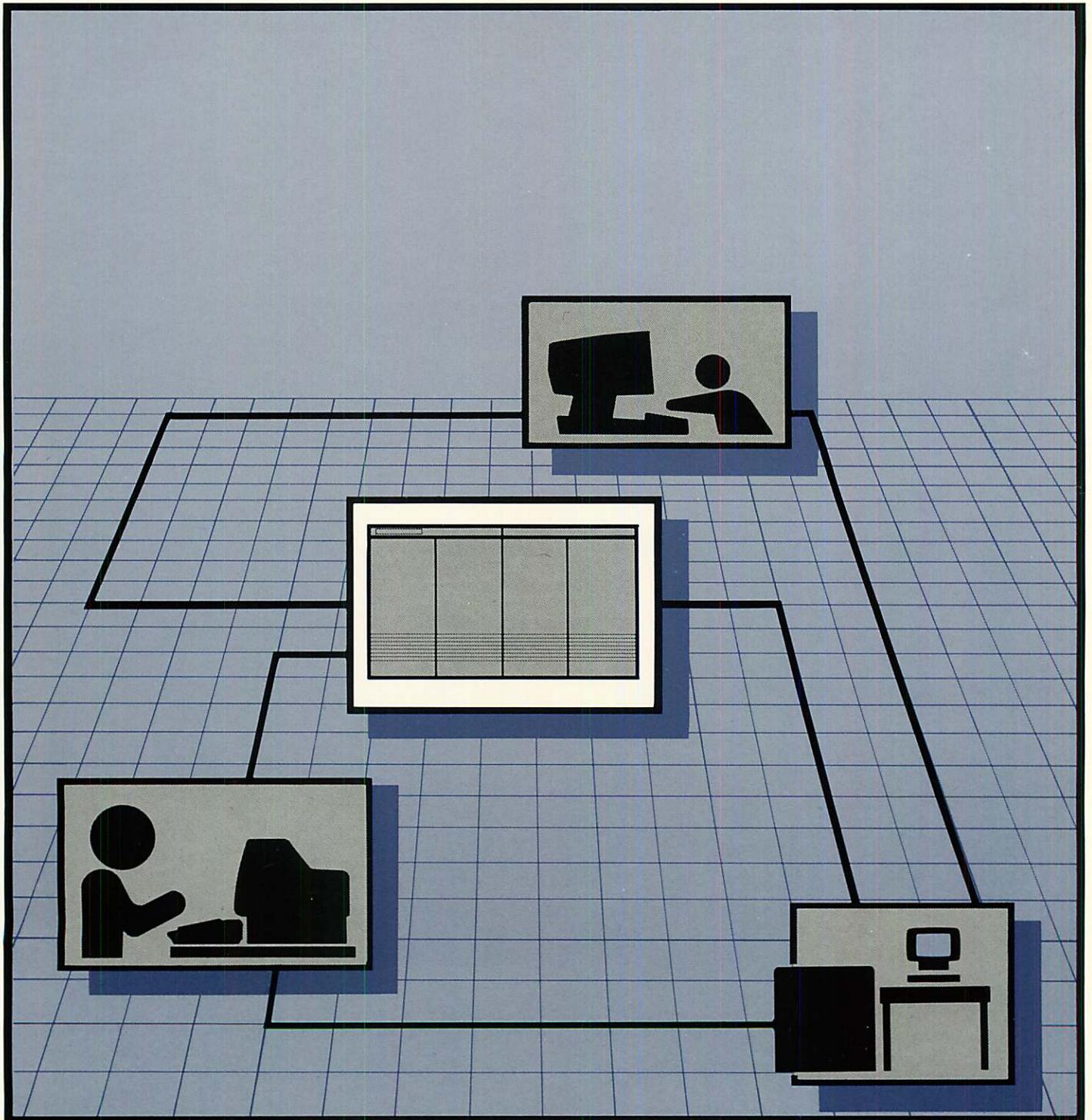


NS3000/V

Network Manager Reference Manual
Volume I



READER COMMENT SHEET

HP AdvanceNet

NS3000/V Network Manager Reference Manual
Volume I

32344-90002 MAY 87

We welcome your evaluation of this manual. Your comments and suggestions help us to improve our publications. Please explain your answers under Comments, below, and use additional pages if necessary.

Is this manual technically accurate?

Yes No

Are the concepts and wording easy to understand?

Yes No

Is the format of this manual convenient in size, arrangement, and readability?

Yes No

Comments:

This form requires no postage stamp if mailed in the U.S. For locations outside the U.S., your local HP representative will ensure that your comments are forwarded.

FROM:

Date _____

Name _____

Company _____

Address _____

FOLD

FOLD



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 1070 CUPERTINO, CA

POSTAGE WILL BE PAID BY ADDRESSEE

Publications Manager
Hewlett-Packard Company
Information Networks Division
1942 Homestead Road
Cupertino, Calif. 95014

FOLD

FOLD

HP AdvanceNet

NS3000/V
Network Manager Reference Manual

Volume I



**HEWLETT
PACKARD**

19420 Homestead Road, Cupertino, CA 95014

Part No. 32344-90002
E0587

Printed in U.S.A. JUN 1985
Edition 2, MAY 1987

NOTICE

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

HEWLETT-PACKARD MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS 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.

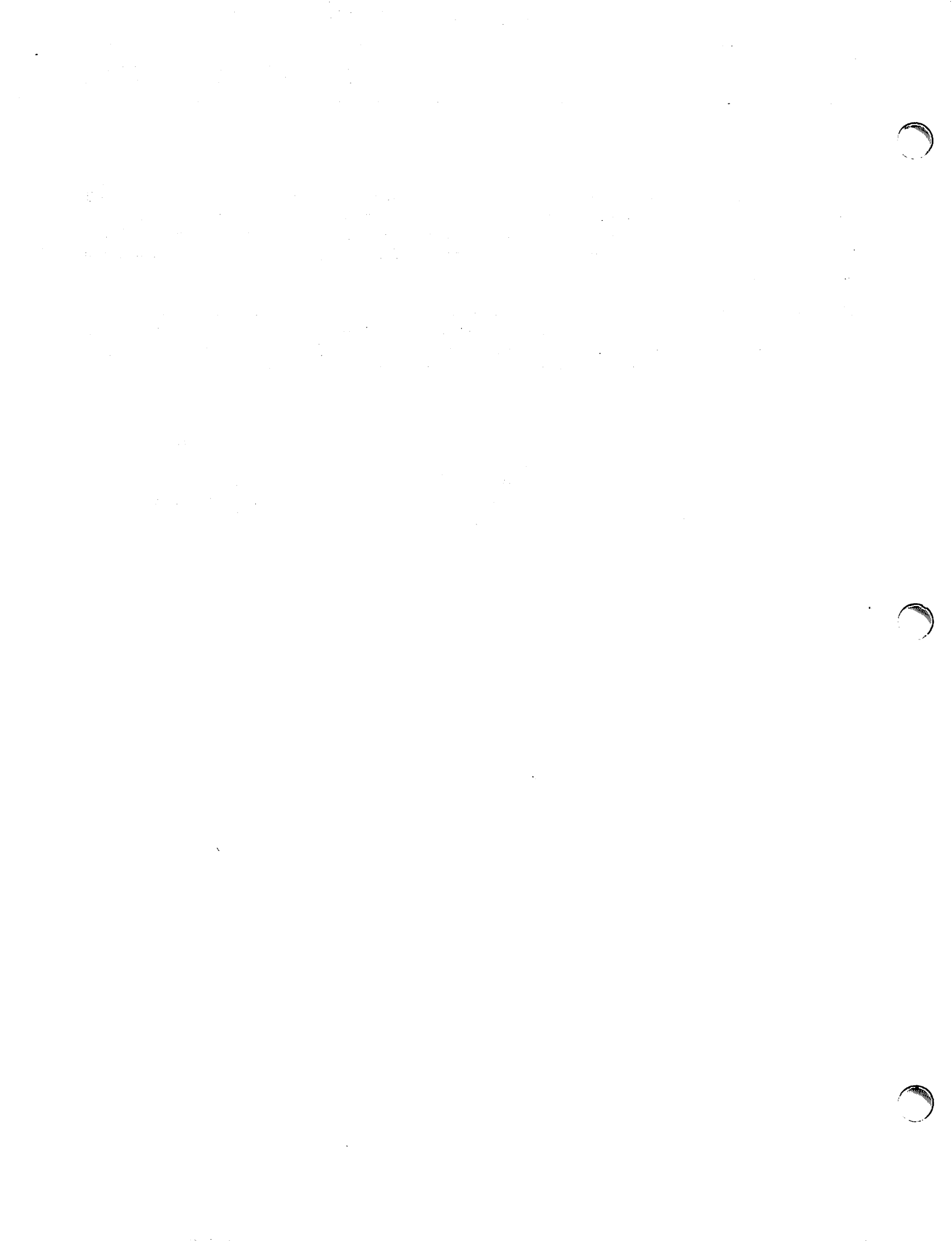
This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Hewlett-Packard Company.

PRINTING HISTORY

New editions are complete revisions of the manual. Update packages, which are issued between editions, contain additional and replacement pages to be merged into the manual by the customer. The dates on the title page change only when a new edition or a new update is published. No information is incorporated into a reprinting unless it appears as a prior update; the edition does not change when an update is incorporated.

The software code printed alongside the date indicates the version level of the software product at the time the manual or update was issued. Many product updates and fixes do not require manual changes and, conversely, manual corrections may be done without accompanying product changes. Therefore, do not expect a one to one correspondence between product updates and manual updates.

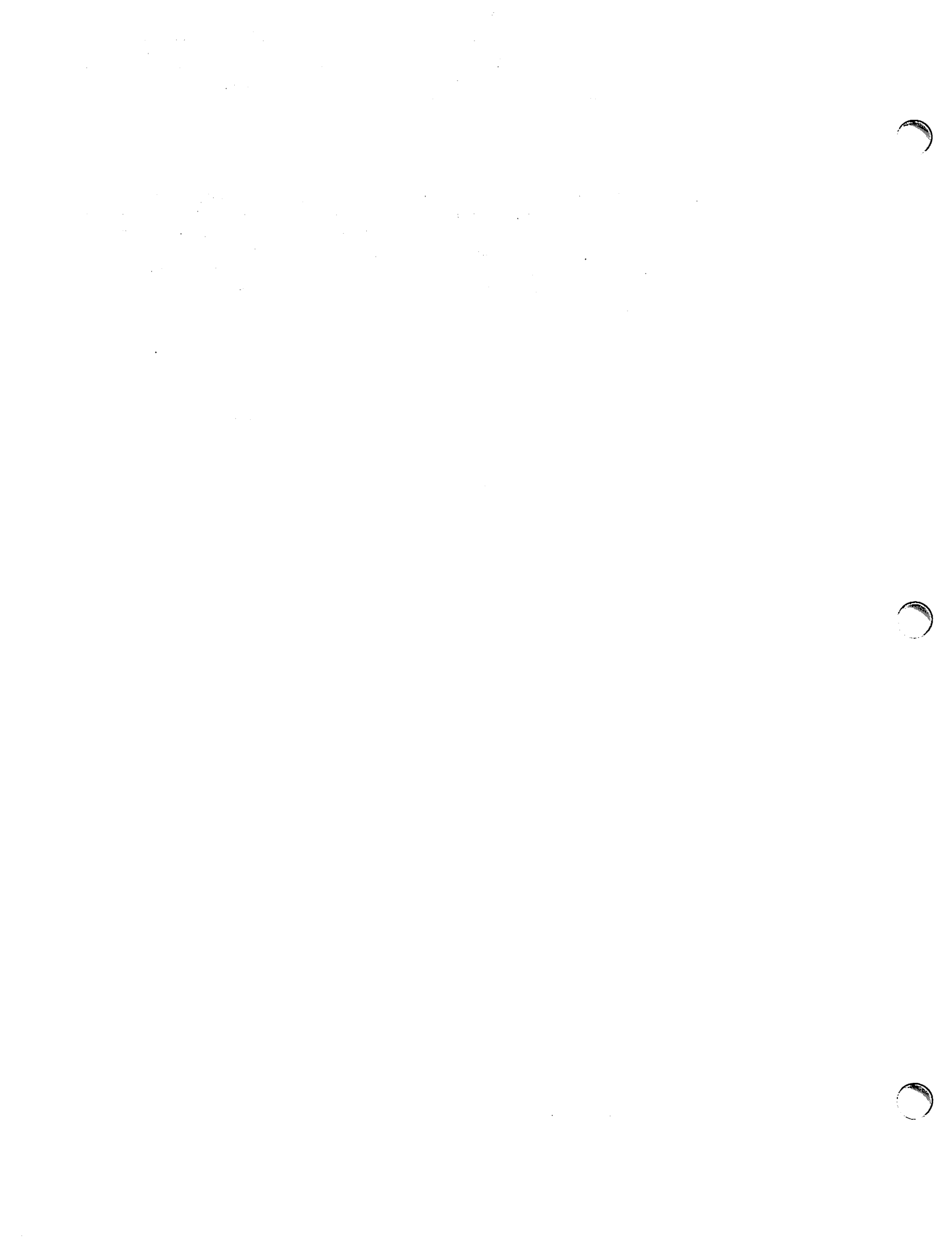
First Edition	JUN 1985.	32344A.00.00
Update 1.	NOV 1985.	32344A.00.00
Update 2.	JULY 1986.	32344A.00.00
Update 3.	NOV 1986.	32344A.00.02
Second Edition	MAY 1987.	32344A.00.04



LIST OF EFFECTIVE PAGES

The List of Effective Pages gives the date of the current edition and of any pages changed in updates to that edition. Within the manual, any page changed since the last edition is indicated by printing the date the changes were made on the bottom of the page. Changes are marked with a vertical bar in the margin. If an update is incorporated when an edition is reprinted, these bars are removed but the dates remain. No information is incorporated into a reprinting unless it appears as a prior update. To verify that your manual contains the most current information, check that the date printed at the bottom of the page matches the date listed below for that page.

Effective Pages	Date
all	MAY 1987



PREFACE

Hewlett-Packard AdvanceNet is a combination of hardware and software products that make it possible for Hewlett-Packard computer systems to communicate with one another and with IBM mainframes. The system to system or system to network connections can be made over the coaxial cable of a local area network, over hardwired or leased lines, over the public telephone facility, or across X.21 or X.25 compatible Packet Switching Networks (PSNs), in any mixture. This capability, coupled with remote-entry capability to IBM computer systems, provides a total solution to large-company electronic data processing (EDP) needs.

HP AdvanceNet allows a large multidivisional corporation to have a truly coordinated world-wide network of computer systems. They are coordinated in the sense that the various commercial and industrial functions within each division and factory are tied together; they are also coordinated in the larger sense of tying together the various divisions and factories at the corporate level.

For example, imagine a large corporation which has factories in the United States, Canada, France, and West Germany. Within each factory there are HP 3000 computer systems performing such functions as inventory control, factory data collection, and operations management. With Hewlett-Packard AdvanceNet data communications products, these manufacturing information systems can be connected to an HP 3000 system which handles the factory's administrative functions (such as finance and accounting). The administrative systems of each factory can, in turn, be connected not only to one another (via a local area network) but also (via remote job entry) to a large computer facility at corporate headquarters. This overall networking capability makes it possible to perform financial analysis and control at a group and corporate level as well as at the individual factories.

PREFACE (continued)

HP Network Services for MPE-V/E Based Systems (NS3000/V) is the HP data communications product that enables your HP 3000 to communicate with other HP computer systems as part of a distributed network. These systems can be other HP 3000s, HP 9000s, HP 1000s and PCs. Networks that operate over NS3000/V links can be interconnected to form a catenet, or internetwork. There are several network link products for NS3000/V, as described below.

The following link products connect computers on a local area network using the IEEE 802.3 networking standard:

- ThinLAN/3000 Link (includes ThickLAN option for thick coaxial cable)
- StarLAN/3000 Link

Two other link products enable you to establish remote connections to HP 3000s, as well as local connections, using point-to-point networking technology:

- Asynchronous SERIAL Network Link for MPE-V/E based systems (Asynchronous 3000/V Link)
- NS Point-to-Point Network Link for MPE-V/E based systems (NS Point-to-Point 3000/V Link).

