following the sequence below:

1. Press any key, resulting in the Command Monitor system program prompt (CM>).

2. Set the break flag for the NM module, as follows:

```
CM> br,NM<RETURN>
```

LANIC Self-Test Command (TC)

This command initiates a LANIC card self-test and returns the results to the user. In addition, all statistics counters maintained by the card are set to zero (see "Statistics Commands" later in this section).

The syntax for this command is:

```
TC[,[ADR][,[LU#][,Rep]]]
```

where:

ADR	This is the "target" Station Address of the node whose LANIC card undergoes self-test. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.
LU#	This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. LU# is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.
Rep	This parameter specifies the number of consecutive times this command is executed. Values from "0" to "9999" may be specified. When set to "0", the command is repeated indefinitely unless a failure occurs. The default value is "1".

Card self-test is conducted through ROM-based instructions and a microprocessor contained on the card. On self-test execution, any requests currently being processed by the LANIC card are terminated. On successful self-test completion, the driver is notified and the card is reset for operation with parameter values stored in NOVRAM (NOVRAM contents are written to RAM).

However, RAM contents may have differed from NOVRAM contents prior to self-test. For example, a Multicast Address List or temporary Station Address may have been configured on the card. To reconfigure the card into the state it was in prior to self-test, the driver writes its copy of the various configuration parameters to card RAM.

LANIC card self-test results are returned to the user. If the card successfully passes self-test, an "[ok]" indication is returned. On failure, a response consisting of an error note and a self-test status word are displayed on the user's terminal.

The self-test failed status word consists of 6 preset bits, and 10 bits designated by characters that reflect self-test failure status. Table 5-8 provides an interpretation of the 10 self-test status bits (also, see Example 2 below).

Table 5-8. Interpretation of TC Command Self-Test Failed Bits

Bit Setting	Interpretation
R1 = 1	RAM failed, replace LANIC card.
R0 = 1	RAM failed, replace LANIC card.
R = 1	RAM failed, replace LANIC card.
P = 1	PROM failed, replace LANIC card.
D = 1	Communications with card DMA controller chip failed, replace LANIC card.
I = 1	Microprocessor interrupt circuitry failed, replace LANIC card.
L = 1	Link controller chip failed, replace LANIC card.
M = 1	MAU power fuse on the LANIC card has failed, replace the fuse.*
N = 1	NOVRAM failed, replace NOVRAM.*
S = 0	No failure, or NOVRAM failure only.
S = 1	Failure other than NOVRAM has occurred.
*See the *HP 12076A LAN/1000 Link Local Area Network Interface Controller (LANIC) Installation Manual*, part number 12076-90001.	

The "S" bit is of special significance. It defines whether a failure is limited to NOVRAM, or whether one of the other failures occurred. If the failure is limited to NOVRAM only (S = 0), the card is still operational, and the driver writes its copy of node configuration data to card RAM (such as Multicast Addresses, temporary Station Address, and so forth). If one of the other failures is indicated (S = 1), the card will not operate properly, and the driver does not write its copy of configuration data to card RAM.

Note If card self-test fails for any reason other than NOVRAM failure, normal operation of the card is prevented by the driver. Card access is limited to self-test initiation.

TC Command Examples

The following examples illustrate command entry and response of the LANIC Self-Test command.

Example 1. Successful Self-Test Response

```
NM> TC,08-00-09-00-02-5A<RETURN>
Initiate 802.3 Card Self Test on node     08-00-09-00-02-5A....  [ok]

NM>
```

In Example 1, a TC command is sent to the node with Station Address 08-00-09-00-02-5A, which may have been a local or remote node. The card self-test was successful, as indicated by the "[ok]" returned.

Example 2. Failed Self-Test Response

```
NM> TC,08-00-09-00-02-0B<RETURN>
Initiate 802.3 Card Self Test on node     08-00-09-00-02-0B....  [failed]
ERROR:   DE00C REPORTING NODE ADR: 08000900020B SAP: F8
Self-test failed

  1  1  1  1  0  0  0  0  0  0  0  0  1  0  0  1
                R1 R0 R  P  D  I  L  M  N     S

bit set to one      failure
--------------      -------
     R1             RAM
     R0             RAM
     R              RAM
     P              PROM
     D              DMA controller
     I              Interrupt system
     L              Link controller
     M              MAU power fuse
     N              NOVRAM
     S              0 = only NOVRAM
                    1 = other failure

NM>
```

In Example 2, a TC command is sent to the node with Station Address 08-00-09-00-02-0B, which may be a local or remote node. A failed indication is returned ("`[failed]`") along with an error message from the driver reporting that self-test failed.

From Table 5-8, the self-test status word returned as a result of the card self-test failure indicates that the MAU power fuse is blown. Since the failure is not limited to NOVRAM failure, the "S" bit is set, and the driver does not rewrite its copy of configuration parameters to card RAM. The card is not useable.

Do External Loopback to MAU Command (EL)

Under control of the LANIC card firmware, this command causes a designated local or remote card to transmit a special loopback test packet from the card to the LAN coaxial cable, and to receive it back again.

Loopback results are displayed on the user's terminal. Loopback failure indications can be used to help isolate a hardware problem to the node or network level.

The syntax of this command is:

```
EL[,[ADR][,[LU#][,Rep]]]
```

where:

`ADR` This is the "target" Station Address of the node whose LANIC card transmits and receives a loopback test packet. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`LU#` This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. LU# is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

`Rep` This parameter specifies the number of consecutive times this command is executed. Values from "0" to "9999" may be specified. When set to "0", the command is repeated indefinitely unless a failure occurs or until the NM module break flag is set (see "The Rep Parameter" earlier in this section).

The EL command is conducted through PROM-based intelligence on the card. When initiated, the LANIC card attempts to transmit a special loopback test packet onto the LAN. From the card, the packet proceeds through the AUI (Attachment Unit Interface) cabling and MAU (Medium Attachment Unit), and onto the LAN. Subsequently, it is received by the LANIC card. Any monitored failures during this process are reported to the driver.

Node Manager software interprets the external loopback test results; on failure of monitored parameters, a "`[failed]`" indication and status word are returned to the user. Each relevant bit in the status word is identified by one or two characters. The applicable bits are defined in Table 5-9. (Also, see Example 2 below.)

The H bit, when set, indicates that the LANIC card did not receive a heartbeat (Signal Quality Error test signal) from the MAU. Most MAUs return this temporary signal to the LANIC card on each transmission to ensure proper operation of collision detection circuitry. Although a "`[failed]`" indication is returned, the lack of a heartbeat, by itself, does not positively identify a failed component. The LANIC card, AUI cabling and MAU may still be functioning properly.

Table 5-9. Interpretation of EL Loopback Test Bits

Bit Setting	Interpretation
NR = 1	The loopback test packet was not received by the LANIC card.
D = 1	The loopback test packet was deferred from transmission (for example, due to a busy network) for a period that exceeded a preset firmware timeout (approximately 1 second).
B = 1	On transmission, the number of valid packet bytes was exceeded and detected by the Link Controller chip (a “babble” error).
H = 1	The LANIC card’s MAU did not return a heartbeat signal.
M = 1	The LANIC card memory subsystem could not be accessed by the Link Controller chip on the card.
BT = 1	The LANIC card transmit buffer was not properly accessed by the Link Controller chip.
U = 1	A transmit data underflow into the Link Controller chip occurred causing faulty or incomplete transmission.
L = 1	On packet transmit, a collision occurred after the allowed slot time for normal collision detection (“Late Collision”).
LC = 1	The LANIC card lost the carrier signal of the transmit packet, that is, LAN medium voltage levels fell below prescribed limits.
R = 1	A collision was detected on each attempt to transmit the packet.
F = 1	Framing error. An integral number of bytes was not received.
O = 1	For the received packet, a data overflow into the Link Controller chip occurred.
CR = 1	For the received packet, a CRC error occurred.
BR = 1	Buffer error on the received data, or the received packet data did not match the transmit packet data.

EL Command Examples

The following examples illustrate command entry and response of the “Do External Loopback to MAU” command.

Example 1. Successful External Loopback Test

```
NM> EL<RETURN>
Do External Loopback on node              08-00-09-00-02-5A....  [ok]

NM>
```

In Example 1, an external loopback packet was transmitted from the node whose Station Address is 08-00-09-00-02-5A. Successful completion is indicated by the “[ok]” message.

Example 2. External Loopback Test Failure

```
NM> EL,08-00-09-00-02-5A<RETURN>
Do External Loopback on node              08-00-09-00-02-5A....  [failed]
ERROR:  DE009 REPORTING NODE ADR: 08000900025A SAP: F8
Ext. loopback failed

0  0  1  0  0  0  0  0  0  0  0  0  0  0  0  0
      NR D  B  H  M  BT U  L  LC R  F  O  CR BR

bit set to one      failure
--------------      -------
      NR            Not receive loopback pkt
      D             Deferred, can't loopback
      B             Transmit babble
      H             No Heartbeat from xceiver
      M             Card memory error
      BT            Buffer error on xmit
      U             Data underflow
      L             Late collision
      LC            Loss of carrier on xmit
      R             Retry failure on xmit
      F             Framing error on rcv
      O             Overflow on xmit
      CR            CRC error
      BR            Rcv Buf err/data mismatch

NM>
```

In Example 2, the EL command is sent to a local or remote node (Station Address 08-00-09-00-02-5A). Because the loopback test conducted by that node is not successful, a "`[failed]`" indication is returned along with an accompanying driver error message (DE009) and status word.

Using Table 5-9, the status word indicates that the loopback test packet was successfully transmitted by the LANIC card, but was not returned to the card. All cabling and connections from the LANIC card to the LAN coaxial cable, or a faulty Medium Attachment Unit (MAU) should be checked.

Note For successful external loopback testing, the MAU must be connected to the LAN coaxial cable.

Issue TEST Loopback Command (TEST)

This command allows the user to transmit an "IEEE 802.2/802.3 TEST command packet" that solicits an "IEEE 802.2/802.3 TEST response packet" from a program or process in the target node. It may be used as a loopback tool to help ensure communications integrity with a remote program or process over the LAN.

The syntax of this command is:

```
TEST,[ADR],DSAP[,[MSGLEN][,[LU#][,Rep]]]
```

where:

`ADR` This is the "target" Station Address of the node to which the TEST command packet is sent. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`DSAP` This is the Destination Service Access Point (DSAP) that specifies the program or process, on the ADR node, for which the IEEE 802.2 TEST command packet is directed, and from which an IEEE 802.2 TEST response packet is desired. This parameter is required and entered as a two-digit hexadecimal number.

`MSGLEN` This parameter defines the length, in bytes, of the Information field to be included in the IEEE 802.2 TEST command. When specified, it is a decimal number from 0 to 1497. The default is 0.

`LU#` This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. LU# is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

`Rep` This parameter specifies the number of consecutive times this command is executed. Values from 0 to 9999 may be specified. When set to "0", the command is repeated indefinitely unless a failure occurs or until the NM module break flag is set (see "The Rep Parameter" earlier in this chapter).

Recall from Chapter 2, an IEEE 802.2/802.3 TEST command packet issued from a sending node program contains a predefined value in its Control field (F3 hex with the P, or Poll, bit set). In addition, data may be contained in the Information field. The corresponding IEEE 802.2/802.3 TEST response packet returned by a responding node program contains the same Control field value (F3 hex with the F, or Final, bit set). Although not required, it is desirable for the responding node to return the same Information field data that was received.

When the Node Manager TEST command is issued, a valid IEEE 802.2/802.3 TEST command packet is constructed and transmitted. The user-specified DSAP parameter is inserted into the packet's DSAP field. The Information field will contain predefined data consisting of alternating zeroes ("0") and ones ("1"), the length of which is determined by the MSGLEN parameter (in bytes).

DSAP Considerations

The DSAP parameter identifies a program or process for which a packet is intended. If this command is sent to a program or process, that routine must be able to recognize the received TEST command packet, and return a TEST response packet.

The Node Manager software on each HP 1000 node utilizes SAP F8 hex, and is able to properly respond. Also, each LANIC card contains firmware that responds to the special Null SAP 00 (the driver and system software are not accessed).