Intended Audience of this Manual

This manual is intended for those with a good deal of knowledge in data communications. Also required is knowledge of the MPE-V operating system at the system supervisor level, and a familiarity with the SYSDUMP dialogue, resource management and console commands.

Related Publications

The following HP publications contain additional information about Network Services (NS3000/V), the MPE-V operating system, and the link products used with NS3000/V.

PREFACE (continued)

General NS3000/V Link Manuals:

- *NS3000/V Network Manager Reference Manual, Volume I* (32344-90002)
- *NS3000/V Network Manager Reference Manual, Volume II* (32344-90012)
- *NetIPC3000/V Programmer's Reference Manual* (5958-8581)
- *NS Message Formats Reference Manual* (5958-8523)

Network Services Manuals:

- *NS3000/V User/Programmer Reference Manual* (32344-90001)
- *NS Cross-System NFT Reference Manual* (5958-8563)
- *NS Cross-System Network Manager Reference Manual* (5958-8564)

HP ThickLAN Manuals:

- *LAN Cable and Accessories Installation Manual* (5955-7680) (For use with coaxial cable LAN links)
- *LAN3000/V Diagnostic and Troubleshooting Guide* (30242-90003)
(This manual is referred to as *LAN/3000 Diagnostic and Troubleshooting Guide* throughout this manual set.)
- *LAN Link Hardware Troubleshooting Manual* (5955-7681)

HP StarLAN Manuals:

- *HP StarLAN PC to HP 3000 Network Configuration Guide* (50906-90000)
- *HP StarLAN Planning Guide for PCs* (50906-90020)
- *HP StarLAN Hardware Installation Manual for PCs* (5959-2222)
- *HP StarLAN PC Server Installation, Configuration, and Operation Guide* (50904-90000)
- *HP StarLAN PC Workstation Installation and Configuration Guide* (50906-90040)
- *HP StarLAN User's Guide for PCs* (50905-90000)
- *HP StarLAN Diagnostics and Troubleshooting Manual for PCs* (50906-90060)
- *HP 28647A Bridge Installation and Reference Manual* (28647-90001)
- *HP 30265A StarLAN/3000 Link Installation and Reference Manual* (30265-90001)

PREFACE (continued)

HP ThinLAN Manuals:

- *HP30240A ThinLAN/3000 Local Area Network Interface Controller (LANIC) Installation and Service Manual (30240-90001)* (For Series 37/MICRO3000 systems, part number 30240-90100).
- *PC to HP 3000 Network Configuration Guide (50909-90000)*
- *HP ThinLAN Planning and Hardware Guide for PCs (50909-90020)*
- *HP ThinLAN PC Server Installation, Configuration, and Operation Guide (50907-90000)*
- *HP ThinLAN Workstation Installation and Configuration Guide for PCs (50909-90040)*
- *HP ThinLAN User's Guide for PCs (50908-90000)*
- *HP ThinLAN Diagnostics and Troubleshooting Manual for PCs (50909-90060)*
- *HP28645A ThinLAN Hub Installation Manual (28645-90001)*

HP SERIAL Manuals:

- *HP SERIAL Network PC to HP 3000 Network Configuration Guide (50911-90000)*
- *HP SERIAL Network Planning and Hardware Guide (50911-90020)*
- *HP SERIAL Network PC Workstation Installation and Configuration Guide (50911-90040)*
- *HP SERIAL Network User's Guide (50910-90000)*
- *HP SERIAL Network Troubleshooting Guide (50911-90060)*

Resource Sharing Manuals:

- *Resource Sharing: System Management (32597-90001)*
- *Resource Sharing: Utilities (32597-90002)*
- *Resource Sharing: Host Diagnostics (32597-90003)*
- *Resource Sharing: Tape Backup User's Guide (35460-90902)*
- *Resource Sharing: Tape Backup Administration (35460-90903)*

PREFACE (continued)

You may also wish to consult the following DS and DS-related reference manuals:

- *DS/3000 HP 3000 to HP 3000 User/Programmer Reference Manual (32185-90001)*
- *DS/3000 HP 3000 to HP 1000 Reference Manual for HP 3000 Users (32185-90005)*
- *DS/3000 HP 3000 to HP 3000 Network Administrator Manual (32185-90002)*
- *X.25 Link for the HP 3000 Reference Manual (32187-90001)*
- *DS/1000-IV User's Manual (91750-90002)*

These additional reference manuals provide documentation for the MPE operating system and several subsystems available on the HP 3000:

- *Fundamental Data Communications Handbook (5957-4634)*
- *HP 3000 Computer Systems, MPE V Commands Reference Manual (32033-90006)*
- *HP 3000 Computer Systems, MPE V Intrinsic Reference Manual (32033-90007)*
- *HP 3000 Computer Systems, MPE V System Operation and Resource Management Reference Manual (32033-90005)*
- *IMAGE/3000 Reference Manual (32215-90003)*
- *QUERY/3000 Reference Manual (30000-90042)*
- *KSAM/3000 Reference Manual (30000-90079)*
- *TurboIMAGE Reference Manual (32215-90050)*
- *V/3000 Reference Manual (32209-90001)*
- *MPE File System Reference Manual (30000-90236)*
- *Workstation Configurator Reference Manual (30239-90001)*

INP Manuals:

- *HP 30020A INP Installation and Service Manual (30010-90001)*
- *HP 30020B INP Installation and Service Manual (30020-90005)*
- *HP 30244M INP Series 37 Installation and Service Manual (30244-90002)*

PREFACE (continued)

ATP Manuals:

- *Point-To-Point Workstation I/O Reference Manual (30000-90250)*
- *Terminal (TERMDSM) On-Line Diagnostic/Support Monitor Reference Manual (For MPE V/E: 30144-90013)*
- *HP 3000 Distributed Systems Network/Advanced Terminal Processor Off-line Diagnostic Procedures Manual (30144-90003)*
- *Asynchronous Data Communications Channel-Main and Asynchronous Data Communications Channel-Extended Diagnostic Manual (30070-90037)*
- *Advanced Terminal Processor (ATP) Installation Manual (30144-90002)*

Organization of the Manual

This manual is divided into two volumes. Volume I, which describes network design and configuration, contains the following sections:

Section 1, Introduction, of this manual introduces the network architecture and product structure of NS3000/V and associated links and describes each of the products in detail.

Section 2, Network Management, provides an overview of the tasks of network management. This section also provides references to other sections that cover certain areas of network management in greater detail.

Section 3, Network Planning and Configuration, explains concepts you will need to understand before planning, configuring, and installing an NS3000/V network or catenet.

Section 4, System Configuration, discusses changes and additions to your original system configuration which may become necessary due to changing circumstances at your installation. This section includes a detailed explanation of I/O configuration for the drivers and virtual terminals. System parameters and the SYSDUMP dialogue are also discussed.

Section 5, the Node Management Configurator (NMMGR), describes the operation of NMMGR, a utility program that provides a series of VPLUS/3000 block-mode screens to display and accept configuration information. The operation of NMMGR and the specifics of the utility screens are described.

PREFACE (continued)

Sections 6, 7, 8, 9, 10, 11, 12, and 13 provide the field definitions of the configuration screens used to define the network configuration. These sections are organized as follows:

- Section 6, Guided Configuration
- Section 7, Link Configuration
- Section 8, Network Transport Configuration
- Section 9, LAN 802.3 Network Interface Configuration
- Section 10, Router Network Interface Configuration
- Section 11, Gateway Half Network Interface Configuration
- Section 12, Loopback Network Interface Configuration
- Section 13, Logging Configuration

Section 14, Network Directory, describes how to create and maintain a master network directory of your installation's network configuration.

Appendix A contains blank configuration worksheets to help you prepare for configuring your network as described in Volume I, Section 3, "Network Planning and Configuration."

Appendix B lists the supported modems for the NS3000/V product.

Appendix C describes how to convert configuration files.

Appendix D describes PC-to-HP 3000 communication.

Appendix E discusses NS versus DS INP configuration.

Volume II, which describes tasks performed after initial network configuration, contains the following sections:

Section 1, Commands, describes the MPE commands for NS3000/V link products.

Section 2, Software and Line Verification, describes both the utilities available for software verification and the line tests used to check that a node is communicating correctly with a network.

Section 3, Logging and Tracing, describes the NMS Trace/Log File Analyzer (NMDUMP).

Section 4, Changing the Network, describes how to change the network topology.

A glossary also is provided. For your convenience, the glossary is included with both volumes of this manual.



CONVENTIONS USED IN THIS MANUAL

NOTATION **DESCRIPTION**

nonitalics Words in syntax statements which are not in italics must be entered exactly as shown. Punctuation characters other than brackets, braces and ellipses must also be entered exactly as shown. For example:

EXIT;

italics Words in syntax statements which are in italics denote a parameter which must be replaced by a user-supplied variable. For example:

CLOSE *filename*

[] An element inside brackets in a syntax statement is optional. Several elements stacked inside brackets means the user may select any one or none of these elements. For example:

$\left[\begin{array}{l} A \\ B \end{array} \right]$ User *may* select A or B or neither.

{ } When several elements are stacked within braces in a syntax statement, the user must select one of those elements. For example:

$\left\{ \begin{array}{l} A \\ B \\ C \end{array} \right\}$ User *must* select A or B or C.

... A horizontal ellipsis in a syntax statement indicates that a previous element may be repeated. For example:

[, *itemname*] ... ;

In addition, vertical and horizontal ellipses may be used in examples to indicate that portions of the example have been omitted.

■ A shaded delimiter preceding a parameter in a syntax statement indicates that the delimiter *must* be supplied whenever (a) that parameter is included or (b) that parameter is omitted and any *other* parameter which follows is included. For example:

itema [■ *itemb*] [■ *itemc*]

means that the following are allowed:

itema
itema, itemb
itema, itemb, itemc
itema, , itemc

CONVENTIONS (continued)

Δ When necessary for clarity, the symbol Δ may be used in a syntax statement to indicate a required blank or an exact number of blanks. For example:

```
SET[(modifier)] $\Delta$ (variable);
```

underlining When necessary for clarity in an example, user input may be underlined. For example:

```
NEW NAME? ALPHA
```

Brackets, braces or ellipses appearing in syntax or format statements which must be entered as shown will be underlined. For example:

```
LET var[[subscript]] = value
```

Output and input/output parameters are underlined. A notation in the description of each parameter distinguishes input/output from output parameters. For example:

```
CREATE (parm1,parm2,flags,error)
```



Shading represents inverse video on the terminal's screen. In addition, it is used to emphasize key portions of an example.



The symbol  may be used to indicate a key on the terminal's keyboard. For example, RETURN indicates the carriage return key.

CONTROLchar

Control characters are indicated by CONTROL followed by the character. For example, CONTROLY means the user presses the control key and the character Y simultaneously.

CONTENTS

Section 1

INTRODUCTION

System Requirements	1-2
Network Architecture	1-3
The OSI Model	1-4
Types of Networks	1-5
NS3000/V Network Types	1-5
Network Topology	1-6
Catenets	1-7
Gateways and Gateway Halves	1-8
NS3000/V Architecture	1-9
Protocols	1-10
OSI Layer 4 (Transport Layer) Protocols	1-11
OSI Layer 3 (Network Layer) Protocols	1-11
OSI Layer 2 (Data Link Layer) Protocols	1-12
OSI Layer 1 (Physical Layer) Protocols	1-12
Auxiliary Protocols	1-13
Network Links	1-14
Common Link Software	1-14
IEEE 802.3 Links	1-15
Medium Access Method for IEEE 802.3 Links	1-18
Hardware Components	1-18
Link Level Software	1-19
NS Point-to-Point 3000/V Link	1-20
Direct Connect Links	1-21
Dial Links	1-22
Leased Lines	1-22
Hardware and Cables for Dial Links and Leased Lines	1-22
Asynchronous SERIAL Network Link	1-22
Hardware and Cabling	1-23
Link Level Protocol	1-24
Optional DS-Compatible Links	1-24
Personal Computers as NS3000/V Nodes	1-25
NS3000/V Network Services	1-26
Services Available	1-26

Section 2

NETWORK MANAGEMENT

Network Management Tasks	2-2
The Network and Catenet Management Lifecycle	2-3
Network Management Tools	2-3
MPE Commands and Utilities	2-4
Node Management Services	2-5
CS/3000 Utilities	2-6
Link Level Tools and Utilities	2-6

CONTENTS (continued)

Installing NS3000/V Links	2-7
Customer Installation Tasks for All NS3000/V Links	2-7
Additional Tasks for IEEE 802.3 Links	2-9
HP Installation Tasks	2-9
Installing Network Services	2-10
Configuration and Initialization Overview	2-10
Network and Configuration Planning	2-13
System Configuration	2-13
Network Configuration with NMMGR	2-14
Configuration Verification	2-14
Network Directory	2-15

Section 3

NETWORK PLANNING AND CONFIGURATION

Software Components	3-2
NS3000/V Software Subsystems	3-2
Configuration Files	3-2
Configuration Concepts	3-3
NS Routing	3-4
Intranet Routing	3-4
Internet Routing	3-5
Symbolic Names	3-6
Node Names	3-6
Other Names	3-7
Network Addresses	3-8
IP Address Format and Assignment	3-8
IEEE 802.3 Station Address Format and Assignment	3-10
Address Resolution	3-10
Node Name to IP Address Resolution	3-10
IP to Subnet Address Resolution	3-12
Configuration Terminology	3-13
General Terms	3-13
Dial Link Terms	3-13
Router Network Terms	3-14
Gateway Terms	3-15
Non-Operational Links	3-16
Router Network Automatic Rerouting	3-16
Internet Redirection	3-19
Network Installation and Administration	3-23
Planning	3-24
Software and Hardware Installation	3-24
Configuration	3-25
SYSDUMP Configuration	3-26
NMMGR Configuration	3-26
Nodal Validation, Verification, and Synchronization	3-27

CONTENTS (continued)

Network Startup	3-28
Line Verification	3-28
Network and Catenet Design Considerations	3-29
Line Speed	3-29
Geographical Location	3-29
Special Cases	3-30
Dial Links	3-30
Personal Computers	3-30
Other Non-HP 3000 Nodes	3-30
DS-Compatible Links	3-30
Network Interfaces and Design	3-31
Number of Network Interfaces	3-31
Gateways	3-31
Network Boundaries	3-32
Network Implementation and Support Plan	3-33
Network Maps and Configuration Worksheets	3-33
Configuration Worksheets: Terminology	3-36
Configuration Worksheets: Instructions	3-38
Catenet Worksheets	3-39
Catenet Map	3-39
Communication Between Networks	3-39
Network Boundaries	3-40
IP Network Addresses	3-40
Completing the Catenet Table	3-41
Network Worksheets	3-43
LAN Network Worksheets	3-44
Router Network Worksheets	3-47
Gateway-Half Pair Worksheets	3-53
Node Worksheets	3-57
LAN Node Internet Routing	3-59
Router Node Routing Information	3-62
Gateway Half Information for Node Worksheets	3-69

Section 4

SYSTEM CONFIGURATION

System Configuration	4-2
I/O Configuration	4-3
Type 16, Subtype 0, 8 -- Virtual Terminals	4-9
Type 17, Subtype 9 -- LANIC Driver	4-9
Type 17, Subtype 0, 1, 3 -- INP Driver	4-10
Type 41, Subtype 0, 1 -- Communications Drivers	4-13
Type 42, Subtype 0, 1, 2 -- ATP Devices	4-14
Recommendations for System Parameters	4-15
Virtual Terminal Configuration Dialogue	4-19
LANIC Configuration Dialogue	4-21
INP Configuration Dialogue	4-22
Device Driver (IOINP0)	4-22
Communications Drivers (IODS0 and IODSX)	4-25

CONTENTS (continued)

ATP Configuration Dialogue	4-27
Completing the SYSDUMP Dialogue	4-30
Configuration Examples	4-34

Section 5

THE NMS CONFIGURATOR (NMMGR)