If a DSAP is specified for which there is no program or process, the TEST packet is treated as an orphan packet (see Chapter 4).

Self-Addressed TEST Packets

When the ADR address (specified or defaulted) identifies the same LANIC card as the LU# parameter, the command is "self-addressed". For self-addressed TEST commands, a warning message is issued, and the command is executed as follows:

1. A self-addressed TEST command issued to DSAP=F8 hex is a software loopback. The Node Manager software from which the command was issued processes the command and issues a response; the packet is never sent to the LANIC card.

2. A self-addressed TEST command issued to any DSAP other than F8 is transmitted on the Link and transparently looped back by the card at the same time. If no process is waiting on this particular DSAP to receive this packet, it will be treated as an orphan packet.

Errors

Command entry errors resulting from TEST commands are the same as for other Node Manager commands. On the other hand, command execution errors (such as driver errors) resulting from the TEST command are not returned to the user; they are returned to system LU 1 (system console) of the node whose NMGR module experienced the error.

TEST Command Examples

The following examples illustrate the use of the TEST command.

Example 1. Defaulting All Parameters

```
NM> TEST<RETURN>
        ^1^2

error  1 ---> Address must be XX-XX-XX-XX-XX-XX, where X is a hex digit
error  2 ---> Missing parameter:  DSAP

NM>
```

Example 1 simply illustrates that a DSAP parameter is required.

Example 2. Incorrect MSGLEN Parameter

```
NM> TEST,08-00-09-00-02-5A,00,10000<RETURN>
                            ^1

error  1 ---> Msglen must be an integer in the range 0 to 1497 (bytes)

NM>
```

Example 2 illustrates the entry error resulting when `MSGLEN` is out of range.

Example 3. Successful Command With Repetition

```
NM> TEST,08-00-09-00-02-5A,F8,1000,,2<RETURN>
Perform Loopback Test through node 08-00-09-00-02-5A....  [ok]

Perform Loopback Test through node 08-00-09-00-02-5A....  [ok]

NM>
```

In Example 3, the command was sent to a remote node (Station Address 08-00-09-00-02-5A). The TEST command packet was delivered to the Node Manager software (identified by SAP F8). The `Rep` parameter was specified as "2"; thus the command was issued and successfully completed twice, as indicated by the returned message.

Example 4. Self-Addressed TEST Commands

```
NM> TEST,,F8<RETURN>
Warning: No response is returned from self-addressed packets (except DSAP F8)
Perform Loopback Test through node 08-00-09-00-02-30....  [ok]

NM> TEST,,00<RETURN>
Warning: No response is returned from self-addressed packets (except DSAP F8)
Perform Loopback Test through node 08-00-09-00-02-30....  [failed]
---> times out - no response from target node

NM>
```

In Example 4, self-addressed TEST commands are sent to the Node Manager SAP, F8, and to the LANIC card Null SAP, 00. In the first case, a software loopback occurs; the local Node Manager reports back to itself that the test completed successfully. In the second case, the packet is treated as an orphan packet; thus, there is no program to generate a TEST response packet and the originating command times out.

XID Command (XID)

This command allows the user to transmit an "IEEE 802.2/802.3 XID command packet" that solicits an "IEEE 802.2/802.3 XID response packet" from a program or process in the target node. It may be used as a loopback tool to help communication integrity with a remote program or process over the LAN.

The syntax of this command is:

```
XID,[ADR],DSAP[,[LU#][,Rep]]
```

where:

`ADR` This is the "target" Station Address of the node to which the XID command packet is sent. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`DSAP` This is the Destination Service Access Point (DSAP) that specifies the program or process (on the ADR node) for which the IEEE 802.2 XID command packet is directed and from which the XID response packet is desired. This parameter is required and entered as a two-digit hexadecimal number.

`LU#` This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. LU# is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

`Rep` This parameter specifies the number of consecutive times this command is executed. Values from 0 to 9999 may be specified. When set to "0", the command is repeated indefinitely unless a failure occurs or until the NM module break flag is set (see "The Rep Parameter" discussed earlier in this chapter).

Recall from Chapter 2, an IEEE 802.2/802.3 XID command packet issued from a program contains a predefined value in its Control field (BF hex with the P, or Poll, bit set). In addition, the Information field contains data that identifies the type of service (Type 1 and/or Type 2) the station provides.

The corresponding IEEE 802.2/802.3 XID response packet returned by a responding program contains the same Control field value (BF hex with the F, or Final, bit set), and an Information field that identifies the type of service supplied by the responding station.

When the Node Manager XID command is issued, a valid IEEE 802.2/802.3 XID command packet is constructed and transmitted. The user-specified DSAP parameter is inserted into the packet's DSAP field. The SSAP field contains F8 hex which identifies the Node Manager software's SAP while also identifying the packet as a command packet (C/R bit not set). The Control field contains BF hex. The Information field contains three bytes of data: 81, 01, and 00 hex, indicating Type 1 service (unacknowledged, connectionless).

The response to the XID command is checked by Node Manager to ensure the same Control field is returned (BF hex). The Information field is checked for the type of service (see Chapter 2 for bit definitions in the XID packet Information field).

If the Node Manager software receives an XID command, it constructs a similar packet. The Source Address and SSAP fields of the command are used to determine the destination of the

response. The response packet's SSAP field contains F9 to identify the Node Manager SAP and to indicate the packet is a response (F8 hex plus the C/R bit is set). The response Control field will contain the same value as the command, and the response Information field will contain: 81, 01, and 00 hex.

DSAP Considerations

The DSAP parameter identifies a program or process for which a packet is intended. If this command is sent to a program or process, that routine must be able to recognize the received XID command packet, and return an XID response packet.

The Node Manager software on each HP 1000 node utilizes SAP F8 hex, and is able to properly respond. Also, each LANIC card contains firmware that responds to the special Null SAP 00 (the driver and system software are not accessed).

If a DSAP is specified for which there is no program or process, the XID packet is treated as an orphan packet (for information on orphan packets, see Chapter 4).

Self-Addressed XID Packets

When the ADR address (specified or defaulted) identifies the same LANIC card as the LU# parameter, the command is "self-addressed". For self-addressed XID commands, a warning message is issued and the command is executed as follows:

1. A self-addressed XID command issued to DSAP=F8 hex is a software loopback. The Node Manager software from which the command was issued processes the command and issues a response; the packet is never sent to the LANIC card.

2. A self-addressed XID command issued to any DSAP other than F8 is transmitted on the Link and transparently looped back by the card at the same time. If no process is waiting on this particular DSAP to receive this packet, it will be treated as an orphan packet.

Errors

Command entry errors resulting from XID commands are the same as for other Node Manager commands. On the other hand, command execution errors (such as driver errors) resulting from the XID command are not returned to the user; they are returned to system LU 1 (system console) of the node whose NMGR module experienced the error.

XID Command Examples

The following examples illustrate use of the XID command.

Example 1. Successful XID Response

```
NM> XID,08-00-09-00-02-5A,00<RETURN>
Perform Loopback Test thru node 08-00-09-00-02-5A....  [ok]
802.2 Basic Format, Class 1 Station : connectionless

NM>
```

In Example 1, an XID command is transmitted to a remote node (Station Address 08-00-09-00-02-5A). Because DSAP is "00" hex, the packet was directed to the LANIC card at that node; the remote system was not accessed. A proper response was received as verified by the "[ok]" indication and the message describing the type of service provided by the card.

Example 2. No XID Response

```
NM> XID,08-00-09-00-02-5A,F8<RETURN>
Perform Loopback Test thru node 08-00-09-00-02-5A....  [failed]
-- > times out - no response from target node

NM>
```

In Example 2, an XID command is transmitted to the same node as Example 1, but the DSAP parameter F8 hex is specified. In this case, Node Manager is not running on the target node, and there is no response.

Event Log Commands

Using the “Create Link File Directories” (CD) command, a Link File directory can be created for each LANIC card installed. Once created, a card’s Link File directory contains a MCAST.TXT file and an EL.TXT file. The Link File directory, MCAST.TXT file, and EL.TXT file are contained in a root directory, FILES802, of a disk-based File Server Node (see Chapter 4).

The MCAST.TXT file is used for storing Multicast Addresses to be configured on the applicable card (see Chapter 4).

The EL.TXT (or event log) file is used for logging of certain events. When a card is properly configured, its EL.TXT file is accessed by Node Manager software to record occurrences of “bad”, “orphan”, or “trace” packets received, that is,

- packets with a Cyclic Redundancy Check or Length errors (bad);
- packets that cannot be routed to an intended program or process due to an invalid or nonexistent class number posted to the packet’s DSAP (orphan);
- packets resulting from self-addressed TEST and XID commands that specify a DSAP of “00” (treated as orphans); and
- packets unsuccessfully transmitted and returned to the driver (trace).

The complete path to the EL.TXT file is as follows:

```
/FILES802/ADDRxxxxxxxxxxxx/EL.TXT
```

where `xxxxxxxxxxxx` are hexadecimal digits of the associated card’s Station Address.

There is only one Event Log command. The Read Event Log File (RE) command is used for reading the EL.TXT file.

Read Event Log File Command (RE)

As the name implies, the Read Event Log File (RE) command displays the latest 256 entries in the Event Log file associated with a particular LANIC card.

Note An event log file associated with a local or remote node may only be read locally, that is, from the disk-based File Server Node on which it resides. Reading an event log file over the LAN is not allowed, and no transmission over the LAN occurs when using this command.

The syntax for this command is:

```
RE[,FileAddress]
```

where,

`FileAddress` This parameter is the Station Address of the node whose event log file is to be read. It is entered as 6 pairs of hexadecimal digits separated by hyphens. If defaulted, the address used is the Station Address of the LANIC card with the lowest LU value installed.

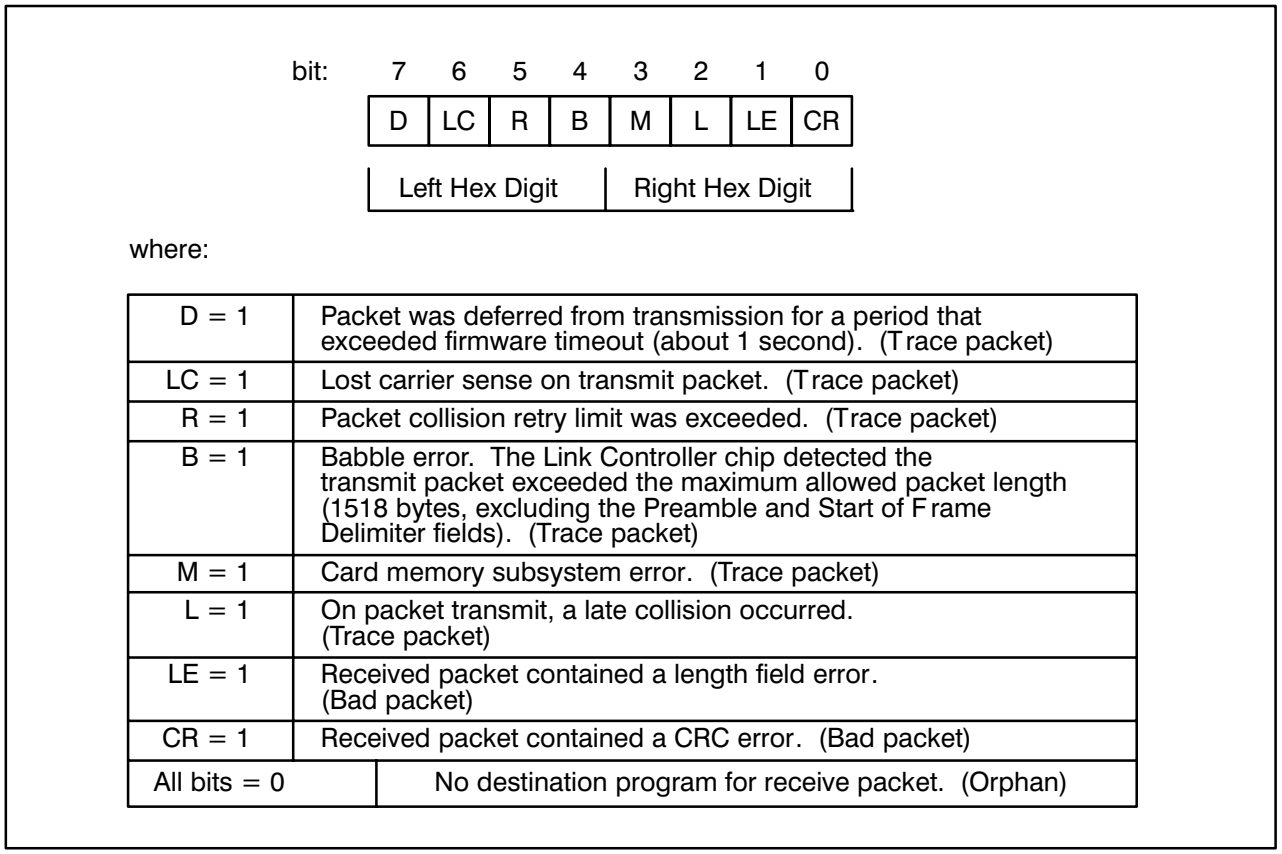
When this command is entered, Node Manager software retrieves the applicable file and displays it in the following form:

TIME	DATE	ERR#	LU	DA	SA	LEN	DSAP	SSAP	CTRL

where,

`Time` : indicates the time of the entry, AM and PM.
`Date` : indicates the day, month, and year of the entry.
`ERR#` : Two hexadecimal digits representing a packet error status byte. (See Figure 5-1.)
`LU` : The Logical Unit number (decimal) of the LANIC card through which the logged packet was received.
`DA` : The Destination Address of the logged packet, 12 hexadecimal digits.
`SA` : The Source Address of the logged packet, 12 hexadecimal digits.
`LEN` : The length of the packet in bytes, specified as 4 hexadecimal digits.
`DSAP` : The DSAP of the logged packet, 2 hexadecimal digits.
`SSAP` : The SSAP of the logged packet, 2 hexadecimal digits.
`CTRL` : The logged packet's Control field value, 2 hexadecimal digits. (See Table 5-10.)

The ERR# value may be decoded to binary, and with Figure 5-1, the cause of packet error may be deciphered.



where:

D = 1	Packet was deferred from transmission for a period that exceeded firmware timeout (about 1 second). (Trace packet)
LC = 1	Lost carrier sense on transmit packet. (Trace packet)
R = 1	Packet collision retry limit was exceeded. (Trace packet)
B = 1	Babble error. The Link Controller chip detected the transmit packet exceeded the maximum allowed packet length (1518 bytes, excluding the Preamble and Start of Frame Delimiter fields). (Trace packet)
M = 1	Card memory subsystem error. (Trace packet)
L = 1	On packet transmit, a late collision occurred. (Trace packet)
LE = 1	Received packet contained a length field error. (Bad packet)
CR = 1	Received packet contained a CRC error. (Bad packet)
All bits = 0	No destination program for receive packet. (Orphan)

Figure 5-1. Deciphering the Packet Error Byte, ERR#

In accordance with the IEEE 802.2 Standard, common CTRL parameter values are shown in Table 5-10 (see Chapter 2 for a review of a packet's Control field).

Table 5-10. IEEE 802.2 Control Field Designations

CTRL Parameter*	Information Field Description
03 or 13 hex	Unnumbered Information
AF or BF hex	XID Loopback Packet Data
E3 or F3 hex	TEST Loopback Packet Data
*Note: Two values, depending on the P/F bit of the control Field (see Chapter 2).	

List Facility

The returned information from an RE command may exceed a single terminal screen display. If the event log file is large, it may be viewed using a "list facility" very similar to the standard RTE-A list facility. Pressing any key other than <A> or <RETURN> will display another full screen. Pressing <A> will abort.

If the <RETURN> key is pressed, the listing will scroll continuously until the last entry is displayed. To interrupt continuous scrolling, any key can be pressed; this runs the Command Monitor program (CM> prompt).

From CM>, hitting <RETURN> or typing br<RETURN> will continue the scrolling.

To exit from continuous scrolling, set the NM2 break flag from CM> by entering

```
CM> br,NM2<RETURN>
```

which will return to a single terminal screen display mode and allow for aborting the listing.

RE Command Examples

The following examples illustrate the use of the Read Event Log File command.

Example 1. Empty Event Log File

```
NM> RE,08-00-09-00-02-00<RETURN>
Event Log File is empty.

NM>
```

Example 1 illustrates the message returned when attempting to read an empty event log file.

Note In Examples 2, 3, and 4 below note that the driver and LANIC card must be configured to save orphan and bad packets, and the trace mode must be enabled.

Example 2. Orphan Packet Event Log File Entries

```
NM> RE,08-00-09-00-02-5A<RETURN>
   TIME        DATE      ERR#   LU      DA             SA       LEN DSAP SSAP CTRL

10:35 AM  13  OCT.  85  00    82  08000900025A  080009000230  0006  90  F8  BF
10:36 AM  13  OCT.  85  00    82  08000900025A  080009000230  0003  BC  F8  F3
    .          .         .     .       .              .          .    .   .   .
    .          .         .     .       .              .          .    .   .   .
    .          .         .     .       .              .          .    .   .   .

More...('a' to abort)
```

In Example 2, two records from the event log file associated with the node (Station Address 08-00-09-00-02-5A) are shown. The program sending each packet was presumably Node Manager software (SSAP = F8) from node 08-00-09-00-02-30.

The first packet was an XID test packet (CTRL = BF) containing 6 bytes in the Protocol Data Unit. Since it contained a DSAP (90) that could not be associated with a receiving program, it was logged as an orphan packet (ERR# = 00).

The second packet was a TEST packet (CTRL = F3) containing 3 bytes in the Protocol Data Unit. Since its DSAP (BC) was also not linked to a program, the packet was logged as an orphan.

This example illustrates two received packets logged to the event log file of the destination node (LU = 82).

Example 3. Bad Packet Entry in Event Log File

```
NM> RE,08-00-09-00-02-5A<RETURN>
   TIME        DATE      ERR#   LU      DA             SA       LEN DSAP SSAP CTRL

12:15 PM  15  OCT.  85  02    82  08000900025A  080009000230  05AA  A8  A4  03
    .          .         .     .       .             .          .    .   .   .
    .          .         .     .       .             .          .    .   .   .
    .          .         .     .       .             .          .    .   .   .

More...('a' to abort)
```

In Example 3, an Unnumbered Information packet (CTRL = 03) sent from Station Address 08-00-09-00-02-30 to Station Address 08-00-09-00-02-5A was logged. The packet was sent from a program whose SAP is A4 hex, to a program whose SAP is A8 hex (SSAP and DSAP are A4 and A8, respectively). This packet was logged with a packet length error (02 hex), presumably due to a mismatch between the length field (05AA bytes) and the actual packet length.

This example illustrates a received packet logged to the event log file of the destination node (LU = 82).

Example 4. Trace Packet Entry in Event Log File

```
NM> RE,08-00-09-00-02-30<RETURN>
   TIME        DATE      ERR#   LU      DA             SA       LEN DSAP SSAP CTRL

12:15 PM  15  OCT.  85  20    62  08000900025A  080009000230  00BA  0C  A4  03
    .          .         .     .       .             .          .    .   .   .
    .          .         .     .       .             .          .    .   .   .
    .          .         .     .       .             .          .    .   .   .

More...('a' to abort)
```

In Example 4, an entry shows that an Unnumbered Information packet (CTRL = 03) was transmitted from a program with SAP A4 on node 08-00-09-00-02-30, to a program with SAP 0C on node 08-00-09-00-02-30. The packet was logged because the transmit packet retry limit was exceeded due to collisions (ERR# = 20). (This example was generated by removing the 50-ohm terminators on the LAN cable.)

This example illustrates a transmit trace packet logged to the event log file of the source node (LU = 62).

Statistics Commands

Each LANIC card contains counters for accumulating various statistics of individual card events. In addition, Node Manager software contains a counter for the occurrence of orphan packets received on the system. These "statistics" may be read or cleared from both local or remote nodes. They are summarized in Table 5-11.

Note The LANIC Self-Test Command, `TC`, will also clear statistics counters maintained by the LANIC card. It will not clear the statistic counter maintained by the Node Manager software.

The maximum value of each statistics counter is shown in Table 5-11. When a counter's maximum value is reached, that value is maintained until cleared; it does not automatically roll-over to zero.

The statistics gathered can provide insight into the efficient operation of the node or network. However, interpretation of the statistics provided is not often trivial. Different conclusions may be deduced from different combinations of statistics.

The ability to interpret the statistics will improve with experience.

There are two Statistics Commands; they are discussed in the pages that follow:

- Read Link Statistics Counters, RS
- Zero Link Statistics Counters, ZS

Table 5-11. Statistics Information Summary

Item #	Description	Maintained By	Maximum Value	Cleared By
1	Number of good bytes transmitted	LANIC card	4294967295	ZS & TC
2	Number of good bytes received	LANIC card	4294967295	ZS & TC
3	Number of good packets transmitted	LANIC card	4294967295	ZS & TC
4	Number of good packets received	LANIC card	4294967295	ZS & TC
5	Number of errors on transmit	LANIC card	65535	ZS & TC
6	Number of errors on receive	LANIC card	65535	ZS & TC
7	Number of babble errors	LANIC card	65535	ZS & TC
8	Number of heartbeat errors on transmit	LANIC card	65535	ZS & TC
9	Number of missed packets due to no receive buffer available	LANIC card	65535	ZS & TC
10	Number of card memory errors	LANIC card	65535	ZS & TC
11	Number of framing errors	LANIC card	65535	ZS & TC
12	Number of packets discarded by the driver	LANIC card	65535	ZS & TC
13	Number of CRC errors on receive	LANIC card	65535	ZS & TC
14	Number of packets with 802.3 length field errors	LANIC card	65535	ZS & TC
15	Number of times more than one retry was needed on transmit	LANIC card	65535	ZS & TC
16	Number of times one retry was needed on transmit	LANIC card	65535	ZS & TC
17	Number of times the Link Controller chip deferred on transmit	LANIC card	65535	ZS & TC
18	Number of transmit data underflow errors into Link Controller chip	LANIC card	65535	ZS & TC
19	Number of late collisions	LANIC card	65535	ZS & TC
20	Number of times carrier was lost	LANIC card	65535	ZS & TC
21	Number of times the transmit retry count was exceeded	LANIC card	65535	ZS & TC
22	TIme Domain Reflectometry (TDR) info, valid if item 21 is not “0”	LANIC card	65535	ZS & TC
23	Number of orphan packets received on the system (all cards)	Node Manager Software	65535	ZS

Statistics Description

Item #1, Good Bytes Transmitted. The firmware counts the number of good bytes transmitted by the card onto the link. In a given packet, applicable bytes subject to counting include the Destination Address field through the Pad field (Preamble, Start of Frame Delimiter, and CRC fields are not counted).

Item #2, Good Bytes Received. The firmware counts the number of bytes received and accepted from the link, that is, subsequent to passing the Address Filter mode set. Applicable bytes subject to counting are from a packet's Destination Address field through the Pad field; also, the packet must not contain any errors.

(Note: This counter is not incremented for self-addressed loopback packets.)

Item #3, Good Packets Transmitted. The firmware counts the number of successful packet transmissions by the card onto the link for which there were no errors. This value is related to Item #1 above.

Item #4, Good Packets Received. The firmware counts the number of packets that are received and pass the Address Filter mode configured on the card. The packet must not contain any errors. This value is related to Item #2 above.

(Note: This counter is not incremented for self-addressed loopback packets.)

Item #5, Errors on Transmit. This statistic is incremented for each packet that experiences at least one error during transmission. Although a single packet may experience several transmission errors, this statistic would be incremented only by one.

(Note: for MAUs that do not return a heartbeat signal, this statistic will be incremented on every transmission. See Item #8 below.)

Item #6, Errors on Receive. This statistic reflects the total number of packets received that pass the Address Filter mode set on the card, but contain one or more receive errors.