Getting Started with NMMGR	5-2
The Open Configuration/Directory File Screen.	5-3
Specifying the Configuration File Name	5-5
Opening or Creating the Configuration File	5-6
The Main Menu Screen.	5-6
Getting Help	5-7
NMMGR Screen Structure.	5-8
Configuration Files	5-9
Using NMMGR Configuration Screens.	5-12
General Operation of Screens.	5-12
The Header and Message Lines	5-13
Data Flag.	5-13
Path Name.	5-13
File Name	5-14
Command Window and the Enter Key	5-14
Screen Fields.	5-17
Prior Screen Key	5-18
Refresh Screen Key	5-19
Menu Screens	5-19
Select Screens.	5-20
Data Screens.	5-23
Using NMMGR Utility Screens.	5-26
Output Configuration File.	5-27
Print Tree and Display Tree	5-28
Print Data	5-30
Print Summary	5-30
Print Subtree	5-33
Compress Configuration File	5-33
Validate Configuration File	5-35
Configuration Subtree Copy.	5-40
The Error Information Screen.	5-43
Copying Configuration Data	5-46
Making Configuration Changes	5-48

Section 6

GUIDED CONFIGURATION

Correcting Configuration Errors.	6-4
Netxport Configuration	6-5
Netxport Update.	6-13

CONTENTS (continued)

Section 7

LINK CONFIGURATION

Link Configuration	7-3
Link Configuration: LAN802.3 Link Data	7-6
Link Configuration: LAN802.3 Link Trace Data	7-8
Link Configuration: BSC Link Data	7-11
Link Configuration: BSC Link Trace Data	7-14
Link Configuration: BSC Link Phone Data	7-17
Link Configuration: LAP-B Link Data	7-19
Link Configuration: LAP-B Link Trace Data	7-22
Link Configuration: LAP-B Link Phone Data	7-25
Link Configuration: ASNP Link Data	7-27
Link Configuration: ASNP Link Trace Data	7-29
Link Configuration: ASNP Link Phone Data	7-32

Section 8

NETWORK TRANSPORT CONFIGURATION

Network Transport Configuration Selection	8-3
Node Configuration	8-4
Node Name Configuration	8-5
Global Transport Configuration	8-7
General Protocol Configuration	8-10
Internet Protocol Update Configuration	8-11
Packet Exchange Protocol (PXP) Configuration	8-14
Transmission Control Protocol (TCP) Configuration	8-17
Network Interface Configuration	8-21

Section 9

LAN802.3 NETWORK INTERFACE CONFIGURATION

LAN802.3 Network Interface Configuration	9-3
Protocol Configuration	9-6
Internet Protocol Configuration	9-7
Probe Protocol Configuration	9-10
LAN802.3 Network Interface Link	9-13
Lan Link Configuration	9-15
Neighbor Gateways	9-17
Neighbor Gateway Reachable Networks	9-19
LAN802.3 Mapping Configuration	9-22
Static Neighbor Node Configuration (LAN802.3)	9-24

CONTENTS (continued)

Section 10

ROUTER NETWORK INTERFACE CONFIGURATION

Router Network Interface Configuration	10-3
Router Network Interface Protocol Configuration	10-7
Internet Protocol Configuration	10-8
Dial ID Protocol Configuration	10-11
Security String(s) Configuration	10-14
Router Network Interface Links	10-16
Direct Connect Link Configuration	10-19
Router Dial Link Configuration	10-21
Neighbor Gateways	10-23
Neighbor Gateway Reachable Networks	10-25
Router Mapping Configuration	10-28
Router Reachable Nodes	10-32

Section 11

GATEWAY HALF NETWORK INTERFACE CONFIGURATION

Gateway Half Network Interface Configuration	11-3
Protocol Configuration	11-6
Internet Protocol Configuration	11-7
Dial ID Protocol Configuration	11-10
Security String(s) Configuration	11-13
Gateway Half Network Interface Link	11-15
Direct Connect Link Configuration	11-17
Gateway Half Dial Link Configuration	11-19
Neighbor Gateways	11-22
Neighbor Gateway Reachable Networks	11-24

Section 12

LOOPBACK NETWORK INTERFACE CONFIGURATION

Loopback Network Interface Configuration	12-2
Protocol Configuration	12-4
IP Protocol Configuration	12-5

Section 13

LOGGING CONFIGURATION

Logging Subsystems Selection	13-4
Logging Classes Selection	13-6
Logging Class Data	13-8

CONTENTS (continued)

Section 14

NETWORK DIRECTORY

What a Network Directory Provides	14-2
Path Report Lists.	14-2
Global and Local Entries.	14-3
Roles and Interfaces.	14-4
Configuration Screens	14-6
Network Directory Main Screen	14-7
Select Node Name Screen	14-9
Network Directory Data Screen	14-11
Directory Maintenance Mode Interface	14-14
OPENDIR Command	14-15
DELETENODE Command.	14-15
MERGEDIR Command.	14-16
LISTDIR Command	14-17
EXPANDDIR Command	14-17
HELP Command	14-18
:MPE Command	14-18
EXIT Command	14-19
MAKESTREAM Command	14-19
LISTDIR Command Sample Output.	14-22

Appendix A

WORKSHEETS

Appendix B

SUPPORTED MODEMS

Appendix C

CONVERTING CONFIGURATION FILES

Using the Conversion Program	C-1
--	-----

CONTENTS (continued)

Appendix D

PC-TO-HP 3000 COMMUNICATION

Requirements for ThinLAN/3000, StarLAN/3000, SERIAL links	D-2
Software Required	D-2
HP 3000 Server Software	D-2
HP 3000 Host Software	D-2
Software for a PC Workstation Using Server Resources	D-2
Software for a PC Workstation Used as a Terminal	D-3
Related Publications	D-4
Hardware and Software Installation	D-5
For HP 3000s	D-5
For PC Workstations	D-6
HP 3000 Logon and Shortname Correspondence	D-6
Configuration Procedures Summary	D-7
PC Workstation Tasks	D-7
Configuring the HP 3000	D-8
Configuring Additional Virtual Terminals	D-8
Configuring the HP 3000 Network Config. File (NSCONF.NET.SYS)	D-9
Assigning HP 3000 Logons	D-15

Appendix E

DS vs NS INP Configuration

Glossary

HP Network Services for MPE-V Based Systems (NS3000/V) is an HP data communications product that provides networking capabilities to interactive users and application programs on HP 3000s running the MPE-V operating system. Through the use of NS3000/V, these HP 3000s can be connected to other HP computer systems in a distributed network.

NS3000/V consists of two parts: NS3000/V Services and NS3000/V links. NS3000/V Network Services consist of software that enables users to access data, initiate processes, and exchange information among all the systems on a network. NS3000/V links provide connections among systems (either HP 3000s or personal computers) in the same network. To use NS3000/V Services, the systems must be connected by an NS3000/V network link.

A variety of network link products are available with NS3000/V. The link product that connects individual systems in an NS3000/V network can be any of the following:

- **NS Point-to-Point Network Link for MPE-V Based Systems (NS Point-to-Point 3000/V Link)**
- **Asynchronous SERIAL Network Link**
- **StarLAN/3000 Link**
- **ThinLAN/3000 Link (includes ThickLAN option for thick coaxial cable, described below)**

The link products listed above can all be used to connect HP 3000s to one another.

The Asynchronous SERIAL Network Link, StarLAN/3000, and ThinLAN/3000 can connect HP 3000s to personal computers as well as to other HP 3000s.

The ThinLAN/3000 Link, including the ThickLAN option, can also connect HP 3000s with HP 1000s and HP 9000s.

ThinLAN/3000 Link connections are usually made with thin (.18 inch) coaxial cable; however, you can also use thicker (.4 inch diameter) coaxial cable, available by ordering the ThickLAN option of ThinLAN/3000.

Table 1-1 shows available links and the kinds of connections they can make-- whether between HP 3000s or between HP 3000s and personal computers.

Table 1-1. Link Types and Connections

Link Type	3000 to 3000	PC to 3000
NS Point-to-Point 3000/V Link	X	
Asynchronous SERIAL Network Link	X	X
ThinLAN/3000 Link (including ThickLAN option)	X	
StarLAN/3000 Link	X (MICRO 3000s, MICRO 3000XEs, Series 37s, and Series 37XEs only)	X

Although NS3000/V Services all require a network link to operate, network links can be purchased without the concurrent purchase of NS3000/V Services.

Network links differ in their supporting hardware, software and in some cases, function. Later subsections of this "Introduction" describe these links and discuss the differences among them.

SYSTEM REQUIREMENTS

NS3000/V is supported on the HP 3000 Series 37/37XE/39/40/42/44/48/58/64/68/70 and the MICRO 3000 and MICRO 3000XE, executing the MPE-V/E operating system, V.U.F. G.02.03 (U-B-delta-3) MIT or later versions. The system must have a minimum of two megabytes of memory and the Expanded System Table Microcode. (Systems that are now memory-limited should add one megabyte to maintain current performance.)

NETWORK ARCHITECTURE

Before you understand the details of NS3000/V links and services, you should understand some general concepts about network architecture and NS3000/V. This section will familiarize you with concepts and terms you will encounter later in this manual.

A network is a group of computer systems connected in such a way that they can exchange information and share resources. In a distributed network, as opposed to a centralized one, the connected systems are independent and equal. One system does not control another system.

NS3000/V networks are distributed networks. Systems that are configured into an NS 3000 network are called nodes. Through participation in a distributed network, users on your system, or local node, can use the processing and storage facilities of another system, or remote node; users at remote nodes can take advantage of the resources of your local node.

A group of networks that are connected to each other is called a catenet. One network is connected to another by means of a node called a gateway node.

The plan that defines the characteristics and interactions of the hardware and software used to connect nodes into a network is called a network architecture. Typically, the software is organized as a series of layers. The user interface is integrated into the top layer and the hardware is integrated into the lowest layer. Hence, a message, composed of data and information necessary to transmit the data to its destination, is sent from the user down through the layers and out onto the network; when the message is received at the remote node, it is passed up through the layers to the remote user.

Layers are required to handle the many tasks involved in translating a message into a form appropriate for the hardware connection to the network, or back into a form understandable to the remote user, depending on whether the message is incoming or outgoing. Each of the layers between the user and the hardware is assigned certain well-defined tasks. Each layer must accomplish its task and pass the message on, in a particular format, to the layers above or below it.

The rules and conventions that define the functions to be performed and the format of messages that are exchanged by each architectural layer are called protocols. Individual layers can be designed, implemented, changed, or updated in any manner their creators choose, as long as they provide the data in the correct format. This also makes it easy to pinpoint and correct errors, because each task is done in a specific layer of the architecture.

Until recently, each computer products company developed its own network architecture as part of the design of its data communications products. For example, Hewlett-Packard developed the Distributed Systems Network (DSN) architecture, a five layered design that uses HP proprietary protocols. The DSN architecture is used by all HP Distributed System Network products, such as DS Network Services for the HP 3000 (DS/3000) and DS/1000-IV. Similarly, IBM developed the System Network Architecture (SNA), a six layered design that uses IBM proprietary protocols. Many HP data communications products can communicate in an SNA environment, such as SNA Link Services for the HP 3000 (SNA Link) and Network Remote Job Entry for the HP 3000 (SNA NRJE).

However, using proprietary protocols and designs can be limiting for data communications applications. Over time, standards have been developed for the tasks and protocols of data communications, starting with the physical connectors. An internationally accepted set of standards based on an architecture known as the "OSI model" is under development by participants from many countries.

The OSI Model

The International Standards Organization (ISO), an agency of the United Nations, developed the first step in the standardization of network architectures by defining the **Open Systems Interconnection (OSI) Reference Model**. The OSI model defines seven architectural layers and specifies the function of each. Figure 1-1 illustrates the OSI model.

Layer	Task
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Figure 1-1. The Seven Layers of the OSI Model

- **Layer 7 (Application)** is the user interface to remote services.
- **Layer 6 (Presentation)** manipulates user data, such as in text compression and encryption.
- **Layer 5 (Session)** negotiates connection establishment at remote nodes.
- **Layer 4 (Transport)** is responsible for end-to-end data integrity. This means that the Transport Layer is responsible for ensuring that the message arrives at the correct remote node, without errors, even if the message had to pass through any intermediate nodes.

Layers 5 - 7 also provide end-to-end services, while Layers 1 - 3 are only responsible for data integrity between each node.

Layer 4 protocols can provide the following services to upper layers: in-order message delivery, retransmission of lost messages, suppression of duplicate messages and flow control.

- **Layer 3 (Network)** determines the routes messages take to get from one node to another. This layer can be split into two sub-layers: 3i and 3s. Layer 3i handles routing *between* networks (internetwork), and 3s handles routing *within* a network (intranetwork).
- **Layer 2 (Data Link)** checks for and corrects transmission errors over the physical link.
- **Layer 1 (Physical)** transmits the electrical signals over the link.

The functions of each layer are performed by software that adheres to established protocols. The protocols used by NS3000/V are described later in this section.

Types of Networks

Computer networks can be broadly classed as of two types: broadcast networks and point-to-point networks. Nodes on a broadcast network share the same communications channel, over which data is transmitted to all the nodes in the network. Networks using HP ThinLAN, including the ThickLAN option, or HP StarLAN links are broadcast networks; the protocol that they use *broadcasts* messages to all the systems on the LAN.

Point-to-point networks, on the other hand, are networks in which data is transmitted from node to node in a network over a defined route until it reaches a specific destination. Because data is passed from one node to another, one node at a time, the means of transmitting data over point-to-point networks is called the store and forward technique. When a message is received at an intermediate node, it is forwarded to either another intermediate node or to its final destination. Point-to-point networks are sometimes referred to as router networks. The term *router* is used within this manual to refer to point-to-point networks. The Point-to-Point 3000/V Link and the Asynchronous SERIAL Network Link can both be used to connect nodes in a router network.

NS3000/V Network Types

An NS3000/V network can be of two types:

- A router network
- An IEEE 802.3 local area network

These types correspond to the types of networks--broadcast and point-to-point --previously described. The NS3000/V IEEE 802.3 local area network is a broadcast network based on standards published by the Institute of Electrical and Electronics Engineers (IEEE). The standards are called "IEEE 802.3" (and a related standard is called IEEE 802.2); therefore, the kind of network it specifies is called an "IEEE 802.3 network."

The NS3000/V router network is a point-to-point network that uses the store-and-forward technique.

Certain NS3000/V link types can be used for each network type, as shown in Table 1-2:

Table 1-2. Network and Link Types

NS3000/V Network Type	NS3000/V Link Type
Router	NS Point-to-Point 3000/V Link Asynchronous SERIAL Network Link
IEEE802.3	ThinLAN/3000 Link (including ThickLAN option) StarLAN/3000 Link

As Table 1-2 shows, NS3000/V router networks can use NS Point-to-Point 3000/V and Asynchronous SERIAL Network Links to connect nodes. IEEE 802.3 networks can use the ThickLAN option, ThinLAN/3000, and StarLAN/3000 Links.

Network Topology

The topology of a network refers to the physical arrangement of its nodes. For example, one type of common topology is a bus topology, in which all nodes are directly linked. Another type is a star topology, in which all nodes are linked in a radiating fashion to a central node or switching device.

The possible topologies for a given network are determined by the type of link used to connect the network's nodes.

For example, a bus topology can be used only for a broadcast network, such as an IEEE 802.3 network.

Figure 1-2 shows a bus topology, in which network nodes (represented by numbered circles) are joined to a common bus.

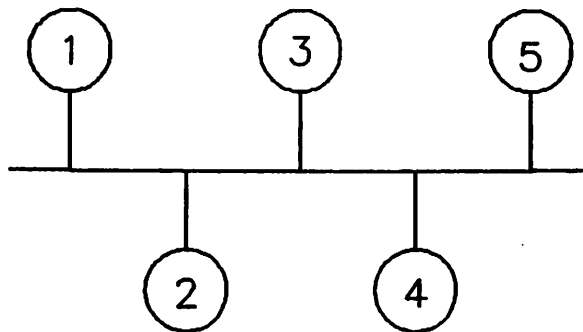


Figure 1-2. Bus topology.

Point-to-point networks cannot use a bus topology. Instead, point-to-point networks must use a topology in which each network node is connected to at least one other node. Data is passed from one node to another, including through any intermediate nodes, until it reaches its destination. NS Point-to-Point 3000/V and Asynchronous SERIAL Network Links can be used to create point-to-point, or router networks.

The actual topologies that can be used for point-to-point networks are widely varying; possibilities include star, ring, hierarchical (sometimes referred to as a tree topology) and string. Any arrangement of nodes will work as long as each node is connected to at least one other node in the same network. Figure 1-3 illustrates several possible topologies for point-to-point networks.