Item #7, Babble Errors. This statistic is incremented by the firmware whenever the Link Controller chip detects a transmit packet that exceeds the allowed packet length (greater than 1518 bytes, not counting the Preamble and Start of Frame Delimiter fields).

Item #8, Heartbeat Errors. Typically, IEEE 802.3 MAUs will return a short signal (heartbeat) to the LANIC card after each transmission to indicate proper operation of collision detect circuitry. This counter is incremented on each transmission that does not return a heartbeat.

Item #9, Missed Packets Due to No Receive Buffers. Before Packet Filter mode processing, this counter is incremented when there is no receive buffer space available in RAM to place the packet, hence the packet is lost.

Item #10, Card Memory Errors. During packet transmission or reception, card RAM must be accessed. The firmware increments this counter when an error occurs during access of the card memory system.

Item #11, Framing Errors. This statistic reflects the number of packets received that do not contain an integral number of bytes, which invalidates the packet.

Item #12, Packets Discarded by the Driver. This statistic is incremented whenever the driver requests that a packet be discarded. This occurs on orphan packets when the node is configured for discarding orphans. In addition, the driver may cause packet discard of good packets if system or other resources are not available (for example, insufficient SAM).

Item #13, CRC Errors. This statistic is incremented on received packets that pass the Packet Filter mode configured, but contain a Cyclic Redundancy Check error.

Item #14, IEEE 802.3 Length Field Errors. When a received packet contains a Length field value that does not match the actual Protocol Data Unit field length (in accordance with the IEEE 802.3 standard), the firmware increments this statistic.

(Note: Although this statistic normally applies to packets received off the link, it will increment on self-addressed loopback packets containing Length field errors.)

Item #15, More Than One Retry Needed. This counter is incremented whenever more than one retry is required for successful transmission, that is, three or more transmission attempts (the first "retry" is the second attempt).

Item #16, Exactly One Retry Needed. This counter is incremented whenever exactly one retry is needed for successful transmission, that is, two transmission attempts.

Item #17, Transmit Deferrals. When the LAN is in use, the local LANIC card must defer from transmission until the LAN is available. This statistic is the number of packets that experienced at least one deferral prior to transmission. Multiple deferrals of a single packet increments this counter only by one.

Item #18, Transmit Data Underflow Errors. For transmit packets, an error may occur where the Link Controller chip may expect more data than is available. This results in a data underflow to the chip and the counter is incremented.

Item #19, Late Collisions. Normal collisions on transmit result in the LANIC card backing off a random period and retrying transmission. Late collisions are abnormal; they occur subsequent to the period in which a normal collision would be detected ("slot time"). When a late collision occurs during a transmission, a counter is incremented. However, the packet is not retransmitted.

Item #20, Carrier Lost. This statistic reflects the number of packets for which the voltage level of the LAN medium fell below prescribed limits at least one or more times during transmission.

Item #21, Transmit Retry Count Exceeded. A retry limit for transmitting packets may be set at "1" or "15" (two or 16 total transmission attempts, respectively). On repeated collisions, if a packet has not successfully transmitted after the number of retries configured, this statistic is incremented.

Item #22, TDR Information. A Time Domain Reflectometer is a tool for locating discontinuities on the LAN medium by essentially converting the time between a transmitted and reflected pulse to a distance on the medium.

The TDR Information statistic employs the 10 MHz clock on the card to indicate the time (in 100 nanosecond increments) between packet transmission and collision detection. It is provided only when Item #21 (Transmit Retry Count Exceeded) is incremented.

Caution *USE OF THIS STATISTIC AS A TDR TOOL IS NOT RECOMMENDED*. The TDR statistic is provided by the Link Controller chip and is returned to the user for information only. Significant errors are introduced from several factors:

- Clock speeds (100 ns increments) are too large relative to transmission speeds on the LAN medium.
- Overhead is incurred by the MAU during packet transmission and reception. Several hundred nanoseconds may be consumed.
- Allowances for transmission ratings of various AUI and LAN cabling must be made.

Item #23, Orphan Packets Received on the System. Node Manager software maintains a counter for orphan packets received on the system. With multiple LANIC cards installed, this counter reflects the total number of orphan packets received through all cards. It may be read or purged through Node Manager statistics commands that specify any installed LANIC card LU.

For this statistic to be incremented, the individual cards must be configured to save orphans, and Node Manager software must receive them.

Read Link Statistics Counters Command (RS)

This command allows the user to locally or remotely read the available statistics maintained by a specified node.

The syntax of the command is:

```
RS[,[ADR][,LU#]]
```

where,

`ADR` This is the "target" Station Address, that is, the node from which the statistics are to be read. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

`LU#` This is the Logical Unit number of the LANIC card through which the command is transmitted and from which a response is received. It is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

If the command successfully executes, the various statistics accumulated for items listed in Table 5-11 are returned to the user.

RS Command Example

The following example illustrates use of the Read Statistics command:

Example 1. Typical Response to the RS Command

```
NM> RS,08-00-09-00-02-00<RETURN>
Read Statistics counters of node  08-00-09-00-02-00....  [ok]

 1. Num of good bytes xmited          77200
 2. Num of good bytes rcved             400
 3. Num of good pkts xmited             386
 4. Num of good pkts rcved                2
 5. Num of errors on xmit                 0
 6. Num of errors on rcv                  0
 7. Num of babble errors                  0
 8. Num of heartbeat errors (xmit)        0
 9. Num of missed pkts--no rcv buf        0
10. Num of memory errors                  0
11. Num of framing errors                 0
12. Num of pkts driver discarded          0
13. Num of CRC errors on rcv              0
14. 802.3 Length field errors             0
15. Num of retry > 1 on xmit              0
16. Num of retry = 1 on xmit              0
17. Num of chip deferred on xmit          0
18. Num of underflow error on xmit        0
19. Num of late collisions                0
20. Num of loss of carrier                0
21. Num of xmit retry cnt exceeded        0
22. TDR info from last TDR                0
23. Orphan messages received by NM        0

NM>
```

Example 1 shows successful execution of this command, as confirmed by the "[ok]" message returned. In addition, the statistics maintained by the card and Node Manager are listed along with their current counter contents.

Zero Link Statistics Counters Command (ZS)

This command allows the user to set all statistics counters to zero.

The syntax of this command is:

```
ZS[,[ADR][,LU#]]
```

where,

ADR — This is the "target" Station Address of the node whose statistics counters will be set to zero. It is entered as 6 pairs of hexadecimal digits separated by hyphens. See Table 5-1 for default addresses.

LU# — This is the Logical Unit number that identifies the LANIC card through which a command is transmitted and from which a response is received. LU# is a number in the range 2 to 255 (decimal) established during system generation; hence, it always applies to a local LANIC card. See Table 5-1 for default values.

ZS Command Example

The following example illustrates the use of the ZS command.

Example 1. Typical ZS Command and Response

```
NM> ZS,08-00-09-00-02-5A<RETURN>
Zero Statistics counters of node        08-00-09-00-02-5A....  [ok]

NM>
```

Example 1 shows the successful completion of the command through the "[ok]" indication.

6

LANVCP Operations

This chapter explains the software and procedures for downloading a memory-based system to another computer and for using the remote VCP over a LAN. This software and procedures may also collectively be referred to as LANVCP.

Memory-Based System, LAN, and VCP

A memory-based system is a system executing entirely in memory without a disk. The memory-based system is downloaded over an IEEE 802.3 LAN (downloading over an Ethernet LAN is not supported) to a remote system. This is done from the remote system, either interactively or automatically on power-up. The remote boot process is not supported over gateways. A gateway node is one that belongs to two separate networks. Therefore, you cannot remotely boot a system in another network.

When describing a memory-based system over a LAN, the *server* refers to the system in control, usually the local node that is running the download monitor program, VCPMT (described later). The *client* refers to the memory-based system that is being downloaded to or controlled. A single server can serve up to 28 downloads simultaneously per LAN interface card.

Downloading and controlling a memory-based system is done by running the LAN-based remote VCP (Virtual Control Panel) program called RMVCP. All the systems must be on the same LAN. By running RMVCP, you can obtain the VCP prompt at your terminal as if you were directly connected to the remote system where VCP is executing. From your node, you can run VCP commands remotely.

There is a remote VCP feature in the DS/1000-IV and NS-ARPA/1000 products called DSVCP. DSVCP works only over HDLC links. This feature is documented in the DS/1000-IV and NS-ARPA/1000 manuals.

Hardware and Software Requirements

The following hardware and software are required to create memory-based nodes on a LAN. Refer to the *HP 12076A LAN/1000 Link Local Area Network Interface Controller Installation Manual*, part number 12076-90001, for information on configuring the LAN card. For information on using the LAN Node Manager software, refer to the other chapters in this manual (*HP 12076A LAN/1000 Link Node Manager's Manual*, part number 12076-90002).

- **LAN cards** – Every HP 1000 A-Series system that is going to be remotely booted must have a LAN card and must be on the same LAN as the server. The remote boot process is not supported over gateways.

  For remote VCP operation, the LAN card on the client must have the VCP enabled (U1S1 [switch 1] in the closed position). Note that only one interface card per system can have the VCP enabled.

- **Automatic boot-up** – For automatic bootup at power on, the select code of the LAN card on the client machine must be set to 24 and the CPU switches on the remote computer must be set for autoboot. Refer to the installation and service manual for your computer for CPU switch information.

  Upon power-up, the client sends out a broadcast message to the LAN to be booted up. However, you could also configure a particular or a multicast download server station address onto the client's LAN card. The client would then be serviced by a particular server or group of servers on the LAN. This configuration can be set by running the LAN Node Manager program, NM, when the client's card is in the backplane of a disk-based system. See Chapter 5 for more information on using the Node Manager software.

- **Required server software** – The following modules are documented in this chapter:

  IPL_BUILD and IPL_EDIT create the configuration file containing each client's LAN station address and memory-based system download file. IPL_BUILD creates the configuration file, and IPL_EDIT is used to alter it.

  DISPATCH monitors the LAN packets and determines whether the packet is to be handled by the remote VCP monitor or the LAN Node Manager.

  VCPMT and RMVCP download the operating system to the memory-based node and handle the remote VCP session. VCPMT is the monitor and RMVCP is the user interface to VCPMT.

IPL_BUILD and IPL_EDIT – Configuration Files

A configuration file is needed to specify the memory-based system download file name and its client. More than one system and/or client can be specified. You create the configuration file with IPL_BUILD and modify it using IPL_EDIT. The names of these programs were derived from the term, IPL, Initial Program Load.

The default configuration file is /FILES802/IPL_TABLE.TXT.

You can also use EDIT/1000 to modify the configuration file once it has been created using IPL_BUILD. The configuration file is a type 4 file. Make sure that you do not accidentally truncate the records as you edit. Otherwise, the entry in the configuration file becomes corrupt.

The configuration file is used by the VCPMT monitor and RMVCP, the remote VCP program, to determine which system to download and its destination.

IPL_BUILD and IPL_EDIT prompt you for the following entries. Enter the required information in between the square brackets ([]), left justified.

IPL table file name	The name of the configuration file. The default file is /FILES802/IPL_TABLE.TXT. A different file can be used for another server system, but VCPMT always looks for /FILES802/IPL_TABLE.TXT.
Node name	The name of the client node. Up to 17 characters can be specified.

This name is used in the runstring for RMVCP, the remote VCP program described later in this chapter. This node name is not defined or recognized as an NS, DS, or ARPA node name. Although the node names may be the same when using any of these networking products, each product specifies and creates them differently.

Node number

(Optional) An integer number of the client node. Up to 5 characters can be specified.

If the node number is not specified, the node number is zero. This number is used interchangeably with the node name in the runstring for RMVCP, the remote VCP program, described later in this chapter.

The node name and node number are used as search keys for RMVCP during an interactive boot up. The first entry that matches in the configuration file (/FILES802/IPL_TABLE.TXT) determines the client.

LAN address

LAN station address of the client node in hexadecimal. Up to 12 characters can be specified.

Download file

The file name of the memory-based system to be downloaded to the remote system (the client). Up to 64 characters can be specified for the file name.

The file can be a FMGR or CI file. This file is created by BUILD, which is documented in the *RTE-A System Generation and Installation Manual*, part number 92077-90034 (in Chapter 10, subsection "Run BUILD to Create the Merged System File," and in Appendix I). Specify the full path name of the system file. If the path name is not specified, RMVCP searches for the file in directory /FILES802.

When a download request comes in from the client, the download file can be accessed in one of two different ways:

a. P00000 file specified at autoboot or in the VCP runstring (%BDS00000sc). VCPMT searches for the default download file specified in /FILES802/IPL_TABLE.TXT. The default download file has the default flag set to 1. If there are no entries for the client with the default flag set, then the last entry for the client is used to obtain the download file name. The download file name can be any legitimate file name.

b. P*fffff* file specified in the VCP runstring. When P*fffff* is specified in the VCP runstring (for example, %BDS7777700sc), VCPMT first searches the directory /FILES802 for the actual P*fffff* file, then performs a search of each FMGR cartridge.

Default flag

(Optional) 1 means that this record in the configuration file is the default system to be downloaded in the case of a non-interactive download session (for example, autoboot).

	If not 1 (0, A, ...), use this record only if none with a “1” is available for this LAN address. The LAN station address is the search key for incoming requests to boot up. If more than one client node specified in /FILES/IPL_TABLE.TXT has the same LAN address, the last one specified with a default flag set is used as the default client. If the client nodes with the same LAN address do not have the default flag set, the last entry is used as the default client.
LU	The transmit LU of the LAN card on the server through which the server communicates with the client. Up to 3 characters can be specified.
continue ?	You can continue adding information for another node. Enter `y` for yes or `n` for no.

When modifying a configuration file using IPL_EDIT, each entry is displayed. Either type over it entirely to change it or type carriage return for no change.

Examples

IPL_BUILD creates the configuration file. Enter parameters in between the brackets, []. User input is underlined:

```
CI> ipl_build

Enter ipl table file name : <cr>

With /files802/ipl_table.txt enter
Name     [memory-node    ]
Number   [900       ]
Address  [08000900524d]

Download
    file [/MBSYS/SYSTEM/download-file]
default flag  [<cr>]
      LU [132]
 continue ? n
```

IPL_EDIT edits the configuration file. Parameters are displayed in between the brackets, []. Type over each entry to be modified; hit carriage return to not change an entry:

```
CI> ipl_edit
Enter ipl table file name : <cr>

With /files802/ipl_table.txt enter

name  [memory-node     ]
name  [memory-based    ]
name  [<cr>]
no.   [       900]
no.   [<cr>]
address [08000900524d]
address [<cr>]
download file [/MBSYS/SYSTEM/download-file]
download file [<cr>]
default flag  [1]
default flag  [<cr>]
      lu [132]
      lu [<cr>]
 continue ? y
name  [next-node]
name  [<cr>]
no.   [1000]
no.   [<cr>]
address [08000900524d]
address [<cr>]
download file [download2file]
download file [<cr>]
default flag  [0]
default flag  [<cr>]
      lu [132]
      lu [134]
      lu [<cr>]
 continue ? n
```

Format of IPL_TABLE.TXT

IPL_TABLE.TXT is a type 4 file. You can also use EDIT/1000 to modify the configuration file once it has been created using IPL_BUILD. Make sure that you do not accidentally truncate the records as you edit. Otherwise, the entry in the configuration file becomes corrupt.

The format of IPL_TABLE.TXT is as follows. Each entry is a total of 110 characters. The length of each field is also shown below. The 'X' is a one-character "don't care" character. Each line is terminated by a semicolon as the end delimiter.

```
<name    >X<number >X<hex address >XX<file name >XX<default>X<LAN LU >;
<17 chars>X<5 chars>X<12 chars    >XX<64 chars  >XX<1 char >X<3 chars>;
```

Selecting the System File to Download

When a download is initiated (whether it is initiated interactively, from the client's VCP console, or upon autoboot), VCP on the client system sends a request out on the LAN for a particular file number. This file number is the file number that is specified in the bootstring. For the LAN card, the bootstring is of the form:

```
%bds ff 00 sc
```

where *ff* is the file number and *sc* is the select code.

If *ff* is non-zero, the "00" in the bootstring is necessary as a placeholder. If *ff* is not specified, *ff* defaults to 0 (and the "00" placeholder is not necessary, giving a bootstring of %bdssc). Also, *ff* defaults to 0 in the case of autoboot.

If the file number is 0, VCPMT running on the server (who receives the request to download file number 0) performs a translation of file number 0. First, VCPMT checks to see if an interactive session has been started with RMVCP on the server system. If an interactive session has been started, VCPMT uses the client name (or number) given in the RMVCP runstring, to perform a search of the configuration file (/FILES802/IPL_TABLE.TXT). The system file in the configuration file associated with the given client name will be the system file that gets downloaded.

If VCPMT receives a request to download file number 0 and an interactive session has **not** been started (that is, the client has just initiated an autoboot), VCPMT will search the configuration file for the system file that has the default flag set. If more than one system file has the default flag set, the last entry with the default flag set will be the one that is downloaded. If no entries have the default flag set, the last entry in the configuration file will be the one that is downloaded.

If the file number is not 0, VCPMT translates the file number to form the file name P*fffff*. For example, the bootstring %bds70024, would initiate a download of system file P00007 from the server (client LAN select code 24). When the file number is non-zero and a P*fffff* file name is to be downloaded, VCPMT does not search the configuration file. VCPMT first searches the /FILES802 directory, then searches each FMGR cartridge on the server system until it finds the correct P*fffff* file to download.

DISPATCH – Monitoring LAN Packets

DISPATCH is the dispatcher module. It monitors the link to the A-Series and ensures that all LAN packets arriving on service access point F8 (hex) are routed correctly to either the LAN Node Manager (NM) or RMVCP for that LAN card. DISPATCH is only required if Node Manager services are needed from other nodes to this node. DISPATCH decreases the download speed by 5%.

The following command schedules the dispatcher program which can be run in the WELCOME file.

Syntax:

```
XQ,DISPATCH,lu
```

Parameters:

lu Specifies the LU number of the LAN LU to the client. DISPATCH verifies that the LAN LU is functioning at that LU number. If not, it returns, an error. Refer to Appendix A for a list of LANVCP error codes.

One copy of DISPATCH is needed for each LAN LU. For example,

```
XQ,DISPATCH,96
XQ,DISPATCH,98
```

Note It does not matter if the NM program is already scheduled on the same LAN LU when the dispatcher is scheduled.

VCPMT Monitor

VCPMT is the monitor that handles the remote VCP interactive user session and sends download records to a requesting client. A VCPMT program is required for each LAN on which the machine is the server.

The following command schedules VCPMT which can be run in the WELCOME file.

Syntax:

XQ,VCPMT,*lu*[,*lu*, ...]

Parameters:

lu Specifies the LU number of the LAN LU to the client. VCPMT examines the parameter to make sure that the LAN LU provided is a valid one. If not, it returns an error. Refer to Appendix A for a list of LANVCP error codes.

Up to seven LUs may be specified, each separated by a comma.

If DISPATCH is not needed and not running, you should always schedule the LAN Node Manager before scheduling VCPMT. Doing so allows you to run NM later.

It is possible to run multiple copies of VCPMT for different LAN interfaces to get higher performance.

RMVCP – Remote VCP

RMVCP allows you to have an interactive VCP session with a remote A-Series computer's VCP. The interactive user interface can designate storage files for VCP memory dump sessions and is used by VCPMT, the remote VCP monitor, to display messages from VCP download sessions.

An interactive VCP session is started by the program RMVCP with the following command:

Syntax:

```
RU,RMVCP,client
```

Parameter:

client	Either the node name or node number of the client. The node name or node number is the one that is supplied to the IPL_BUILD or IPL_EDIT programs and is contained in the configuration file /FILES802/IPL_TABLE.TXT.

When the remote system is ready to accept commands, the following RMVCP prompt is displayed on the server's terminal:

```
RMVCP>
```

The rest of this section explains:

- RMVCP commands
- VCP messages from the remote or client node
- RMVCP memory dump session

RMVCP Commands

RMVCP and remote VCP commands may be entered from the server's terminal during a VCP interactive session. RMVCP commands all begin with the slash (/) character, and any command string beginning with a slash is interpreted as being an RMVCP command. All other command strings are interpreted as VCP commands and passed on to the remote VCP.

The remote LAN interface card displays a VCP protocol error message on the server's terminal in one of the following situations:

- The remote CPU is not in VCP mode (a remote VCP command was sent before a /B).
- The remote LAN interface card is already engaged in a VCP session with some other node.

However, if the RMVCP /BREAK command is issued, the remote LAN interface disconnects from any existing VCP session and returns to VCP mode.

RMVCP supports the following five commands which are explained below:

- /BREAK or /B — Send break to client's VCP.
- /EXIT or /E — Return to server and terminate RMVCP.
- /HELP or /? — Display RMVCP commands and display node name and LAN station address of client node.
- /READ or /R — Send read request to LAN card.
- /WAIT or /W — Wait for input from client node.

/BREAK

The /BREAK or /B command causes RMVCP to send a type 1 "Break-to-VCP" command which causes the remote A-Series node to go into VCP mode. This is equivalent to hitting the break key on a system console which is enabled for VCP.

```
RMVCP> /B
```

The LAN interface card firmware does not accept any VCP commands until the client's CPU is in VCP mode.

Note The /BREAK command halts the remote A-Series system, and all activity on that node stops.

/EXIT

The /EXIT or /E command terminates the VCP interactive session between you and the remote node and terminates RMVCP. Once the interactive session terminates, VCP messages arriving at the server node are printed on the system console instead of the server's terminal.

/HELP

The /HELP or /? command causes RMVCP to display the node name and LAN address of the remote node with which the VCP interactive session is active, and a list of the supported RMVCP commands.

/READ

The /READ or /R command causes the VCP interactive session to go into the read state for one time-out period or until a VCP message from the remote node arrives. No VCP message and no RMVCP prompt is displayed, and control is not returned to you.

/WAIT

The /WAIT or /W command causes RMVCP to wait for a VCP message from the remote computer before returning to you with a RMVCP prompt.

When any VCP command is passed through to the remote A-Series, or when the RMVCP /BREAK command is issued, the VCP interactive session goes into a read state waiting for a response from the remote A-Series VCP program. If no response arrives after one time-out period (about 10 seconds), a RMVCP prompt is printed and control returns to you.

The /WAIT command causes RMVCP to enter the read state without a timeout and to wait until a VCP message arrives from the remote node. To regain control of RMVCP, you must enter the system break command:

```
CM> BR RMVCP
```

which causes RMVCP to send a break message to VCPMT.

VCP Messages From the Remote Node/Client

VCP messages arriving at the server from the remote node during a VCP interactive session are displayed on the server terminal in the format below. Refer to Appendix A for a list of LANVCP error codes.

If an RMVCP prompt is displayed and RMVCP is waiting for input from you, the VCP messages are queued up and displayed on the terminal when the RMVCP read completes. The user command typed in response to the RMVCP prompt is ignored. You are informed that a message arrived while the user read was pending.

```
>>---VCP <message type description> arrived--------------------------<<
>>---from <node_name>-----------------------------------------<<
>>---at address <hex address> on lu <LAN lu>---------------------<<
          :
           text of message...
          :
          :
          :
>>-------<date and time stamp>-------------------------------------<<
```

The fields in the RMVCP VCP message are described here:

message type description — This field can have any one of the following entries:

- *message*: Normal VCP display with text in interactive session.
- *unexpected message*: As above but unexpected.
- *download request file number*: Boot request for file number P*fffff*.
- *memory dump request*: After a memory dump has been requested.
- *address acquisition request*: Response by RMVCP is automatic.
- *protocol error text*: Self-explanatory text included in the message.

node_name — Node name of the client node.

hex_address	LAN station address, in hex, of the client node.
LAN lu	LAN LU of the client node.
text of message	Main text of the RMVCP VCP message.
date and time stamp	Date and time of the message.