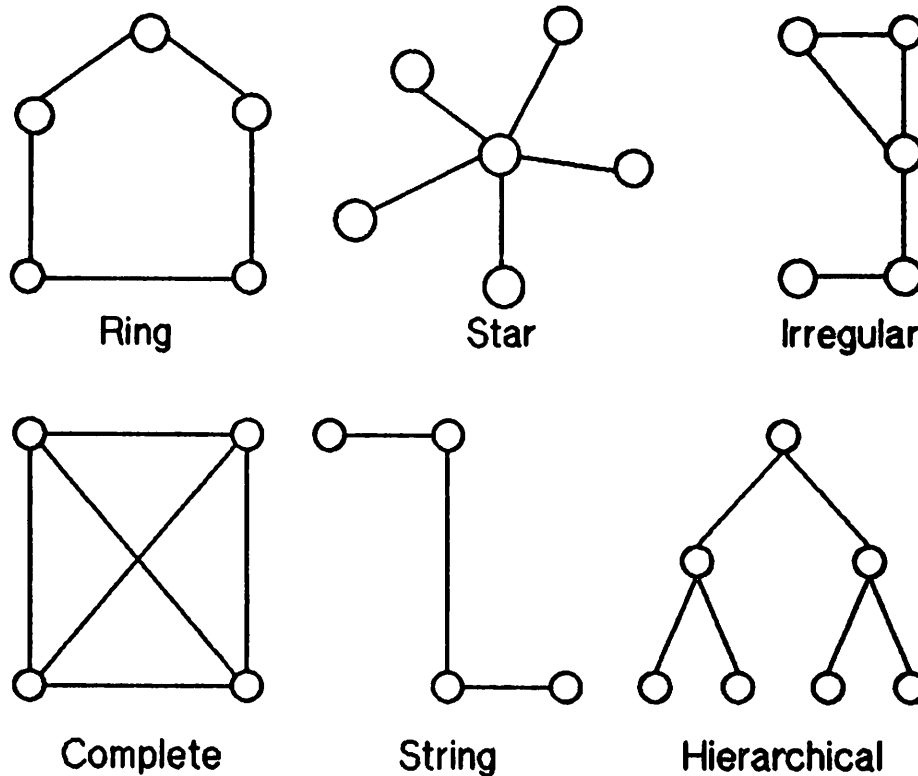


Figure 1-3. Point-to-point topologies.

Nodes that are directly connected to only one other node in point-to-point networks are referred to as *leaf nodes*. In the illustration above, each of the endpoints of the star topology are leaf nodes, as are some of the nodes in the string, hierarchical, and irregular topologies. In NS3000/V networks, personal computers can be used only as leaf nodes.

Catenets

Two or more networks can be linked together to form an internetwork or *catenet* (derived from *concatenated networks*). For example, if you wanted to connect the nodes in a router network with the nodes in an IEEE 802.3 network, the combination of the two networks would be called a catenet. Creation of a catenet allows any node on one network to communicate with any node on another network that is part of the same catenet. Up to 256 individual networks can belong to the same NS3000/V catenet.

The divisions between the networks in a catenet are called *network boundaries*. Figure 1-4 shows a catenet, with a network boundary indicated by a dashed line.

Gateways and Gateway Halves

Networks in the same internetwork are joined together by gateway nodes. A gateway node is a node that is a member of two or more networks and allows communication between the networks to which it belongs. Communication between networks is also called internetwork communication. For example, in Figure 1-4, Node 11 belongs to Network C and to Network D; it serves as a gateway between Networks C and D. Internetwork protocols determine how data and associated messages are routed through multiple networks. In the example (Figure 1-4), the internet protocol used determines how data and associated messages are routed from one network to the other. NS3000's Internet Protocol (IP) is based on the DARPA (Defense Advanced Research Projects Agency) standard for an internetwork protocol.

If Node 7 in Network C wants to send a message to Node 14 in Network D, Node 7's message would be sent to Node 11. Node 11 would then send the message to Node 14. All datacomm traffic from Network C to Network D must go through Node 11, the gateway to Network D.

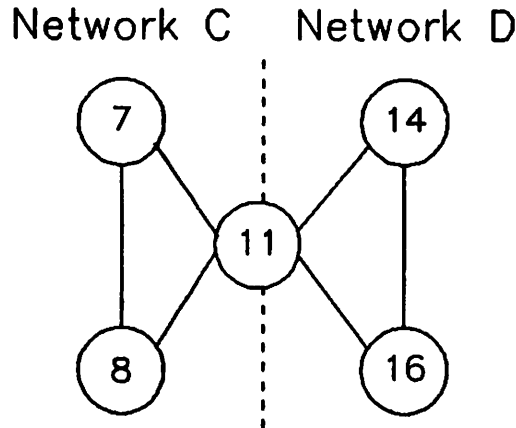


Figure 1-4. Gateway (Node 11).

Networks can also communicate via gateway halves. A gateway half is a degenerate case of a gateway; instead of one gateway node providing internetwork communication, two gateway halves are needed. Each gateway half belongs to only one of the networks that it links; each has a Gateway Half link over which it is connected to the other gateway.

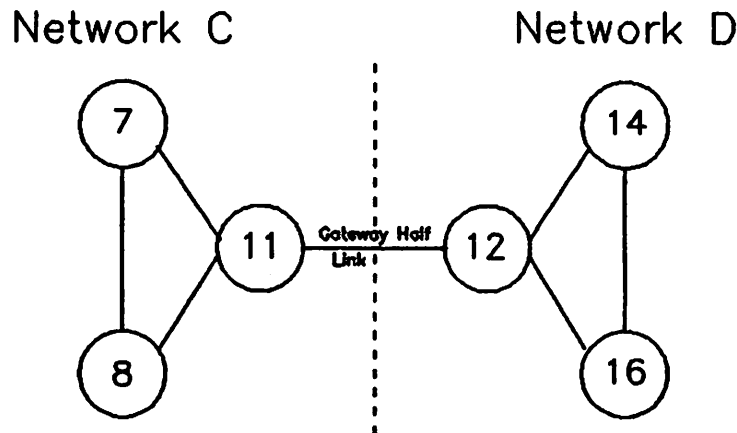


Figure 1-5. Gateway Halves (Nodes 11 and 12).

For example, in Figure 1-5, Node 11 is a gateway half that belongs to Network C, and Node 12 is a gateway half that belongs to Network D. The link between Nodes 11 and 12 is a Gateway Half link. Messages from Network C destined for Network D are first sent to Node 11, the gateway half for Network C. Node 11 sends the message to Node 12, which is Network D's gateway half. Node 12 then routes the message to the appropriate node in Network D.

A node can be a gateway and a gateway half. If a node has three links and belongs to two networks, it would be a gateway to the two networks that it belongs to, but a gateway half to the network to which it did not belong. For example, in Figure 1-6, Node 5 is a member of Networks A and B, and is a gateway between them. Although Node 5 has a link to Network C, it does not belong to Network C and so is a gateway *half* to that network.

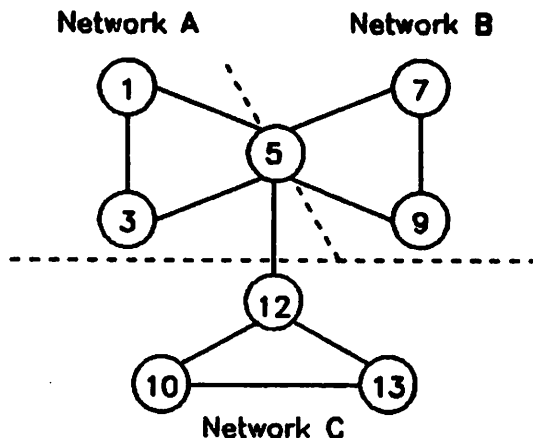


Figure 1-6. Catenet.

NS3000/V Architecture

NS3000/V is composed of two parts: NS3000/V Services and NS3000/V Links. NS3000 Services perform functions of layer 5 (Session layer), layer 6 (Presentation layer), and layer 7 (application layer) of the OSI model. Each of the available NS3000/V links performs the functions of layers 1 through 4 of the OSI model. Figure 1-7 shows the relationship of NS3000/V Services and Links to the OSI model.

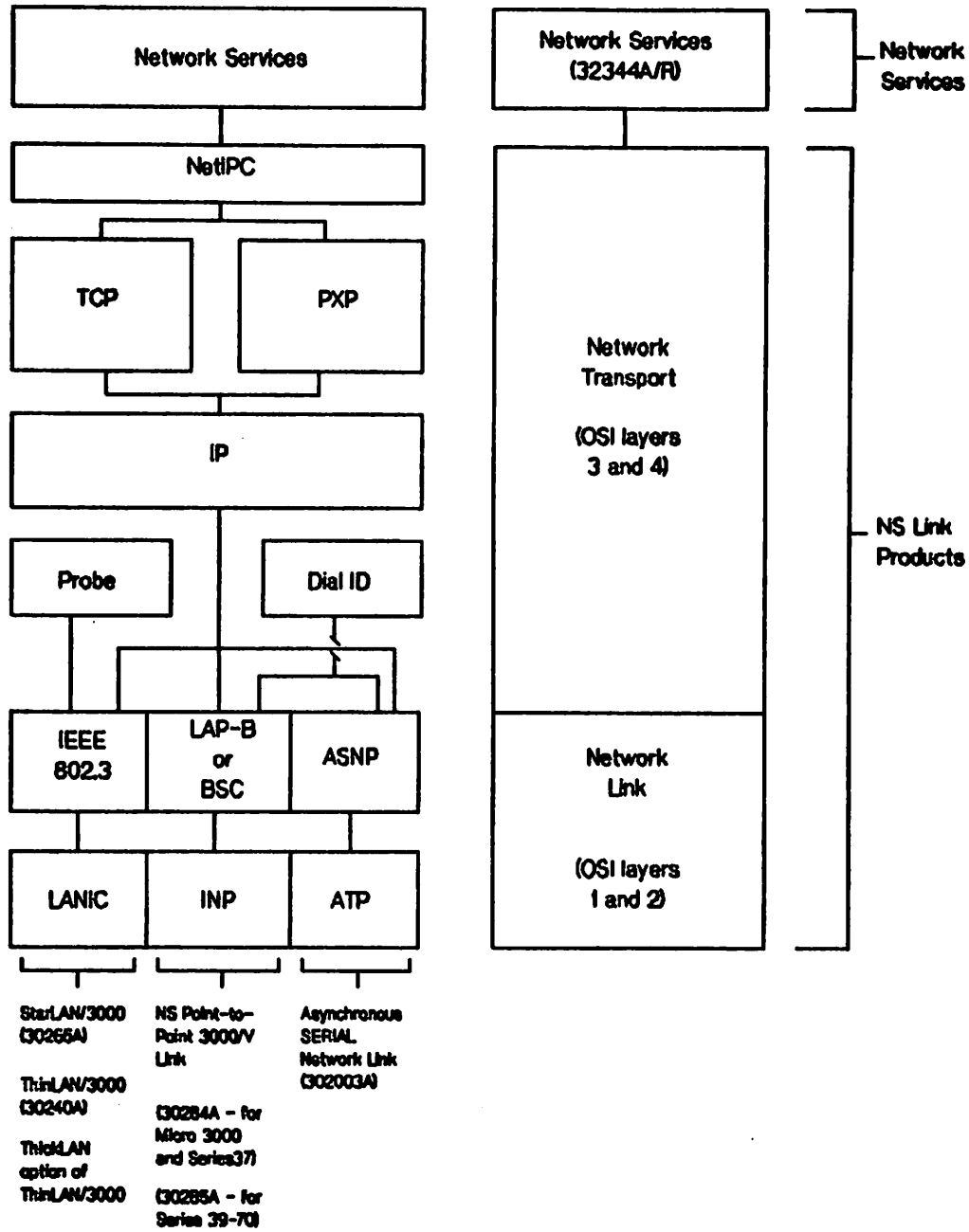


Figure 1-7. NS3000/V Architecture.

Protocols

The protocols, or rules that specify the format of each NS3000/V architectural layer ensure that NS3000/V communication occurs successfully. Some protocols, such as the protocols for layers 3 and 4 (the Network and Transport Layers, respectively) are used by all network nodes, regardless of the type of links that connect them. Other protocols, such as those for layers 1 and 2 (the Physical and Data Link Layers, respectively), differ depending on what kind of link and what kind of network is being used.

This section briefly describes the protocols used by NS3000/V for various network layers, and explains the variations associated with different network link types. Figure 1-7 shows the protocols used for each type of network link. Figure 1-7 also shows the composition of NS3000/V link products. Each link product consists of software and hardware that performs the functions of layers 1 through 4 of the OSI model. NS3000/V Network Services consists of software that performs the functions of layers 5 through 7 of the OSI model.

As Figure 1-7 also shows, the software and hardware comprising each NS3000/V link product can be divided into two main portions: the Network Transport and the Network Link. The Network Transport software performs the functions of layers 3 and 4 of the OSI model. The Network Link hardware and software performs the functions of layers 1 and 2 of the OSI model.

The protocols that are implemented by the Network Transport and Network Link software and hardware are described in the following sections.

OSI Layer 4 (Transport Layer) Protocols

All NS3000/V communication makes use of one or both of two protocols for the Transport Layer; i.e., the network layer that is responsible for ensuring that a message arrives at the correct remote computer.

All NS3000/V communication uses TCP (Transmission Control Protocol). TCP is a reliable, end-to-end, connection-oriented protocol. This means that the protocol recovers from transmission errors and delivers packets of data to their final destination in the correct sequence. It also means that when data is being sent from one node to another, the TCP modules residing on the source and destination nodes maintain status information about the transmission of that data. The combination of information maintained at each endpoint is called a connection. TCP is also flow-controlled, which means that it regulates the flow of data, breaking messages into fragments if necessary, and reassembling them correctly at their destination.

TCP, which is the Defense Advanced Research Projects Agency (DARPA) standard for a Transport Layer protocol, is used by NS3000/V services and can be accessed directly by programs that use NetIPC intrinsics. The use of these intrinsics is described in the *NetIPC3000/V Programmer's Reference Manual*.

The other Transport Layer protocol used by NS3000/V is called PXP, for Packet Exchange Protocol. PXP is a request/reply datagram protocol used indirectly by programs using the socket registry mechanism of NetIPC (IPCLOOKUP intrinsic). PXP is an HP proprietary protocol that cannot be directly accessed by user programs.

OSI Layer 3 (Network Layer) Protocols

The Network Layer of the OSI model is divided into two sublayers: 3_i, which routes messages between networks (internetwork), and 3_s, which provides routing within a network. The routing provided by level 3_s is often called intranetwork or subnet routing.

Internet Protocol (IP). The NS3000/V protocol used for layer 3_i (the internetwork layer) and for layer 3_s (the intranetwork layer) in router networks is called the Internet Protocol (IP). Just as TCP is the DARPA (Defense Advanced Research Projects Agency) standard for a Transport Layer protocol, IP is the DARPA standard for an internetwork protocol.

The purpose of the IP protocol is to route data from source nodes to destination nodes throughout the catenet. IP determines the route that a packet of data should take through the catenet based on

Introduction

addresses. Each node in the catenet is assigned a unique address. Each data packet also includes a destination address, which is compared with the addresses of the nodes the data passes through. When the addresses match, it means that the data has reached its destination. NS3000/V uses IP for internet routing (routing between networks in the catenet) and for intranet routing in router networks.

Section 3 of this manual discusses IP routing and addressing in more detail.

Although NS3000/V uses IP to provide routing information for nodes within the same router network, additional protocols must be used to provide intranet routing for other network types. For example, IEEE 802.3 networks use the protocols defined in the IEEE 802.3 standard for which these networks are named. These protocols are described below.

IEEE 802.3 Local Area Network Protocols. The ThickLAN, ThinLAN/3000, and StarLAN/3000 links all use protocols defined in the IEEE 802.3 standard for layer 3s, as well as for layers 1 and 2. (The IEEE 802.3 standard encompasses standards for layers 1, 2, and 3 of the OSI model.)

OSI Layer 2 (Data Link Layer) Protocols

The protocols used for the data link layer, which is responsible for getting data from one side of a physical link to another without error, vary according to the type of NS3000/V link product that is providing the connection. The three layer 2 (link-level) protocols used for NS3000/V links are called LAP-B, BSC, and ASNP.

LAP-B. NS Point-to-Point 3000/V links use a protocol called LAP-B, for Link Access Procedure, Balanced. LAP-B is a bit-oriented, full-duplex protocol.

Direct-connect (hardwired) and leased line NS Point-to-Point 3000/V Links use the LAP-B protocol.

BSC. The BSC protocol (sometimes also called Bisync) is a character-oriented, half-duplex protocol. It can be used by NS Point-to-Point 3000/V Links that are using dial links. Dial links use public, switched telephone lines to carry data.

ASNP. Finally, Asynchronous SERIAL Network Links use a data link layer protocol called the Asynchronous Serial Network Protocol, or ASNP. ASNP ensures error detection and data integrity by using a 16-bit cyclic redundancy checksum polynomial.

OSI Layer 1 (Physical Layer) Protocols

As with data link layer protocols, protocols for the OSI physical layer vary, and depend on the type of NS3000/V link in use. Figure 1-7 shows the Hewlett-Packard hardware interface cards that implement physical layer protocols: the Advanced Terminal Processor (ATP) for the Asynchronous SERIAL Network Link, the Intelligent Network Processor (INP) for the NS Point-to-Point 3000/V Links, and the Local Area Network Interface Controller (LANIC) for ThinLAN/3000, the ThickLAN option, and StarLAN/3000 links.

The layer 1 protocols supported by each interface card are standards for physical connectors. Table 1-3 lists the standards supported by each interface card that can be used for NS3000/V links:

Table 1-3. Interface Cards and Connection Standards

Card	Connection Standards
INP	EIA RS-232-C EIA RS-422 CCITT V. 24/V. 28 CCITT V. 35
LANIC	IEEE 802.3
ATP	EIA RS-232-C EIA RS-422

Auxiliary Protocols

Two additional protocols are used by NS3000/V link products. These are the **Probe protocol** and the **Dial ID protocol**.

Probe Protocol. The Probe protocol is a proprietary Hewlett-Packard protocol used by IEEE 802.3 links. It is a connectionless protocol that provides name-to-address resolution and information about which networking protocols are used on a given remote node. The Probe protocol broadcasts a request to all the nodes on the network, and the correct node responds. Depending on the request the response provides either the IP address that corresponds to a given node name, or the IEEE 802.3 address that corresponds to a particular IP address.

Dial ID Protocol. Both the NS Point-to-Point 3000/V Link and the Asynchronous SERIAL Network Link can be used over direct-connect (hardwired) or telephone lines. When used over telephone lines (dial links), a Hewlett-Packard protocol called the Dial ID protocol provides security checking and IP address exchange.

NETWORK LINKS

As noted previously, NS3000/V operates over the following network links:

- **ThinLAN/3000 Link**, including the thicker cable **ThickLAN** option
- **StarLAN/3000 Link**
- **NS Point-to-Point 3000/V Link**
- **Asynchronous SERIAL Network Link**

Each link product consists of both hardware and software components. Later sections of this chapter describe the software and hardware that is specific to each link product. However, some of the software comprising each link is common to all link products. This software is described below.

Common Link Software

The following software is common to all NS3000/V link products:

- **Network Interprocess Communication (NetIPC)** is a peer-to-peer communications interface. NetIPC allows programs, running concurrently, to exchange information and synchronize actions.
- **The Network Transport** provides the functionality of the network and transport layers (OSI Layers 3 and 4), respectively. The Network Transport moves the data from a user's application out to the communications link and receives data from the communications link, routing it to the appropriate user. It implements the specifications of the Transmission Control Protocol (TCP) and Internet Protocol (IP).
- **Node Management Services** provides configuration file version checking and logging. Logging enables network transactions to be "logged," or recorded, in a disc file. Such a record can be used to assist in network troubleshooting.
- **Node Management Configurator.** The Node Management Configurator subsystem provides NMMGR, the Node Management Configurator program that allows you to configure each node on the network..
- **The Link Support Services** subsystem contains software that opens, closes, and otherwise controls physical links.
- **Communication Services (CS/3000).** CS/3000 provides some of the diagnostic and link management software required for NS3000/V links. CS/3000 is also used by DS-Compatible links.

IEEE 802.3 Links

NOTE

The information contained in this subsection is divided into three headings--ThickLAN, ThinLAN/3000 Link, and StarLAN/3000 Link. Because these link products are all based on the IEEE 802.3 local area networking standard, they are similar in many respects. As a result, the information stated for ThickLAN applies to ThinLAN/3000 and StarLAN/3000 *except* where differences are noted.

Note, however, that this section discusses the use of ThinLAN/3000 and StarLAN/3000 to connect multiple HP 3000s; it *does not* describe the use of HP ThinLAN for PCs or HP StarLAN for PCs. Both of these products can be used to connect personal computers in a network. Refer to the HP ThinLAN and HP StarLAN publications listed in the Preface for complete information about HP ThinLAN for PCs and HP StarLAN for PCs.

ThickLAN. The ThickLAN option of ThinLAN/3000 includes all the components to connect an HP 3000 to a coaxial cable based on the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard. This standard specifies a 10 million bits per second baseband local area network (LAN) with a bus topology. The LAN uses a shielded 0.4 inch diameter coaxial cable as the data transmission medium and the Carrier Sense, Multiple Access with Collision Detect (CSMA/CD) medium access method.

Figure 1-8 shows the hardware components (described below) that the ThickLAN provides to connect an HP 3000 to an IEEE 802.3 coaxial cable.

ThinLAN/3000 Link. Same as ThickLAN except that ThinLAN/3000 Link uses a 0.18-inch diameter coaxial cable. Figure 1-9 shows the hardware components that ThinLAN/3000 provides to connect an HP 3000 to an IEEE 802.3 coaxial cable.

StarLAN/3000 Link. The StarLAN/3000 Link allows personal computers and MICRO 3000s, MICRO 3000XEs, and Series 37s to operate as an IEEE 802.3 local area network with connections among systems made via twisted-pair telephone wires. Figure 1-9 shows a StarLAN network that is attached to a ThinLAN/3000 link. Hewlett-Packard has published a manual set specifically addressing the StarLAN networks. Refer to the appropriate manuals as listed in the Preface for more information. The configuration of an HP 3000 as a node in a StarLAN network is described in Sections 7 through 14 of this manual.

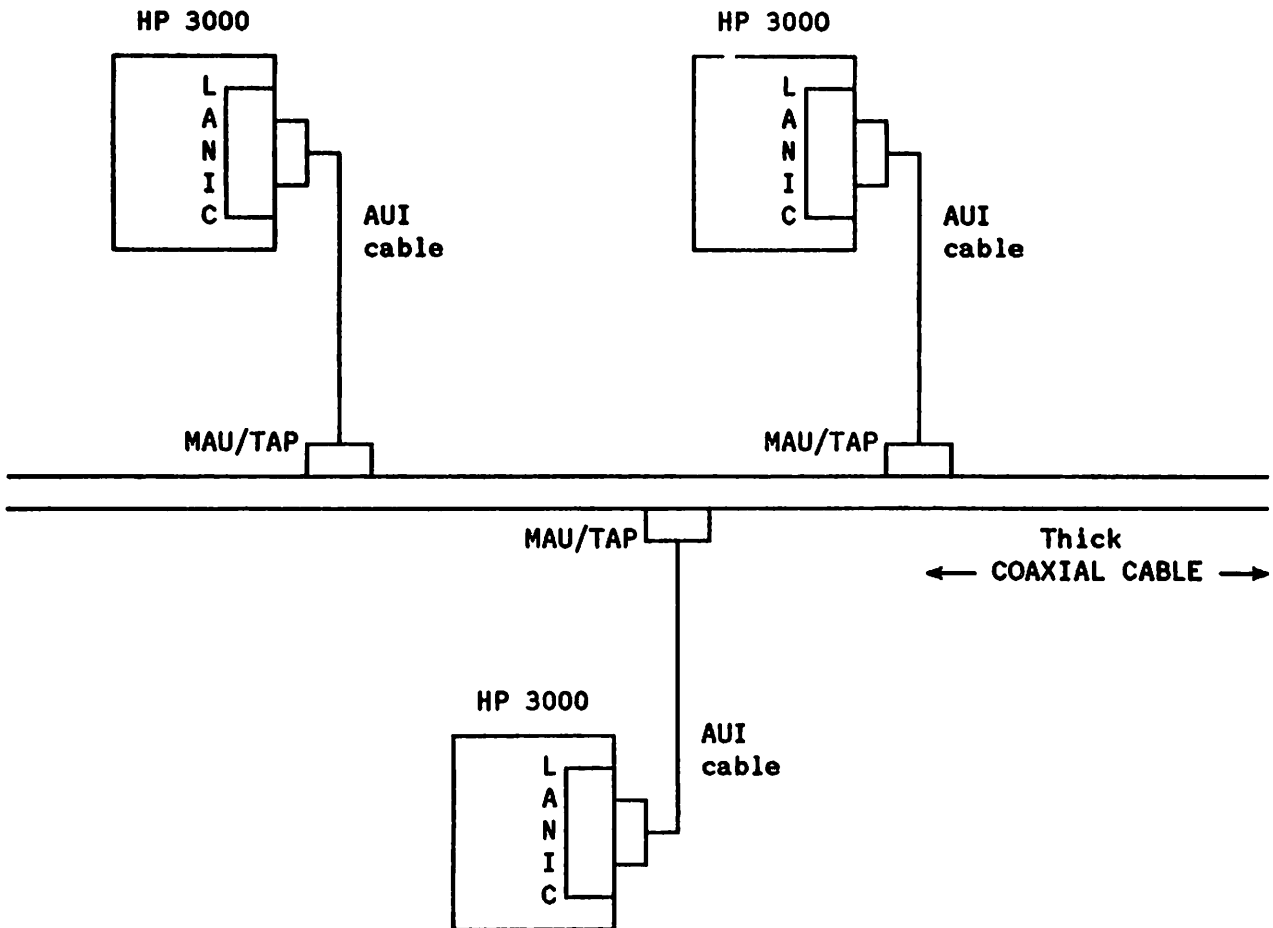


Figure 1-8. ThickLAN Hardware Components

ThinLAN/3000

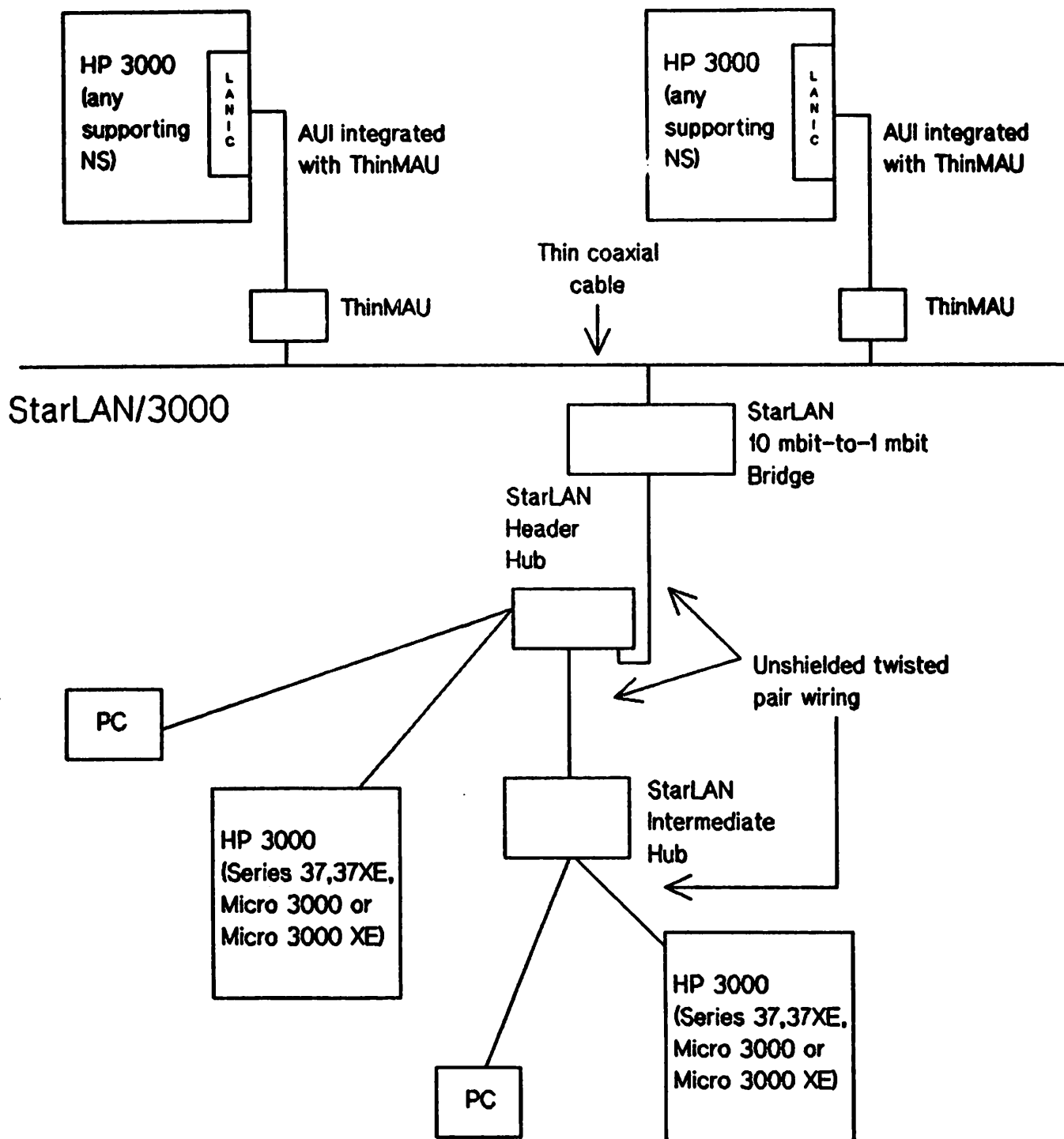


Figure 1-9. ThinLAN/3000 and StarLAN/3000 Hardware Components

Medium Access Method for IEEE 802.3 Links

The IEEE 802.3 standard specifies the Carrier Sense, Multiple Access with Collision Detect (CSMA/CD) medium access method. This method provides an ideal means of transmitting bursts of data at high speeds between nodes on a LAN. With CSMA/CD, all nodes have equal access to the network (Multiple Access); there is no central control node. Before transmitting data, a node monitors the network to verify that no other node is transmitting data (Carrier Sense). If a signal is sensed, the node desiring access defers its transmission. Although the carrier sense makes collisions unlikely, they can occur when two nodes sense that no other carriers are on the network and begin transmitting simultaneously. To deal with this possibility, nodes listen for collisions while transmitting (Collision Detect). If one is detected, the node will initiate a jam signal to warn the entire network. All nodes must then cease their transmission. Each delays for a random period of time and then restarts its transmission. This means that each node eventually gets to transmit its data.

Although nodes in an Ethernet network also use CSMA/CD, a node based on IEEE 802.2/802.3 cannot communicate with an Ethernet node. Nonetheless, both nodes may coexist on the same network cable. This is because there is an incompatibility in the frame format at the data link level (OSI Layer 2) that interferes with communications but not with transmissions. The frame format specified by IEEE 802.2/802.3 provides for higher network reliability.

Hardware Components

ThickLAN. There are three major hardware components of ThickLAN. These are:

- **Local Area Network Interface Controller (LANIC).** The LANIC is a microprocessor-based communication controller that plugs into the HP 3000 backplane. It handles link-level buffering, error checking, the IEEE 802.2 and 802.3 protocols and includes a built-in self-test. When addressed by another node on the network, the LANIC receives the frames of information and checks them for accuracy before passing them to the HP 3000. When transmitting, an addressed frame is passed to the LANIC where error checking information is added. The LANIC then tests to see if the cable is busy and if not, transmits the frame.
- **Medium Attachment Unit (MAU).** The MAU provides the physical and electrical connection to the coaxial cable; it is powered by the LANIC through the AUI (Attachment Unit Interface) cable. The MAU receives signals from and sends signals to the coaxial cable. It also detects collisions resulting from two nodes starting to transmit simultaneously. A MAU is attached to the coaxial cable with a cable tap and can remain permanently attached to the cable. A MAU can be attached on an active network without interrupting network traffic.
- **Attachment Unit Interface (AUI) Cable.** The AUI cable and two-meter internal LANIC cable attach the LANIC to the MAU. It can be up to 48 meters in length. It is available with either FEP coating for installation in passages restricted for breathable air or with PVC coating for installation in less restricted spaces.