If a VCP interactive session is active with the node from which the message arrived, or a download session or memory dump session is spawned by an interactive session, the message is displayed on the user's terminal. If, however, no interactive session with the remote node is active or if the interactive session is suspended, the message is displayed on the system console of the server. A request to the user for a memory dump file name is sent to the same terminal as the one that displays the message.

Examples

User input is underlined. The following examples show a remote download to node 900.

```
CI> rmvcp,900

 Virtual Control Panel Monitor Interactive Session
   with memory-node
   at LAN lu 132 address 08000900524d

RMVCP> /b
>>--VCP Message arrived-------------------------------------------<<
>>--from memory-node----------------------------------------------<<
>>--at address 08000900524d on lu 132-----------------------------<<

    P  000000 A 000024 B 004020  RW 000000  M 000000 T 000000
VCP>
>>-------------------------Wed Jun 31, 1990  2:06 pm--------------<<

RMVCP> %bds
>>--VCP Boot Request for File #00000 arrived----------------------<<
>>--from memory-node----------------------------------------------<<
>>--at address 08000900524d on lu 132-----------------------------<<

>>-------------------------Wed Jun 31, 1990  2:06 pm--------------<<

RMVCP> Download started from file name
       /MBSYS/SYSTEM/download-file
       to memory-node

>>--VCP Message arrived-------------------------------------------<<
>>--from memory-node----------------------------------------------<<
>>--at address 08000900524d on lu 132-----------------------------<<

>>-------------------------Wed Jun 31, 1990  2:06 pm--------------<<

RMVCP> /e
VCP Interactive Session Ended
```

RMVCP Memory Dump Session

A memory dump from the remote node can be stored into a file on the local node. You can use the %WDS VCP command. Following a memory dump request message display after the %WDS from the VCP, the user is asked for the size of the memory dump to be done.

```
RMVCP>       enter number of 2048 byte pages of memory dump
             from
             <node name>
             (none or zero length aborts memory dump)

RMVCP> _
```

Next, the user is prompted for the file name of the memory dump file. The user must enter the full file path name (/dir/.../dir/filename.ext) and the file must not currently exist.

```
RMVCP>       enter file name for memory dump data from <node name>
             (no file name aborts memory dump)

RMVCP> _
```

A type 1 file of the correct size is created to hold the memory dump data. A message informing the user of memory dump progress is printed on the user terminal after each 64K bytes dumped.

When the memory dump completes, the number of pages dumped is displayed, and the user is prompted for comments that are stored at the end of the memory dump file.

```
RMVCP>       for memory dump data from
             <node name>
             enter up to <256 > memory dump comment characters
             (blank line terminates comments)

RMVCP> _
```

Comments are accepted as lines of text until a zero length line is entered or 256 bytes have been entered. If no comments are desired, simply hit carriage return to close the file.

RMVCP returns any FMP errors to the user with the following message:

```
RMVCP>       FMP error <err number> <opening/writing to>
             memory dump file name
             <file name>
```

Downloading Over a LAN Link

Before loading a memory-based system over a LAN link, perform the following steps. These steps are also summarized in DOC/IPL_BUILD.READ and DOC/INSTALL.READ.

Your local computer is known as the server. The destination or remote computer is the client.

1. Create the merged system file using BUILD. Refer to Chapter 10 and Appendix I in the *RTE-A System Generation and Installation Manual*, part number 92077-90034, for BUILD information. The system file is also known as a download file because it is downloaded to the remote node. The default directory for these system files is /FILES802.

2. Obtain the server LAN card's station address using the LAN Node Manager, NM. If multicast addressing is desired, also run NM to set the server's LAN station address on the client LAN card.

   Refer to Chapter 5 for information on using the Node Manager software.

3. Link the LANVCP programs using the INSTALL_VCP.CMD command file as follows:

   ```
   CI> wd /vcplus/lanvcp
   CI> tr install/install_vcp.cmd [snap] [number]
   ```

   where:

   snap is your snap file name. If not specified, the default is the current system snap file.

   number is the number of clients that can be simultaneously serviced. If not specified, the default is 16 clients, 28 is the maximum.

4. Transfer to INSTALL/BOOT_VCP.CMD to execute the LANVCP programs, VCPMT and DISPATCH. VCPMT is the LAN VCP monitor that downloads the system and handles the remote VCP session. DISPATCH is the program that monitors LAN packets and determines if they should be handled by the LAN Node Manager software or by VCPMT.

   ```
   CI> tr install/boot_vcp.cmd <lu>
   ```

   where

   <lu> is the LAN link LU of the server's LAN card.

   The programs are installed onto the /PROGRAMS directory.

5. Run IPL_BUILD to create a configuration file used during the download process by VCPMT. IPL_BUILD is part of the LANVCP software. The configuration file contains the system file name, the LAN LU, and LAN station address of the client. The default configuration file is /FILES802/IPL_TABLE.TXT. If you need to modify the configuration file, run IPL_EDIT or EDIT/1000. Both IPL_BUILD and IPL_EDIT are interactive programs and prompt you for the information to enter or to change. IPL_BUILD and IPL_EDIT are explained in more detail in this chapter.

6. If you want to set the client CPU for automatic boot over LAN on power up, refer to the A-Series computer hardware documentation.

After completing the above steps from the server's node, download and boot your memory-based system at the client's node:

1. Make sure that VCPMT, the remote LAN VCP monitor program, is scheduled (see INSTALL/BOOT_VCP.CMD) at the server's node.

2. Break into the VCP front panel mode at the client in one of the following ways:

   If the client has a direct VCP terminal, simply hit the BREAK key. Then enter the VCP boot command:

   ```
   VCP> %BDSff00sc
   ```

   If the client has a LAN card with the VCP enabled, then run RMVCP on the server. RMVCP is the interactive user interface to VCPMT. At the RMVCP prompt, enter the /BREAK or /B command and then enter the VCP boot command.

   ```
   CI> RMVCP <client>
   RMVCP> /BREAK
   RMVCP> %BDSff00sc
   ```

   where:

client	is the computer name of the destination system. The client name is specified during the IPL_BUILD process described later in this chapter.
%BDS	executes the boot loader program and begins execution of the system when the entire merged system file has been loaded into the client's memory.
ff	an octal number from 00000 to 77777. It is converted to ASCII to form the P*fffff* file name. For example, %BDS150024 means to boot from system file P00015 from the interface card in select code 24. Refer to the "LAN Link" subsection under "Special Considerations" in Chapter 10 of the *RTE-A System Generation and Installation Manual*, part number 92077-90034. The system file is also referred to as a "P" file or download file. Download files are to be stored in directory /FILES802 and are specified in the IPL_BUILD configuration file, /FILES802/IPL_TABLE.TXT. If you default the *ff* parameter in the bootstring to P00000, a default system file is used as specified in /FILES802/IPL_TABLE.TXT. Refer to the "Download file" description earlier in this chapter for more information.
00	is used as a placeholder in the bootstring if the *ff* parameter is not zero.
sc	is the select code of the client's LAN card.

Upon successful download, the client stops communicating with the server. RMVCP waits for a reply from the client that it will never receive. To regain control of RMVCP, you must wait for RMVCP to time out (about 10 seconds) or you can issue a CM> BR RMVCP command. Then you can issue the RMVCP /EXIT command.

A

Error Codes & Descriptions

NMGR Error Codes

As described in Chapter 4, the Node Manager software returns a description on command entry errors (from the NM and NM2 modules), and error codes on command execution errors (from the NMGR module). Table A-1 describes NMGR error codes returned.

Table A-1. Command Execution Errors Returned by the NMGR Module

Error Type	Error Code Number and Description
0 = No Error	None
1 = Link Error (LE###)	000 = Invalid NM Command
	008 = Multicast Address does not exist
	009 = Multicast Address already exists
	00A = Already 64 entries in the Multicast ADR list
	00C = Multicast list is empty
	00E = Corrupted MCAST.TXT file
2 = NM Error (NM###)	001 = Entity not supported
	002 = Entity unknown
	003 = Parameter not supported
	004 = Illegal function for this parameter
	005 = Function not supported
	006 = Service not supported
3 = FMP Error (FM###)	The positive FMP Error Code value converted to hexadecimal (see system manuals)
4 = Driver Error (DE###)	ID.67 Error Code (see Table A-2)
Note: ### indicates 3 hexadecimal digits.	

Note For Table A-1, refer to your system manuals for File Management Package error codes (Type 3 errors).

Driver Error Codes

Driver error codes (Type 4 errors) are returned to the user through Node Manager software (specifically, the NMGR module) and defined in Table A-2.

For Table A-2, driver reported errors may be recoverable, or irrecoverable. Recoverable errors are considered transient, and the driver will likely respond to new Node Manager requests. Irrecoverable errors, on the other hand, imply that new driver requests will fail and may result in an inoperative node.

Table A-2. Driver Error Codes

RECOVERABLE ERRORS	
Error Code	**Error Description**
000 hex	No Error. Driver successfully executed the command.
001 hex	Powerfail. An active request will complete with this error.
002 hex	DMA Error. Commonly, a parity error during DMA transfer, or DMA handshake failure.
003 hex	(reserved)
004 hex	Driver request contains no or invalid security code.
005 hex	Driver request is invalid or not recognized.
006 hex	Parameter value in request is illegal or out of range.
007 hex	Illegal buffer size detected during driver request.
008 hex	Card transmit buffer space is not available.
009 hex	External loopback failure indicated by card.
IRRECOVERABLE ERRORS	
00A hex	No card response (driver times out).
00B hex	Hardware failure (bad NOVRAM and/or MAU power fuse)
00C hex	Card self-test failed.
00D hex	Initial write to card failed after self-test or powerfail.
00E hex	Initial read from card failed after booting.

LANVCP Error Codes

LANVCP error messages can be reported to either of the following two locations:

- The user's terminal when the error occurs during an interactive session or a session spawned from an interactive session.
- The system console when the error occurs during an unexpected session or session spawned from an unexpected session.

The error numbers are negative (to distinguish them from the positive, non-error trace message numbers).

−1: Class get return error <RTE error>

The RTE error occurred while attempting a class get; usually aborts VCPMT.

−2: Class write/read error <RTE error>

The RTE error occurred while attempting a class write, read, or write/read; usually aborts VCPMT.

−3: Attempt to exceed maximum number of sessions

An attempt was made to start a new session and the memory space required would have exceeded the memory allocated for VCPMT. (Either let the node retry, or use a slower VCPMT which is able to handle more nodes.)

−4: Error in logging trace data, tracing disabled

Some error occurred in writing to the trace file or LU and tracing was automatically turned off. Tracing is not supported.

−5: IPL Table File access error

Some error occurred while attempting to look up the node_name, LAN address and LU, or download file name in the IPL table file (/FILES802/IPL_TABLE.TXT).

−11: VCPMT aborted due to excess RTE errors

VCPMT had too many RTE errors and aborted. See errors −1 and −2, above.

−12: Detected error in opening trace file

VCPMT was unable to open the trace file when an attempt was made to initiate tracing. Tracing is not supported.

−13: Detected LAN interface error <error number>

VCPMT received a bad LAN driver status from a request to the LAN card.

–14: Unexpected_session received message in error, type:

<VCP message type>

Some message types are not expected during unexpected sessions.

–15: Error in opening error_printer file

VCPMT initialization was unable to open the error printer file (LU 1).

–17: Interactive session received message in error, type:

<VCP message type>

Some message types are not expected in interactive sessions (for example, download record acknowledgements).

–18: Error in opening download file, FMP error: <FMP error>

The FMP error occurred when attempting to open a download file.

–19: Error in reading download file, FMP error: <FMP error>

The FMP error occurred when attempting to read from a download file.

–20: Download failed on LAN address <address>

A download session has failed to download the indicated address.

–21: Error in opening memory dump file, FMP error: <FMP error>

The FMP error occurred when attempting to open a memory dump file.

–22: Error in writing to memory dump file, FMP error: <FMP error>

The FMP error occurred when attempting to write memory dump data to a memory dump file.

–23: Memory dump failed on LAN address <address>

A memory dump session has failed to complete a memory dump from the indicated address.

–24: Session already active, cannot initiate a new session

If any kind of VCP session is active between this node and a remote node, a new interactive session or programmatic interactive session may not be initiated with the remote node.

B

NM Command Summary

This appendix provides a summary of Node Manager software commands and may be used as a "quick reference." The commands are displayed in a format that would result from a "Help" command (that is, "?") entry.

```
NM Command Summary:

CONFIGURATION:

1. Read Link Configuration          RC[,[ADR][,[PAR#][,[option][,LU#]]]]
2. Set Link Configuration           SC,[ADR],PAR#[,[PAR-Value][,[option][,LU#]]]
3. Update Link Configuration        UC[,[ADR][,[option][,LU#]]]
4. Insert Multicast Address         IM,[ADR],MulticastAddress[,LU#]
5. Delete Multicast Address         DM,[ADR],MulticastAddress[,LU#]
6. Create Link File Directories     CD[,[ADR][,[FileAddress][,LU#]]]
7. Purge Link File Directories      PD[,[ADR][,[FileAddress][,LU#]]]
8. Check Link File Existence        CK[,[ADR][,[FileAddress][,LU#]]]

DIAGNOSTICS

1. Initiate Card Self Test          TC[,[ADR][,[LU#][,Rep]]]
2. Do External Loopback to MAU      EL[,[ADR][,[LU#][,Rep]]]
3. Issue Test Loopback Command      TEST,[ADR],DSAP[,[MSGLEN][,[LU#][,Rep]]]
4. Issue XID  Loopback Command      XID,[ADR],DSAP[,[LU#][,Rep]]

EVENT LOGGING:

1. Read Event Log File              RE[,File-Address]

STATISTICS:

1. Read Link Statistics Counters    RS[,[ADR][,LU#]]
2. Zero Link Statistics Counters    ZS[,[ADR][,LU#]]

COMMAND STACK:

1. Display Command Stack            /[n]
```

```
Parameters enclosed in [] can be omitted if no parameter follows,
and the default values are used.  If there are any parameters following
the [], a NULL parameter ",," has to be used before the next parameter.
For instance:  IM,,FF-FF-FF-FF-FF-0E


Blank(s) and Comma(s) are both legal parameter separators.
Either uppercase or lowercase letters are allowed.


ADR   = 12 digit hex 802.3 address (XX-XX-XX-XX-XX-XX, X: a hex digit).

        Specifies the destination station address of the NM command.
        [default]- local station ADR of the 802.3 LU specified by the LU#.

LU#   = A decimal number in the range of 2 to 255.

        [default]- lowest 802.3 LU (even).

        When there is more than one 802.3 card in the system,
        LU in conjunction with ADR specifies the following:

        If ADR=local   LU identifies the card for which this command
                       is addressed to (if LU and ADR specify the
                       same card).

                       NOTE :  When both ADR and LU are
                       specified and represent different 802.3
                       cards, the LU specifies the card that will
                       send the request onto the network and ADR
                       specifies the station address to which the
                       request will be sent.

             For instance, in a system with 2 802.3 cards:
               card1 : LU=60, ADR=00-01-00-02-00-03
               card2 : LU=70, ADR=00-03-00-04-00-05

             NM command : RC,00-01-00-02-00-03,1,T,70

             will tell NM to send a Read Temporary station address command
             onto the network using LU=70 addressed to ADR=00-01-00-02-00-03.

        If ADR=remote  LU identifies the card from which this request
                       is being sent onto the network.
```

PAR# = A decimal number or a character explained below:

1	:	Station Address
2	:	Multicast Address List
4	:	Receive Packet Filter
5	:	Retry Limit
6	:	Save Bad Packet Flag
7	:	Trace Mode Flag
8	:	DSAP/CLASS number (program id) table
9	:	Downloading Server Station Address
10	:	File Server Station Address
11	:	Card Status
A	:	[default] All of the above except for 2,8, and 11; this PAR number only applies to RC command.

Option = A character explained below:

P Permanent configuration parameters – this option only applies to the following parameters : (1,4,5,6,7,9) These are card parameters stored in the NOVRAM. Card parameters that are stored in the RAM as well as other parameters stored by the NM are referred to as 'Temporary' parameters.

T Temporary configuration parameters. [default]

DSAP = 2 hex digits that specify the Destination SAP. [no default value]

MSGLEN = a decimal number specifies the 802.3 information field length in bytes from 0 to 1497. [default = 0]

Multicast Address = same syntax as ADR, an 802.3 address with LSB(bit)=1. For example, in ADR=XY–XX–XX–XX–XX–XX, Y is one hex digit, and the LSB(bit) of the 802.3 address is the LSB(bit) of Y, i.e. for ADR to be a multicast address, Y must be odd. [no default value]

File–Address = same syntax as ADR, a link file identifier. Must be an individual 802.3 address. [default to ADR]

PAR–Value = the new value of the parameter PAR#, applies to parameters: 1,4,5,6,7,9,10.
Default values: for parameters 1,9,10 – default to ADR,
for parameters 4,5,6,7 – default to 0.

Rep = Number of repetitions requested. The TC, EL, TEST, and XID commands will repeat Rep number of times, or until failure, as a diagnostic aid. The command may be aborted before completion by entering 'BR,NM' from the CM> prompt. (An input value of Rep = 0 will loop 'infinitely' until a failure occurs or 'BR,NM' is input from the CM> prompt.) The default value is Rep = 1.

C

IEEE 802 Family Relationships

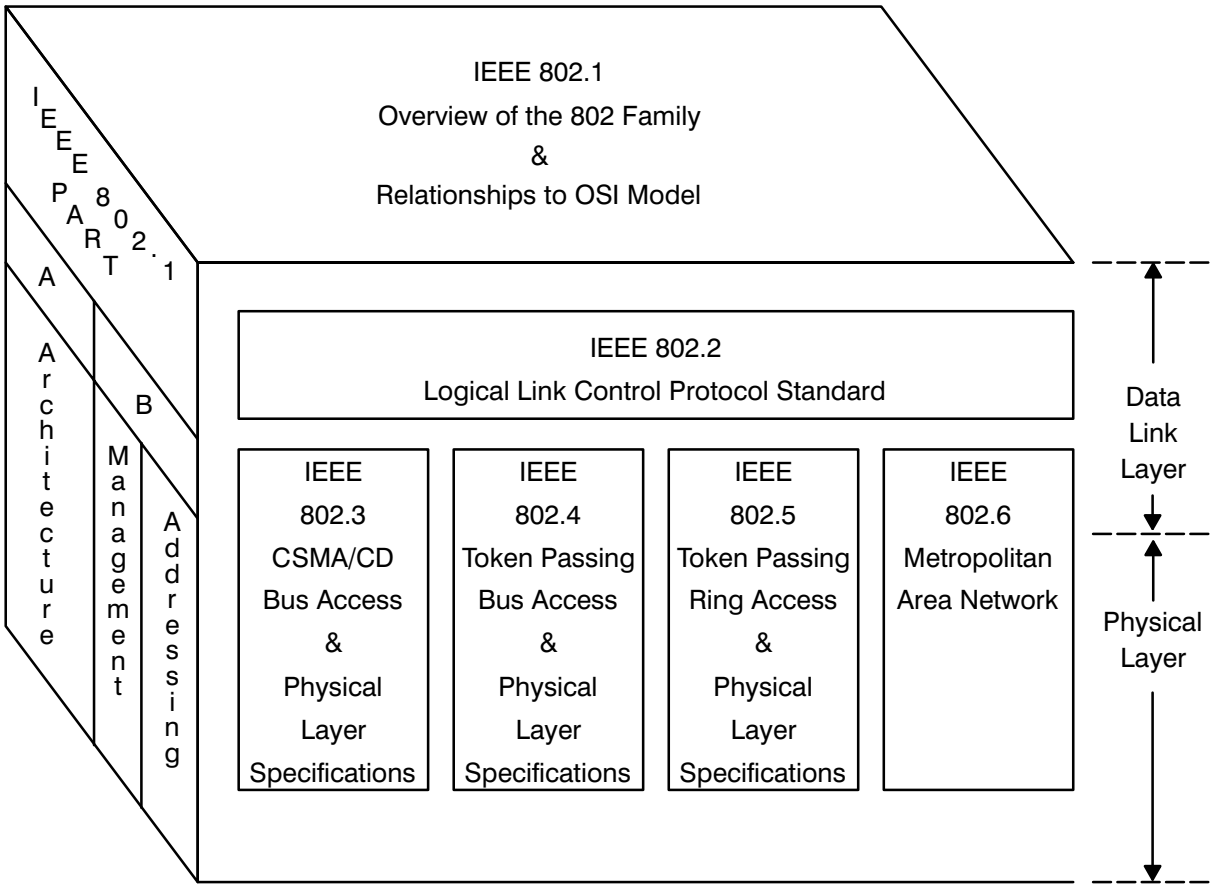


Figure C-1. IEEE 802 Family Relationships

D

Record of Changes

EDITION/ UPDATE	DESCRIPTION
1st Edition	First release of manual, no changes.
Update 1	Printed circuit board components changed to correct a timing problem in NOVRAM support circuitry. Assembly 12076-60001 date code advanced to B-2614. The driver name was changed from “ID.67” to “ID*67”. Also, the product structure was modified to provide the driver, Node Manager software, and related modules with the operating system, HP 92077A, RTE-A Version 4.1 (Rev 4010) or later.
Update 2	With RTE-A Version 5.0, or later, the Node Management software was enhanced with a Command Stack feature. The Command Stack is accessed from the user interface program, NM. In addition, the software now checks for the availability of the driver packet read program, READR, when NM is run. If READ1 is not restored or running, applicable error messages are displayed.
2nd Edition	At the RTE 6.1 release, system table space required by the LAN driver was significantly reduced; only one LU and DVT are now required for each LAN card, and the LU can be odd or even. (Previously, two consecutive LUs were used and the first had to be an even-numbered LU.) The default IFT extension was reduced from 204 words to 73 words; the READR program (RPed as READ1 and READ2) is no longer required by the LAN driver or Node Manager software; and %GEN67 which contained default driver parameters is no longer used. Driver and Node Manager software installation documentation was pulled from the *HP 12076A LAN/1000 Link Local Area Network Interface Controller (LANIC) Installation Manual*, part number 12076-90001 and is now included as part of the *HP 12076A Node Manager’s Manual*, part number 12076-90002.

“Remote VCP and Download Over LAN” (Chapter 11 of the *RTE-A System Generation and Installation Manual*, part number 92077-90034) information is included as of this revision as Chapter 6, LANVCP Operations.