ThinLAN/3000 Link. There are two major hardware components of ThinLAN/3000 Link, as follows:

- **Local Area Network Interface Controller (LANIC)**--same as for ThickLAN.

- **Thin Medium Attachment Unit (ThinMAU).** The ThinMAU provides the connection from the LAN hardware to the thin coaxial cable. The ThinMAU connects to the LANIC with an AUI cable. The AUI cable is one meter in length and is integrated with the ThinMAU. Additional or alternate cables are not supported. The AUI cable attaches to a two-meter internal LANIC cable.

StarLAN/3000 Link. StarLAN/3000 Link includes the following hardware:

- **Local Area Network Interface Controller (LANIC).** An interface card similar to that provided with ThickLAN and ThinLAN/3000 Link except it provides connection to an HP StarLAN twisted-pair cable, and it applies to HP 3000 Series 37, 37XE, MICRO 3000, and MICRO 3000XE systems only. The LANIC comes with all StarLAN/3000 Links.

Other StarLAN-related hardware which must be ordered separately to correspond to the needs of the network design includes:

- **Cabling.** StarLAN cabling consists of unshielded twisted-pair wiring that conforms to the IEEE 802.3 Type 1BASE5 standard (draft).
- **StarLAN Bridge.** A bridge is a device that allows connection between different types of LANs, but is transparent to the nodes that communicate across it. For example, a Bridge permits the connection of a coaxial cable LAN to a StarLAN, allowing Series 4x/5x/6x/70 HP 3000s to communicate with StarLAN nodes. In this case, the Bridge connects to the coaxial cable LAN through a MAU/ThinMAU and AUI cables, as appropriate, and to the StarLAN via a StarLAN cable to a StarLAN Hub. In addition, it compensates for differences in transmission speeds between the LANs, for example, the 10 Mbit/second coaxial cable LAN and the 1 Mbit/second StarLAN.
- **StarLAN Hub.** A Hub is a central device on a StarLAN. Using StarLAN cables, a single Hub can be connected with up to 11 nodes (personal computers or the supported HP3000s) or other Hubs. With multiple Hubs connected, up to 50 nodes on a StarLAN can be supported.

Figure 1-9 illustrates an HP StarLAN attached via a Bridge to a ThinLAN.

Link Level Software

ThickLAN. The link level software implements the specifications of IEEE 802.2 and 802.3, the protocols used for OSI layers 1 and 2, the physical and data link layers, respectively.

ThinLAN/3000. Same as for ThickLAN, plus software that provides PC access to most HP 3000 applications.

StarLAN/3000. Same as for ThickLAN, plus software that provides PC access to most HP 3000 applications.

NS Point-to-Point 3000/V Link

The Point-to-Point 3000/V Link is, as its name implies, a point-to-point link. Point-to-point links transfer data by sending it from one node in a network to another until it reaches its destination.

Three types of Point-to-Point 3000/V Links are available; they are distinguished by the kind of physical connections that exist between nodes on the network:

- Direct connect links, which use direct connect cable to connect nodes in the network. Such connections are often referred to as "hardwired" connections.
- Dial links, in which a modem attached to a node is used to transmit and receive data carried across telephone wires. Dial links are also referred to as switched lines.
- Leased lines, in which data is sent over data-grade lines leased from a private carrier.

Figure 1-10 shows a router network consisting of some NS Point-to-Point 3000/V Links, as well as Asynchronous SERIAL Network Links.

NS Point-to-Point 3000/V links use an HP 3000 Intelligent Network Processor (INP) to perform link-level communications protocol management. The INP is a hardware card that fits into the backplane of the HP 3000. Software that implements a particular link-level protocol is downloaded from the HP 3000 when the system is being installed as part of the network. Each HP 3000 with a Point-to-Point 3000/V link must have an INP installed.

The direct connect, dial, and leased Point-to-Point 3000/V links differ in the link-level protocols available and in the hardware additional to the INP that is used to interconnect systems. The following sections describe these differing features.

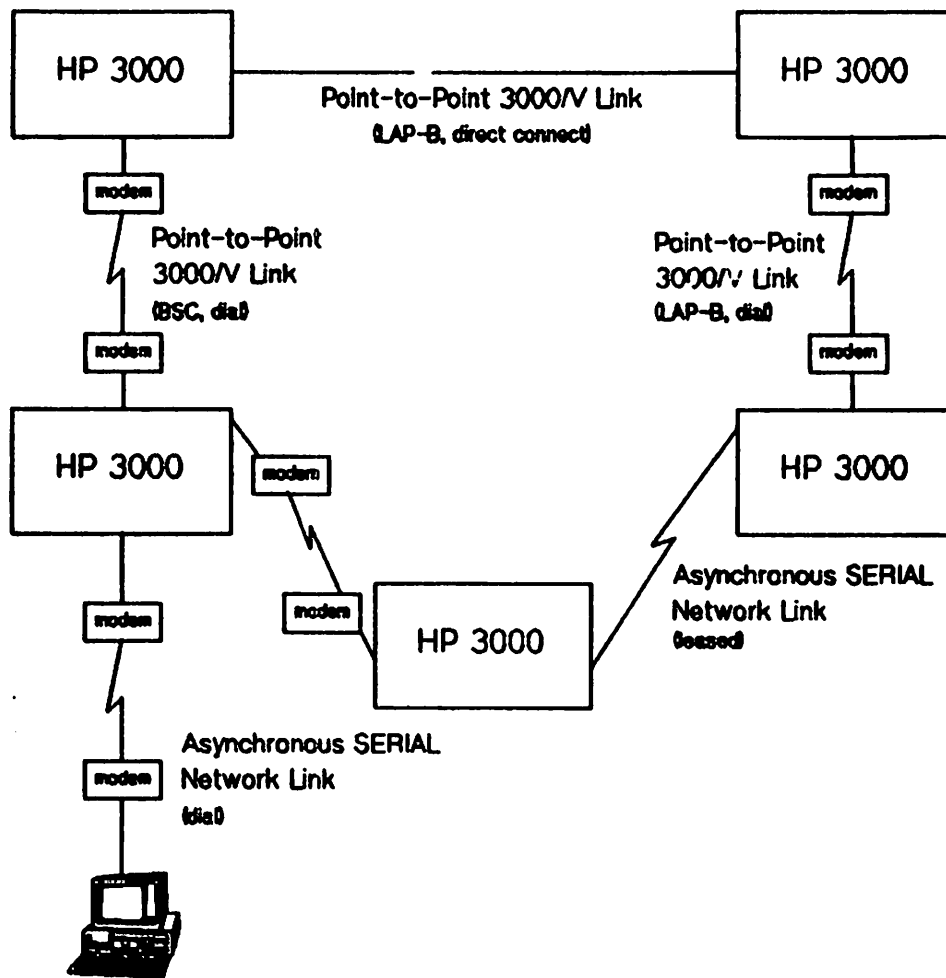


Figure 1-10. Router network with NS Point-to-Point and SERIAL Links.

Direct Connect Links

Link Level Protocol. The direct connect NS Point-to-Point 3000/V Link uses the LAP-B link-level protocol. LAP-B is a bit-oriented, full duplex, peer-to-peer protocol.

Hardware and Cables. As noted previously, each HP 3000 with an NS Point-to-Point 3000/V link, including those using direct connect links, requires its own INP. Direct connect cable terminated by EIA RS-422 connectors connects the systems in the network. These cables must be ordered separately from the NS Point-to-Point 3000/V Link.

Dial Links

Dial links can be implemented using either direct dial modems, for which the telephone number of a connected node is manually dialed by the user, or autodial modems, in which the telephone number of a connected node is configured into NS3000/V network management configuration software. Whether direct dial or autodial connections are used depends upon the features of the modem connected to a particular node.

Link Level Protocols. Both the LAP-B and BSC protocols can be used as link-level protocols to support NS Point-to-Point 3000/V dial links.

LAP-B is a full-duplex protocol. Because data can be transmitted in two directions at once using a full-duplex protocol, and in only one direction at a time using a half-duplex protocol, better throughput is achieved using the LAP-B protocol. Full-duplex modems are required when using LAP-B.

BSC is a half-duplex protocol; it therefore can operate over half-duplex modems. However, better throughput (although poorer than with LAP-B) can be achieved by using BSC over full-duplex modems.

See Appendix B, "Supported Modems," for a list of the modems supported for each link-level protocol.

Leased Lines

The company that owns a leased line allocates use of the line specifically for a subscriber's data communication needs. A cable from the INP to a modem that is attached directly to the leased line connects the HP 3000 to the leased line.

Link Level Protocol. HP only supports the use of the LAP-B protocol over leased lines for NS Point-to-Point 3000/V Links. Due to greater throughput efficiency, LAP-B is the preferred link level protocol for leased lines.

LAP-B requires the use of full-duplex modems. See Appendix B, "Supported Modems," for a list of the modems supported for LAP-B.

Hardware and Cables for Dial Links and Leased Lines

As previously noted, each HP 3000 with an NS Point-to-Point 3000/V link, including those using switched (dial links) or leased lines, requires its own INP (HP part number 30020B for Series 39-70, part number 30244M for MICRO 3000, MICRO 3000XE, Series 37, and Series 37XE). In addition, each HP 3000 connected via a modem link requires a modem and cable connecting the modem to the INP. These cables are direct connect and are terminated by connectors adhering to the EIA RS-232-C standard. Direct dial modem links require a telephone; autodial and leased line modem links require only a modem. Refer to Appendix B of this manual for a list of supported modems.

Asynchronous SERIAL Network Link

The Asynchronous SERIAL Network Link for the HP 3000 provides asynchronous data transfer between HP 3000s and between personal computers and HP 3000s.

The Asynchronous SERIAL Network Link uses the Advanced Terminal Processor (ATP) hardware subsystem to make connections. The ATP is a terminal/printer controller used on MICRO 3000, MICRO 3000XE, Series 37, 37XE, 39, 4x, 5x, 6x, and 70 HP 3000s. It is the only controller available for MICRO 3000, MICRO 3000XE, Series 37, 37XE, 64, 68, and 70 systems. Note that the ADCC, which is another terminal/printer controller available on Series 39, 4x, and 5x HP 3000s, does not support the Asynchronous SERIAL Network Link. One port on the ATP is needed for each system-to-system or system-to-PC connection.

Like the NS Point-to-Point 3000/V Link, the Asynchronous SERIAL Network Link uses the store and forward technique to transfer data among nodes in a network. The Asynchronous SERIAL Network Link is therefore also considered a "point-to-point" link even though it is not part of the NS Point-to-Point 3000/V Link product. An NS3000/V router network can consist of a combination of NS Point-to-Point 3000/V links and Asynchronous SERIAL Network links.

The Asynchronous SERIAL Network Link can be of three types:

- Dial link (switched line)
- Leased line (non-switched)
- Direct connect (from PCs to HP 3000s only)

Dial links can use either direct dial modems, for which the user dials a telephone number to initiate a connection to a remote node, or autodial modems, for which the remote node's telephone number is configured into network management software so that dialing is not necessary.

Leased lines, for which a data-grade line is allocated specifically for a subscriber's needs, can be attached to the HP 3000 by a modem. The router network shown in Figure 1-10 contains two Asynchronous SERIAL Network Links: one is a dial link, and the other is a leased line.

Direct connect links can be used to connect PCs to HP 3000s; however, HP only recommends using ThinLAN/3000 or StarLAN/3000 Links for local-area PC-to-HP 3000 communication.

Hardware and Cabling

To operate, the Asynchronous SERIAL Network Link requires the installation of an ATP. Because the ATP supports a number of asynchronous point-to-point data communication functions such as hardwired and dial connections between HP 3000s and terminals, your system may have had an ATP before you purchased an Asynchronous SERIAL Network Link.

The ATP consists of cards that fit into the backplane of the HP 3000. The minimum ATP subsystem consists of one System Interface Board (SIB) and one Port Controller. Each Port Controller (Direct Connect or Modem) can provide connection to the HP 3000 for up to 12 personal computers or additional HP 3000s. Each HP 3000 can support more than one Port Controller to increase the number of nodes supported by the system up to a maximum of 40.

The maximum number of PC workstations supported for each HP 3000 acting as a SERIAL network server/host is as follows:

MICRO 3000, MICRO 3000XE, Series 37 and 37XE 10

Introduction

Series 39, 42, 44, 48, 52, 58	20
Series 64, 68, 70	40

See your HP representative to discuss the recommended number of SERIAL connections to PCs given your network and application load.

Dial Link and Leased Line Modems and Cabling. Any node (which can be either a personal computer or an HP 3000) connected to the network using an Asynchronous SERIAL Network Link requires a modem and connecting cable. The cable connects the system's Port Controller to the modem using HP Direct-Connect 232 connectors at both ends. Refer to Appendix B of this manual for a list of supported modems.

PC-to-HP 3000 Links. The following personal computers can operate as nodes on an Asynchronous SERIAL Network: HP 150s, HP Vectra personal computers, and IBM personal computers. Refer to the *HP SERIAL Network PC-to-HP 3000 Network Configuration Guide* for a summary of the steps required to attach a PC to an HP 3000 with the Asynchronous SERIAL Network Link. Refer to Sections 6 through 14 of this manual, however, for information about configuring an Asynchronous SERIAL Network Link for an HP 3000.

Link Level Protocol

The Asynchronous SERIAL Network Link uses the ASNIP protocol as a link-level protocol. (Refer to "Protocols" earlier in this chapter for a description of ASNIP.)

Optional DS-Compatible Links

Hewlett-Packard's AdvanceNet Architecture includes HP data communications products based on the principles of the OSI model, as well as extensions for the AdvanceNet predecessor, DSN. Each HP data communications product uses one or more of the different network architectures encompassed in the HP AdvanceNet Architecture. Communication is possible only between data communications products using the same architecture. As a result, it is important to know which architecture is used by which data communications product.

NS3000/V Network Services includes DS Services software as a subset. This enables applications that have been written for operation over DS links to operate over NS links with little or no modification. However, only NS links support the full capabilities of each network service. (Refer to the *NS3000/V User/Programmer Reference Manual* for information on the differences between using various services over NS or DS links.)

DS-Compatible Links can be used to connect a node on a network connected by an NS link to an HP system using DS. The systems and links that can connect them are as follows:

- HP 3000 or HP 1000 with the Point-to-Point Hardwired Link (HP 30270A),
- HP 3000, HP 1000, or HP 9845 with the DS Point-to-Point Modem Link (HP 30271A),
- HP 3000 or HP 1000 with the DS X.25 Network Link (HP 32187A),
- HP 3000 with the DS Satellite Network Link (HP 32188A).

Because these links use the DSN architecture and also work with DS/3000, they will be referred to as **DS-Compatible Links** in this manual.

Each **DS-Compatible Link** provides all the components needed for one side of a connection: link management software, the Intelligent Network Processor (INP) hardware interface card and cables.

A node can have both DS and NS links configured; this allows nodes connected to the node by DS links to communicate with other nodes connected to the same node by NS links.

However, nodes that are using an INP for NS3000/V communication cannot use the same INP for DS communication concurrently. If the node has multiple INPs, it can have DS and NS links operating concurrently; each INP must be used for a different NS or DS link. Figure 1-11 shows a network consisting of both DS and NS links. Node B is shown as supporting both NS and DS because it has two INPs; one INP is configured to support the DS link with node A, and the other INP is configured to support the NS link with node C.