Index

Symbols

/BREAK command, 6-9
/EXIT command, 6-9
/HELP command, 6-9
/READ command, 6-9
/WAIT command, 6-10

A

ADR parameter, 5-8
  defaults, 5-8, 5-9
  null address default, 5-9
answer file entries, 3-3
  driver relocation, 3-3
  memory allocation, 3-6
  system relocation, 3-3
  table generation, 3-4
Attachment Unit Interface. *See* AUI
AUI, 1-2
  and external loopback, 5-38

B

babble, 5-39, 5-54
bad packet, 1-6, 4-15
  logging, 4-4, 4-7, 5-29, 5-47
  routing, 4-9
bad packet routine, program code, 4-9
Broadcast Address, 2-5, 2-6
  packet filter, 4-18
buffer error, 5-39, 5-54

C

C/R bit, SSAP, 2-10
card configuration
  driver's copy, 4-12
  NOVRAM, 4-11
  RAM, 4-11
card failures, 5-36
card status
  bit definitions, 5-15
  displaying, 5-12, 5-14
carrier lost, 5-55
CD command, 5-29
CK command, 5-32
Class 1 station, 2-3
Class 2 station, 2-3
class number table, 4-8
  displaying, 5-12, 5-16
collision, 5-39
command entry, 5-2, 5-4
  during initialization, 4-16
  errors, 4-2, 5-4
command execution errors, 4-3, 5-6, A-1
command notation, 5-1
command parsing, 4-2
command routing, 4-20
command stack, 5-4
command summary, 5-3, B-1
commands
  check link file existence (CK), 5-32
  configuration, 5-10
  create link file directories (CD), 5-29
  delete multicast address (DM), 5-27
  diagnostic, 5-34
  do external loopback to MAU command (EL), 5-38
  event log, 5-47
  insert multicast address command (IM), 5-25
  issue test loopback (TEST), 5-41
  LANIC self-test (TC), 5-35
  purge link file directories (PD), 5-31
  read event log file (RE), 5-48
  read link configuration (RC), 5-11
  read link statistics counters (RS), 5-56
  remote VCP (RMVCP), 6-8
    /BREAK, 6-9
    /EXIT, 6-9
    /HELP, 6-9
    /READ, 6-9
    /WAIT, 6-10
  set link configuration (SC), 5-17
  statistics, 5-52
  to broadcast addresses, 5-7
  to multicast addresses, 5-7
  update link configuration (UC), 5-22
  XID, 5-44
  zero link statistic counters (ZS), 5-58
configuration, node, 1-6
configuration commands, 5-10
configuration file
  for download over LAN, 6-2
    example, 6-4
  IPL_BUILD, 6-2
  IPL_EDIT, 6-2
connection, hardware, 1-1
Control field, 5-49
  command set, 2-12
  F bit (Final), 2-12
  P bit (Poll), 2-12
  response set, 2-12
  TEST command, 2-12, 5-41
  TEST response, 2-12
  UI command, 2-12

XID command, 2-12, 5-44
XID response, 2-12
CRC, 2-15, 5-39, 5-55

D

defaults, interdependent, 5-7
Destination Address field, 2-5
I/G bit, 2-6
U/L bit, 2-6
diagnostic commands, 5-34
command repetition, 5-34
diagnostic services, 1-6
directory
Link File, 4-5, 5-29, 5-31, 5-32
root, 4-5
disk access, 4-20
disk files
EL.TXT, 4-4
MCAST.TXT, 4-4, 4-5
disk-based node, 1-7
DISPATCH, monitoring LAN packets, 6-6
Dispatcher, 1-5, 4-10
program code, 4-10
DM command, 5-27
download, over LAN, system file selection, 6-6
Download Server Station Address, 1-6
displaying, 5-12
during initialization, 4-15
file server, 5-20
initial, 4-11
limitations, 5-20
setting, 5-18
VCP, 5-20
driver
card configuration, 4-12
class number table, 4-8
error codes, A-2
initialization, 3-8
multicast address, 5-11
relocation, 3-3
DSAP
field, 2-8
globally administered, 2-9
Group, 2-8, 4-10, 5-16
I/G bit, 2-8
individual, 2-8
locally administered, 2-8
null, 2-9
reserved, 2-9
TEST command, 5-42
XID command, 5-45

E

EL command, 5-38
interpreting failure bits, 5-39
EL.TXT file, 4-4, 4-7, 5-29, 5-47
path, 5-47
using the RE command to read, 5-47
error codes, A-1
driver, A-2
LANVCP, A-3
errors
codes, 5-6
command entry, 4-2, 5-4
command execution, 4-3, 5-6, A-1
during initialization, 4-16
event log file, 5-48
NM, 4-17
NM2, 4-17
NMGR, 4-17
NMGR type, 4-3, 5-6, A-1
NMtimeout, 5-6
statistics counters, 5-54
TEST command, 5-42
XID command, 5-45
Ethernet Packet type (ET), class number table entry, 4-8
event log commands, 5-47
event log file, 1-6, 4-7, 5-47
displaying, 5-48
errors, 5-48
event logging, services, 1-6
exiting Node Manager, 5-3
external loopback, 5-38
and MAU, 5-40

F

failures
external loopback, 5-39
NOVRAM, 5-36
RAM, 5-36
fields, packets/frames, 2-4
file server node, 1-7
File Server Station Address
changing, 5-20, 5-29, 5-31
displaying, 5-12
during initialization, 4-15
setting, 5-18
FileAddress parameter, 5-8
defaults, 5-9
Frame Check Sequence field, 2-15
frames, 2-3
invalid (IEEE 802.3), 2-15
framing, 5-39, 5-54
fuse, MAU power, 5-36

G

generating a new system, 3-6
globally administered
Destination Address, 2-6
DSAP, 2-9
Group DSAP, 2-8
packet processing, 4-10, 5-16
program code, 4-10

H

heartbeat, 5-38, 5-39, 5-54
help facility, 5-3
  aborting, 5-4
  listing, 5-4
  MENU file, 4-5, 5-3
    display, B-1

I

I/G bit
  Destination Address, 2-6
  DSAP, 2-8
identification, software media, 1-1
IEEE 802
  invalid frames, 2-15
  services, 2-3
IEEE 802.3 packets, frames, 2-4
IEEE 802.3 Protocol Data Unit, 2-4, 2-7
IM command, 5-25
Individual address, packet filter, 4-18
Information field
  with TEST control field, 2-15
  with UI control field, 2-13
  with XID control field, 2-13
initialization
  errors, 4-16
  Link File directory, 4-15
  Node Manager software, 4-13
International Standards Organization. *See* ISO
invalid packets, frames/IEEE 802, 2-15
IPL_BUILD, 6-2
IPL_EDIT, 6-2
IPL_TABLE.TXT, format, 6-5
ISO, 2-1

L

LAN
  autoboot over, 6-2
  download over, 6-13
  monitoring LAN packets, 6-6
LAN connection, 1-2
LANIC cards, 1-1
LANVCP
  error codes, A-3
  operation, 1-5, 6-1
Late Collision, 5-39, 5-55
Length field, 2-7
Link File directory, 4-5
  creating, 5-29
  during initialization, 4-15
  event log commands, 5-47
  existence of, 5-32
  purging, 5-31
list facility, RE command, 5-49
locally administered
  Destination Address, 2-6
  DSAP, 2-8
  SSAP, 2-10
LU# parameter, 5-8
  defaults, 5-8, 5-9

M

manager node, 1-7, 4-1
Manufacturer's Address, 2-6
MAU, 1-2
  and external loopback, 5-38, 5-40
  power fuse, 5-36
MCAST.TXT file, 4-4, 4-5, 5-26, 5-29, 5-47
  card configuration, 4-7
  editing, 4-6
  path, 4-6
Medium Access Control Frame, 2-4, 2-15
Medium Attachment Unit. *See* MAU
memory allocation, 3-6
memory-based node, 1-7
memory-based system, downloading over LAN, 6-1
MENU file, 4-5, 5-3
  display, B-1
module
  NM, 4-1
  NM2, 4-1
  NMGR, 4-1
modules provided, 3-3
Multicast Address, 2-5, 2-6, 4-4
  card configuration, 4-7, 5-26
  deleting, 5-27
  displaying, 5-12, 5-13
  driver's copy, 5-11, 5-26
  MCAST.TXT, 4-5, 5-26, 5-28
  packet filter, 4-18
  requirements, 5-25
multiple cards
  command routing, 4-20
  disk access, 4-20

N

NM module, 4-1
  configurable parameters, 5-2
  errors, 4-2, 4-17
  system status, 4-17
NM2 module, 4-1, 4-2
NMGR module, 4-1
  errors, 4-3, 4-17, A-1
  system status, 4-17
NMretry parameter, 5-2
NMtimeout parameter, 5-2
  errors, 5-6
node
  designation considerations, 1-8
    economy, 1-8
    high availability, 1-8
    performance, 1-8
    security, 1-8
  implementation considerations, 1-7
  types, 1-7
Node Manager

command processing, 4-2
exiting, 5-3
initialization, 3-8, 4-13
multiple cards, 4-20
security, 5-1
software services, 1-5
configuration services, 1-6
starting the program, 5-2
NOVRAM
changes to, 5-18, 5-23
configuration data, 4-11
download server station address, 5-20
failures, 5-36
initial settings, 4-12
station address, 5-19
null DSAP, 2-9
null SSAP, 2-11

O

Open Systems Interconnection model. *See* OSI Model
orphan packet routine, program code, 4-9
orphan packets, 1-6, 4-15
logging, 4-4, 4-7, 5-29, 5-47
routing, 4-9
saving, 4-10
statistics, 5-56
OSI model, 2-1

P

packet, 2-3
bad, 1-6, 4-7, 5-29, 5-47
Destination Address, 2-5
fields, 2-4
format, 2-4
Frame Check Sequence, 2-15
Group DSAP, 4-10, 5-16
invalid (IEEE 802.3), 2-15
length, 2-4
Length field, 2-7
orphan, 1-6, 4-7, 5-29, 5-47
Pad field, 2-15
preamble, 2-5
Protocol Data Unit field, 2-7
receiving, 4-18
routing, 4-9
Source Address, 2-7
Start Frame Delimiter, 2-5
TEST, 1-6
trace, 1-6, 4-7, 5-29, 5-47
XID, 1-6
packet filter, 5-20
displaying, 5-12
initial, 4-11
modes, 1-6, 4-18, 5-11
receiving packets, 4-18
settings, 4-19, 5-12, 5-18
Pad field, 2-15
parsing, 4-2
PD command, 5-31
preamble field, 2-5
Program Code (PC)
class number table entry, 4-8
special programs, 4-8
Promiscuous mode, 5-20
packet filter, 4-18
Protocol Data Unit, 2-7
Control field, 2-11
DSAP field, 2-8
Information field, 2-13
SSAP field, 2-10

R

RAM, configuration data, 4-11
RC command, 5-11
RE command, 5-48
list facility, 5-49
remote VCP, 6-8
download example, 6-11
error codes. *See* LANVCP
memory dump, 6-12
messages from remote node, 6-10
VCPMT monitor program, 6-7
Rep parameter, 5-34
retry limit, 1-6
displaying, 5-12
setting, 5-18
RMVCP program, 6-8
commands, 6-8
/BREAK, 6-9
/EXIT, 6-9
/HELP, 6-9
/READ, 6-9
/WAIT, 6-10
memory dump session, 6-12
root directory, 4-5
routing packets, 4-9
RS command, 5-56

S

SAP, 2-8
class number table entry, 5-16
Save Bad Packet flag
displaying, 5-12
initial, 4-11
setting, 5-18
SC command, 5-17
security, Node Manager software, 5-1
Security/1000, 3-6
select code, 1-2
self-test, 5-35
interpreting failure bits, 5-36
Service Access Point (SAP), class number table entry, 4-8
services, IEEE 802, 2-3
slave node, 1-7, 4-1

software media, 1-1
Source Address field, 2-7
SSAP
  C/R bit, 2-10
  field, 2-10
  locally administered, 2-10
  null, 2-11
Start Frame Delimiter field, 2-5
Station Address, 5-19
  displaying, 5-12
  factory setting, 1-3
  initial, 4-11
  setting, 5-18
statistics
  commands, 5-52
  counters
    description, 5-54
    maximum values, 5-52
    reading, 5-56
    resetting, 5-58
    self-test, 5-35, 5-52
  services, 1-6
system relocation, 3-3
system requirements
  hardware, 1-1
  memory, 1-4
  RTE-A, 1-3
system status, with Node Manager, 4-17

T

table generation, 3-4
TC command, 5-35
  interpreting failure bits, 5-36
TEST command, 5-41
  errors, 5-42
  self-addressed, 5-42
TEST packets, 1-6
testing
  card self-test, 5-35
  external loopback, 5-38
Time Domain Reflectometer (TDR), 5-55
Trace Mode flag
  displaying, 5-12
  initial, 4-11
  setting, 5-18
trace packet, 1-6, 4-15
  logging, 4-4, 4-7, 5-29, 5-47
  routing, 4-9
trace packet routine, program code, 4-9
Type 1 service, 2-3, 2-11, 2-13, 5-44
Type 2 service, 2-3, 2-11, 2-13, 5-44

U

U/L bit, Destination Address, 2-6
UC command, 5-22
UI command, Control field, 2-12
user interface, 4-2, 5-2

V

VCP, 4-10
  messages from remote node, 6-10
  program code, 4-10
VCPMT monitor program, 6-7
verifying the system, 3-9

X

XID command, 5-44
  errors, 5-45
  self-addressed, 5-45
  uses, 2-14
XID packets, 1-6

Z

ZS command, 5-58