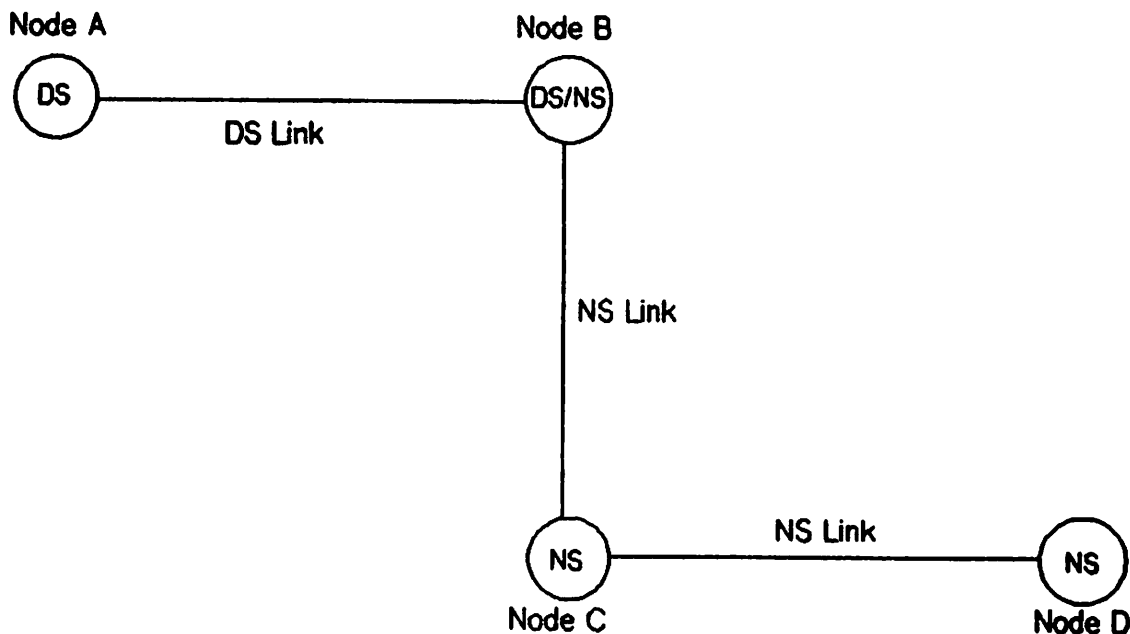


Figure 1-11. Network with NS and DS Links.

Refer to the publications listed in the Preface of this manual for more information on **DS-Compatible links**.

PERSONAL COMPUTERS AS NS3000/V NODES

When used as nodes in NS3000/V networks personal computers (PCs) provide a subset of the network communication functions provided by HP 3000s.

Unlike HP 3000s, PCs cannot provide transparent internet or intranet point-to-point communication. Instead, a PC must establish communication with the HP 3000 to which it is adjacent (this means a link extends from a particular HP 3000 directly to the PC). In addition, PCs do not accept inbound communication; that is, communication with other nodes must always be initiated from the PC.

Introduction

As a result, PC users must log on to the adjacent HP 3000 from the PC (using the :DSLIN command); HP 3000 users cannot log on to the PC from an HP 3000 terminal. Once the PC user has logged on to the HP 3000, he or she can access other nodes in the network by using Network Services commands initiated at the HP 3000.

Note that PCs must therefore be leaf nodes in the network; they cannot be used as intermediate nodes on a point-to-point router network or as gateways between networks.

NS3000/V NETWORK SERVICES

NS3000/V Network Services extend the capabilities of the HP 3000 operating system (MPE) and permit users to share information, programs, processing capabilities, storage facilities, and other resources provided by the various nodes of the distributed network.

The logical environment in which a user or an application process gives instructions to the computer is called a session. In Hewlett-Packard networks, sessions which are established on remote nodes for the purpose of carrying out data communications tasks are called environments. The remote environments may or may not be interactive, depending on the task involved. To accomplish a desired task, users or processes issue instructions similar to those they would use on their own system. In fact, all MPE-V commands and most MPE-V intrinsics can be executed on a remote node once the remote environment is established. In addition, a variety of NS3000/V services include commands or intrinsics to be used for specific tasks on remote nodes. This variety allows the user or programmer to choose the right tool for the task.

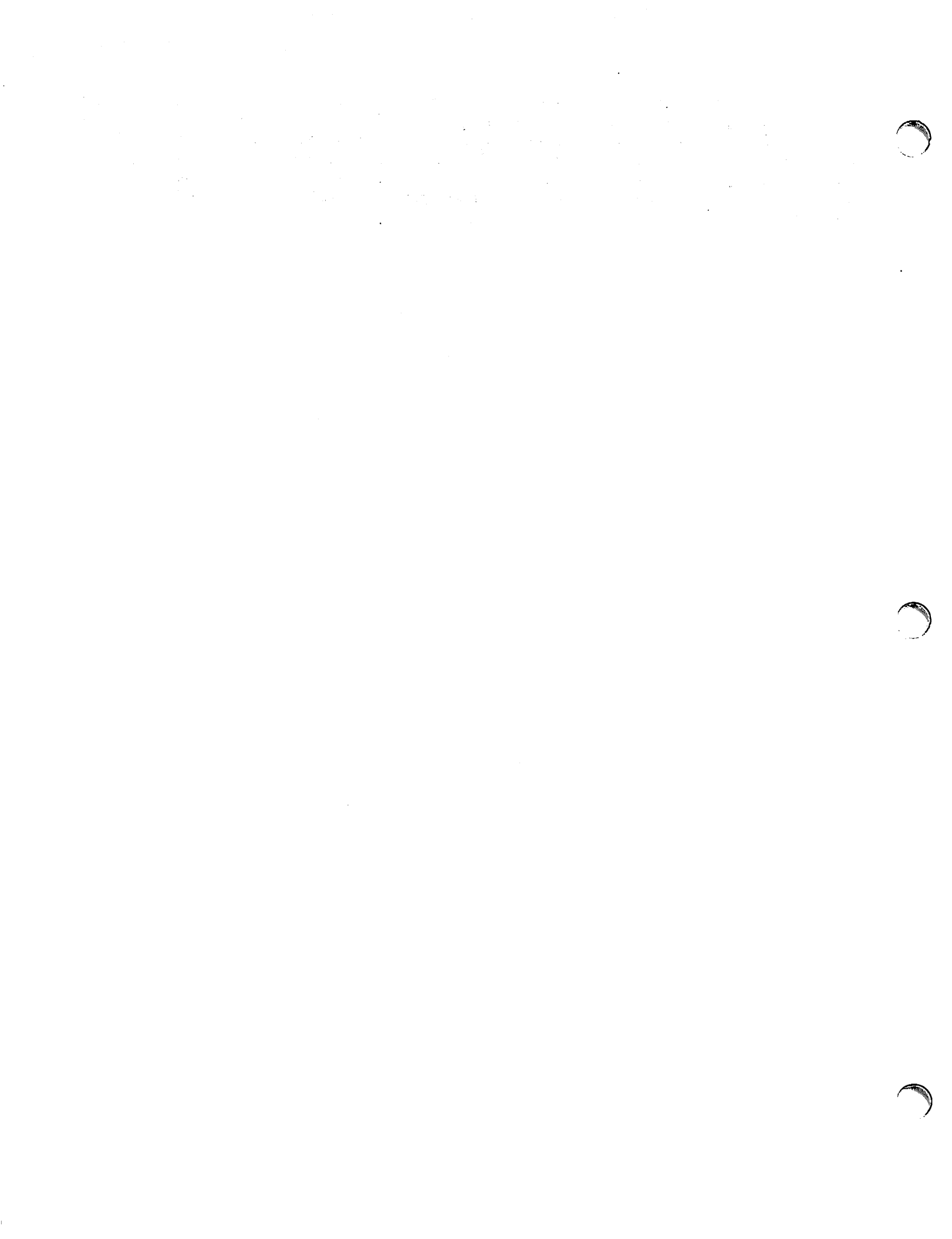
Services Available

The following services are provided by NS3000/V over 3000/V links:

- **Remote Process Management (RPM).** Allows a process to programmatically initiate and terminate other processes throughout a network from any node on the network. RPM is normally used in conjunction with NetIPC.
- **Virtual Terminal (VT and VTR).** Gives the user interactive capabilities on the remote node, even though the user's terminal is physically connected to the local node. Reverse VT (VTR) refers to programmatic access of remote terminals.
- **Remote File Access (RFA).** Allows a user to access files and devices on remote nodes.
- **Remote Data Base Access (RDBA).** Allows a user to access data bases on remote nodes. The same security protection used for data bases on the local node applies to remote access.
- **Network File Transfer (NFT).** A facility that efficiently transfers disc files between nodes on the network. NFT is supported for HP 3000-to-HP 1000, HP 3000-to-HP 9000 (Series 300 and 500) and HP 3000-to- DEC VAX* computers.
- **Program-to-Program Communication (PTOP).** Permits programs residing on different nodes to exchange information with one another in a master/slave relationship.

*DEC and VAX are U.S. registered trademarks of Digital Equipment Corporation.

These services enable users and programmers to perform essential functions in a network- and catenet-wide context. When used over DS-Compatible links, NS3000/V services observe the features and syntax used for the DSN architecture, whether the communication is between NS3000/V and NS3000/V or between NS3000/V and other products using the DSN architecture, such as DS/3000 and DS/1000. However, communication through intermediate nodes is not transparent to the user, as it is when NS3000/V links are used. For details on using these services, refer to the *NS3000/V User/Programmer Reference Manual*.



The advantages of a distributed network are accompanied by the responsibilities of network management, the management of systems in a distributed network. These responsibilities are assigned to the user identified as the network manager, just as the system management of the HP 3000 is primarily the responsibility of those users identified as the system manager and the system supervisor/operator. The network manager's role can be further subdivided by delegating certain tasks to additional users:

- Users called node managers can be assigned to perform network management tasks required for each node on the network.
- If the network is part of a catenet, tasks related to coordinating individual network operation with the operation of the catenet can be assigned to a catenet administrator.
- If a personal computer network uses an HP 3000 as a server, the management of the PC network will be assigned to a PC network manager.

These collective network management responsibilities can be distributed among several individuals, as described above, with coordination among them provided by the network manager. Or, the node manager for a particular node can also manage the entire network. An alternative to any such division of responsibility is where the single network manager can perform all functions: that of node manager for all the nodes on the network, that of network manager, and that of catenet administrator. The PC network manager should coordinate the operation of the PC network with the network manager.

Remember that system management of a single HP 3000 is assigned to a user identified as the system manager and the system supervisor/operator. As a result, it may be appropriate to assign one of these users the role of node manager for an individual system.

All of these system management and network management role assignments are based on the MPE capabilities they require to perform their functions:

- system manager (SM) capability for system manager
- Operator (OP) capability for system supervisor/operator
- node manager (NM) capability for node manager
- network administrator (NA) capability for network manager

NOTE

Although this manual refers to the person responsible for managing the network as the network manager, this title and other titles defined in this section are only used for convenience. The person responsible for maintaining the operation of the network, the PC network, or the catenet needs no particular title, as long as it is clearly defined who is responsible for various parts of the network's operation.

Node manager (NM) and network administrator (NA) capabilities currently provide almost identical access rights. The single difference is that NA capability is required to access and update the network directory, part of the NMMGR utility. The node manager should therefore be assigned NM capability; the network manager should be assigned NA capability. (You might want to call your network manager a "network administrator," to correspond to the NA capability provided by MPE.) By logging on as a user that is assigned the MPE capability of NM or NA, the network manager can execute the utilities and commands needed for the operation of NS3000/V services and link products. In this manual, it is assumed that one person, the network manager, will be completing the tasks required to establish a working NS3000/V network.

As previously noted, these responsibilities may be distributed among several individuals or may be assigned to one person at your installation.

Later portions of this chapter describe the tasks required of the network manager, covering the following topics:

- The Network Management Lifecycle
- Network Management Tools
- Configuration and Initialization Overview

In addition to explaining each major functional area and the corresponding commands or utilities that make up the network manager's job, this section explains background information as needed. Other complex subjects can only be introduced here. In such cases, you will be referred to appropriate additional sources.

NETWORK MANAGEMENT TASKS

As the network manager, you are directly responsible for executing the utilities and commands needed for the operation of NS3000/V services and link products for all the nodes directly connected to your network. In addition, your network may be linked (via gateway nodes) to other networks in the same catenet. DS-Compatible Links may also link your network to DS networks.

The catenet administrator is responsible for the coordination of tasks among all networks that ensure the complete operation of the entire catenet.

As the network manager, you are also responsible for coordination with any network, possibly through the catenet administrator, with which your local network can communicate.

Although the network manager does not have full responsibility for the other networks with which the local network can communicate, he or she needs to be aware of the requirements of establishing connections, such as the naming or addressing conventions used by each type of network.

The Network and Catenet Management Lifecycle

To understand the responsibilities of network and catenet management, it is helpful to examine the major stages of development in a typical network or catenet, generalized into the network/catenet life cycle shown in Figure 2-1.

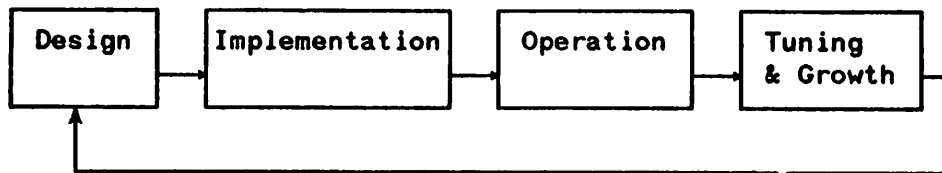


Figure 2-1. The Network/Catenet Life Cycle

Both networks and catenets evolve in much the same way as is illustrated in Figure 2-1. First is the design stage, a time of defining requirements and designing a network to meet those requirements. This stage is followed by the implementation stage. During the implementation stage, each network manager is responsible for managing the installation, configuration, and initialization of all the nodes in the network. The catenet administrator is responsible for managing the overall installation, configuration, and initialization of all networks in the catenet. This includes informing all network managers of configuration information that must be coordinated to achieve internetwork communication. Once the network or catenet is established, management consists of two main tasks:

- **Ensuring network availability.** Each network manager is responsible for changing configurations, controlling the operation of the data communications products on each node, and resolving any problems.
- **Maintaining performance levels.** The network manager monitors performance to ensure consistent response time. The catenet administrator can monitor performance internetwork traffic.

Eventually, in response to the requirements of these tasks, the network manager determines the need for growth or tuning of a particular network, returns to the design stage, and the cycle begins again. Similarly, the catenet administrator must determine the need for growth, tuning, or other alteration of the catenet, and must as a result return to the design stage and begin the cycle again.

Thus, network and catenet management requirements change over time, depending on where your network or catenet is in the network life cycle.

Network Management Tools

The responsibilities of managing a node in a network and coordinating with remote nodes and networks may require the network manager to use a combination of software utilities, data communications test equipment, and network support services. The network manager has a variety of tools and utilities available to supervise the operation of NS3000/V services and link products. Some are provided with the data communications products and some are provided with the HP 3000.

MPE Commands and Utilities

The responsibilities of the network manager, node manager and the system supervisor/operator tend to overlap because of the similarities of their roles. NA, NM, and OP capabilities allow users to issue MPE commands and interact with the system to fulfill designated responsibilities.

A variety of utilities and commands used by the system supervisor/operator are also available to the network manager (and/or node manager, network administrator, or catenet administrator) for use in managing NS3000/V networks. These include:

- **SYSDUMP**--the system I/O configuration utility used to add devices and change system tables. The SYSDUMP responses necessary for NS3000/V services and link products are documented in Section 4 of this manual.
- **MPE Networking Commands.** There are MPE commands specifically designed for starting and stopping NS3000/V link products, and for specifying the operation of certain components. Table 2-1 lists these networking commands. They are described in Volume II, Section 1 of this manual.

Additional MPE commands, such as SHOWDEV and ALLOW, may also be helpful in managing NS3000/V services and link products. Refer to the *MPE V Commands Reference Manual* for information about commands not explained in Volume II of this manual.

- **Software Dump Facility (SDF), DPAN5 and NSDPAN.** The SDF utility provides a memory dump of the HP 3000. It is used following a system failure, halt, or other abnormal condition. DPAN5 is the system utility used to format a memory dump. NSDPAN is an enhanced version of DPAN5. NSDPAN formats the data structures important for analyzing memory dumps from NS3000/V link products and services. If the problem is related to NS3000/V services or link products, a memory dump needs to be submitted with the Service Request. The memory dump should be formatted with NSDPAN rather than DPAN5. The *NS3000/V Error Message and Recovery Manual* describes these programs in more detail.
- **LISTLOG5.** This utility analyzes files in the MPE system log files. An MPE log file records events such as session or job initiation and termination, process termination, file closure, I/O errors, and system shutdown.

Refer to the *MPE V System Operation and Resource Management Reference Manual (32033-90005)* and *MPE V Commands Reference Manual (32033-90006)* for more information.

TABLE 2-1. NS3000/V NETWORKING COMMANDS

Command Name	Description
DSCONTROL	Initiates, terminates, and controls the operation of the DS Compatible Links.
LINKCONTROL	Activates or deactivates link level tracing on the specified communications line. The line must already be initialized.
NETCONTROL	Initiates, terminates, and controls the operation of the Network Transport subsystem of NS3000/V.
NSCONTROL	Initiates, terminates, and controls the operation of the Network Services subsystem of NS3000/V.
RESUMENMLOG	Resumes NMS logging after a recoverable error.
SHOWCOM	Displays the status of a communications device.
SHOWNMLOG	Displays the identification number and available space for the NMS log file.
SWITCHNMLOG	Closes the current NMS log file and creates and opens a new one.

Node Management Services

Node Management Services (NMS), used by the network manager to configure, initialize, and maintain NS3000/V services and link products are used in much the same way that MPE operating system utilities are used by the system supervisor for similar tasks. For example, the SYSDUMP utility is used to configure system hardware into MPE; the network equivalent is the Node Management Configurator, abbreviated NMMGR, which is used for network configuration. The utilities and commands combined as Node Management Services include:

- **The Node Management Configurator (NMMGR).** NMMGR is a menu driven configuration utility that is used to create and enter information into a configuration file. The information in a configuration file is used by the data communications product, *when it is active*, to determine its operating characteristics.
- **The NMS Conversion Utility (NMMGRVER).** NMMGRVER converts a configuration file created with earlier versions of NMMGR to the format required by NMMGR, version A.01.00. Refer to Appendix C for more information.
- **The NMS Trace/Log Formatter (NMDUMP).** The diagnostic functions of logging events and tracing messages are handled by NMS using a common set of internal intrinsics. NMS provides the NMDUMP formatting utility to format the files created by logging or tracing operations. Refer to Volume II, Section 3 of this manual for more information.

Network Management

- **The NMS Maintenance Utility (NMMAINT).** This utility provides a list of software module version numbers and verifies that all modules are current and compatible. Refer to Volume II, Section 2 of this manual for more information.
- **The NODESTAT Utility.** You can use a utility called NODESTAT to display information about the network activities occurring on a node as a troubleshooting aid.

CS/3000 Utilities

There are also several utilities supplied with the Communications Systems (CS/3000) that supplement the diagnostic capabilities provided by NMS. These utilities are:

- **CSLIST and DSLIST.** These utilities supplement the information provided by NMMAINT. They provide a list of software module version numbers for the DS-Compatible Links. These utilities also verify that all modules are current and compatible. Refer to Volume II, Section 2 of this manual for more information.
- **The CS/3000 Trace Facility (CSTRACE).** This utility is used to provide a record of the line actions, states and events that occur during link operation. CS/3000 link tracing is enabled during configuration with NMMGR or with the MPE command LINKCONTROL (refer to Volume II, Section 1.)
- **CSDUMP.** The diagnostic function of tracing messages is handled by CS using a common set of internal intrinsics. CS provides the CSDUMP formatting utility to format the files created by CSTRACE link tracing operations. Refer to the *LAN/3000 Diagnostic and Troubleshooting Guide* for LAN/3000 Link tracing; refer to the *DS/3000 HP 3000 to HP 3000 Network Administrator Manual* for DS-Compatible Link tracing.

Link Level Tools and Utilities

This manual covers those aspects of network management used by the network manager on a day-to-day basis. There are also a variety of link-specific troubleshooting tools that are beyond the scope of this manual. However, because it may be helpful to know what is available, the link-level tools are listed here, with references to the appropriate manuals.

IEEE 802.3 Links. For IEEE 802.3 links, the following tools are available:

- **LANIC Dump Analysis (LANDPAN).** This utility is used to generate a formatted dump of a LANIC log file. These files are produced when an error occurs and contain the contents of the LANIC memory.
- **LANIC Self Test.** This test exercises the major portion of the LANIC hardware and reports status.
- **LAN Node Diagnostic (LANDIAG).** This utility is an interactive on-line program designed to help identify any malfunctioning hardware units of the LAN3000/V Link.
- **Time Domain Reflectometer (TDR).** The TDR that HP recommends is the TEKTRONIX 1503 Cable Fault Locator.

Refer to the *LAN/3000 Diagnostic and Troubleshooting Guide* for more information on these tools. For information on troubleshooting HP StarLAN links connecting personal computers, refer to the *HP StarLAN Diagnostics and Troubleshooting Manual for PCs*.

Links Using an INP. The NS Point-to-Point 3000/V Link and DS-Compatible links use the Intelligent Network Processor (INP) card to perform lower-level data communication functions. The following utilities are available for INP troubleshooting:

- **INP Dump Analysis (INPDPAN).** This utility is used to generate a formatted dump of an INP log file. These files are produced when an error occurs and contain the contents of the INP memory.
- **INP Diagnostic Support Monitor (DSM).** This utility is an interactive on-line program designed to help identify any malfunctioning hardware units of the INP.
- **DSDUMP.** When formatted with DSDUMP, instead of CSDUMP, the link trace file created by CSTRACE can provide additional information on the data link and network levels of the BSC and X.25 protocols.

Refer to the *DS/3000 HP 3000 to HP 3000 Network Administrator Manual* and the *INP Diagnostic Procedures Manual* for more information.

Asynchronous SERIAL Network Link. The following tool is available specifically for troubleshooting Asynchronous SERIAL Network Links:

TERMDSM. The TERMDSM utility is the diagnostic tool for the ATP card used by Asynchronous SERIAL Network Links. Refer to the *TERMDSM On-Line Diagnostic/Support Monitor Reference Manual* for instructions on using TERMDSM.

Installing NS3000/V Links

The installation procedure for each NS3000/V link product specifies responsibilities of the customer and of HP.

Customer Installation Tasks for All NS3000/V Links

You must complete the tasks listed in Table 2-2 before your HP representative begins to install any NS3000/V link product:

TABLE 2-2. Customer Installation Tasks

Required Steps	References
Install modems and phone lines for remote NS3000/V links, if any.	Refer to the appropriate cabling, modem, or auto-dial unit or reference guide.
Install external interconnect cable between HP 3000 system for hardwired NS Point-to-Point 3000/V connections, if any.	<p><i>HP 30020B Intelligent Network Processor (INP) Installation and Service Manual (30020-90005)</i> <i>HP 30244M Intelligent Network Processor (INP) Installation and Service Manual (30244-90002)</i></p>
If installing any of the optional DS Compatible Links, install the communications line and test that the line is functioning correctly.	<p>Refer to the appropriate cabling, modem, auto-dial unit reference manual or other guide for any components to be installed.</p> <p>For the DS X.25 Link, refer to <i>X.25: The PSN Connection (5958-3402)</i> and <i>X.25 Link for the HP 3000 Reference Manual (32187-90001)</i>.</p> <p>For the DS Point-to-Point Links, refer to <i>DS/3000 HP 3000 to HP 3000 Network Administrator Manual (32185-90002)</i>.</p> <p>If connecting to an HP 1000, refer to the <i>DS/3000 HP 3000 to HP 1000 User/Programmer Reference Manual (32185-90005)</i>.</p>
Perform a system backup (including MPE and @.PUB.SYS) and make the system available for installation of the data communications software, interface card(s), and cable.	<p><i>MPE V System Operation and Resource Management Reference Manual (32033-90005)</i> <i>LANIC Installation and Service Manual (30242-90001)</i> <i>Option 100 LANIC Installation and Service Manual (30242-90100)</i> <i>LANIC Installation and Service Manual (30240-90001)</i> <i>Option 100 LANIC Installation and Service Manual (30240-90100)</i> <i>StarLAN/3000 Link Installation and Service Manual (30265-90001)</i> <i>HP 30244M Intelligent Network Processor (INP) Installation and Service Manual (30244-90002)</i> <i>HP 30020B INP Installation and Service Manual (30020-90005)</i></p>

In addition, if any NS3000/V links will be used to connect personal computers to an HP 3000, the customer is responsible for installing the personal computers.

It is also the customer's responsibility to install some hardware and cables for IEEE 802.3 links, as described below.

Additional Tasks for IEEE 802.3 Links

Table 2-3 lists the steps you must complete before beginning to install the software for ThinLAN/3000 (or the ThickLAN, option) and StarLAN/3000 links:

TABLE 2-3. IEEE 802.3 Link Customer Installation Tasks

Required Steps	References
<p>ThickLAN: Install the coaxial cable, MAU/tap, and AUI cables. Test that the line is functioning correctly.</p>	<p><i>LAN/3000 Design Guide (5955-7689)</i> <i>LAN Cable and Accessories Installation Manual (5955-7680)</i> or <i>Local Area Network Cabling and Installation Guide (30242-90002)</i> <i>LAN/3000 Diagnostic and Troubleshooting Guide (30242-90003)</i> <i>LAN Link Hardware Troubleshooting Manual, IEEE 802.3 Coaxial Cable LAN (5955-7681)</i></p>
<p>ThinLAN/3000: Install the thin coaxial cable and ThinMAU. Test that the line is functioning correctly.</p>	<p><i>LAN/3000 Design Guide (5955-7689)</i> <i>LAN Cable and Accessories Installation Manual (5955-7680)</i> <i>LAN/3000 Diagnostic and Troubleshooting Guide (30242-90003)</i> <i>LAN Link Hardware Troubleshooting Manual, IEEE 802.3 Coaxial Cable LAN (5955-7681)</i></p>
<p>StarLAN/3000: Install the Hubs and unshielded twisted-pair cable. Test that the line is functioning correctly. If necessary, install the HP StarLAN Bridge.</p>	<p><i>HP 28647A Bridge Installation and Reference Manual (28647-90001)</i></p>

After the hardware described in Table 2-3 has been installed, you must perform a system backup, as described in Table 2-2.

HP Installation Tasks

During the installation of NS3000/V links, HP is responsible for:

- Taking the system down and performing a system update to add the product software modules to the system if the system is on the current release; otherwise a full system update will be performed.
- Creating the DADCONF.NET.SYS configuration file to allow the initiation of all purchased network services. See the note on the following page for details.
- Verifying that the correct number and version of the software modules have been installed.

Network Management

- Installing the link product hardware, with the exception of the IEEE 802.3 link hardware described in Table 2-3, modems and phone lines, and external interconnect cable between hardwired HP 3000s.
- Adding the link product hardware into the I/O software configuration and configuring it in accordance with the customer's intended use.
- Initially configuring the software in accordance with the network links used.
- Connecting the network link to the communication line (only if the line is available).
- Verifying that a link properly connects a personal computer to the HP 3000. HP can verify this only if the personal computer has been previously been wired to the HP 3000 and if the personal computer is available for testing.
- Verifying that the product properly opens the line when started by command.

Installing Network Services

For UB-MIT and later installations of NS3000/V services and link products, an additional configuration file is required. This file is DADCONF.NET.SYS. Without this file, NS3000/V Network Services will not operate.

DADCONF.NET.SYS is required to initiate the services purchased, such as VT (virtual terminal)-only for ThinLAN/3000 Link. These services become available only when NS3000/V recognizes their existence by means of DADCONF.NET.SYS. This file must be created after product installation because the file defines the services purchased. A configuration file specifying an incorrect set of services may result in unusable purchased services or error messages.

The time to create DADCONF.NET.SYS is after the final SYSDUMP tape has been loaded and the system is fully up (and before NMMGR configuration). Enter the command `STREAM CONFJOB.NET.SYS`. Passwords for `MANAGER.SYS`, `NET` should be added to the `JOB` logon string when appropriate. The job should take two or three minutes to run and should return a message to the console telling you if your file has been successfully created. If a failure occurs, try streaming the job again. If another failure occurs, contact your SE.

You may encounter a situation where you have ThinLAN/3000 Link with incoming VT as your only service, and then you decide to purchase all services for system-to-system communications. To revert from having a VT-only service to having all services, restore `@.NET.SYS`, and then perform `STREAM CONFJOB.NET.SYS`.

Configuration and Initialization Overview

Configuration and initialization of an NS3000/V network is a complex process. The configuration portion of this process is made as easy as possible through the use of NMMGR, a utility that enables you to interactively enter configuration information. Once each node in the network has been correctly configured, the network can be initialized. Initialization is accomplished through the use of MPE network commands.

Configuring and initializing an NS3000/V network involves the following major steps:

- Network and configuration planning
- System Configuration
- Configuring the network with NMMGR
- Verifying network configuration with software utilities and tests
- Maintaining an up-to-date network directory through the use of the NS3000/V network directory utility

Table 2-4 summarizes the required configuration and initialization steps, which are also briefly described in the following subsections. Table 2-4 lists the appropriate sections of this manual where you will find the information required to complete each step. In addition, for each step there is a list of the additional references that you can consult for more or related information. The sections of this manual are arranged in an order that closely corresponds to the steps required to configure and operate NS3000/V.

TABLE 2-4. CONFIGURATION AND INITIALIZATION SUMMARY

Required Steps	References
Create the configuration file required for initiating purchased services.	"Installing Network Services," earlier in this section.
Prepare for network configuration using worksheets and network/catenet maps.	Volume I, Section 3, Network Planning and Configuration
Configure the link hardware devices and pseudo-devices into the HP 3000 operating system.	Volume I, Section 4, System Configuration For additional information: <i>MPE V System Operation and Resource Management Reference Manual (32033-90005)</i>
Study the use of the Node Management Configurator, NMMGR.	Volume I, Section 5, NMS Configurator (NMMGR)
Using NMMGR, prepare the configuration files required for NS3000/V service and link operation.	(All of the following are in Volume I of this manual.) Section 6, Guided Configuration or Section 7, Link Configuration Section 8, Network Transport Configuration and one or more of Section 9, IEEE 802.3 Network Interface Configuration Section 10, Router Network Interface Configuration Section 11, Gateway Half Network Interface Configuration Section 12, Loopback Network Interface Configuration
Create a network directory for nodes requiring one; synchronize network directories among all nodes in network and catenet.	Volume I, Section 14, Network Directory Volume I, Section 3, Network Planning and Configuration

TABLE 2-4. CONFIGURATION AND INITIALIZATION SUMMARY, continued

Required Steps	References
Configure any installed DS X.25 Link(s) using NETCONF.	<i>X.25 Link for the HP 3000 Reference Manual (32187-90001)</i>
Initialize the Network Transport with NETCONTROL, then the Network Services with NSCONTROL.	Volume II, Section 1, Commands
Initialize any optional DS Compatible Links with DSCONTROL.	Volume II, Section 1, Commands

Network and Configuration Planning

Before beginning configuration with NMMGR, you should prepare for the configuration activity by completing the configuration worksheets included in Section 3. These worksheets will enable you to collect and consolidate the information you will need to interactively enter via NMMGR.

System Configuration

Before starting a node's network configuration with NMMGR, you must define to the MPE operating system all of the peripheral devices and software "pseudo-devices" attached to the HP 3000 required for input or output of data (I/O). This definition process is referred to as system configuration. System configuration is accomplished via the interactive SYSDUMP utility. Using SYSDUMP you can configure software drivers for the INP (for Point-to-Point 3000/V, X.25 3000/V, and DS-Compatible links), the ATP (for the ASN 3000/V link), and the Lanic Local Area Network Interface Controller (LANIC), for StarLAN/3000 and ThinLAN/3000 links (including the ThickLAN option of ThinLAN/3000).

HP 3000 data communications connections require pseudo-devices called virtual terminals which consist of software that simulates the function of terminals. NS3000/V links and DS-Compatible links require virtual terminals, which can be configured with SYSDUMP.

Finally, NS3000/V and its links may require changes to MPE system tables. This, too, can be accomplished with SYSDUMP. System configuration for NS3000/V is described in detail in Section 4 of this manual.

Network Configuration with NMMGR

The information required for an HP 3000 to function as a network node is stored in a file called a configuration file. This file can be created and subsequently modified using NMMGR. NM or NA capability is required to run NMMGR, which uses a series of VPLUS/3000 block-mode screens to display and accept configuration information. Use of NMMGR can be divided into three kinds of configuration:

- Link configuration, which defines link level parameters.
- Transport configuration, which defines network transport (OSI layer 3 and 4) information.
- Logging configuration, which enables you to define which information about network activity should be recorded. This information can be printed displayed on a terminal, or routed to a file. This information is useful for network analysis and troubleshooting.

You can access NMMGR in two ways: using a function called Guided Configuration, or through what is referred to as *manual configuration*. Guided Configuration enables you to configure the network more quickly by automatically using default values for certain required configuration parameters, and by automatically bypassing certain optional configuration tasks. To accomplish any of the tasks bypassed by Guided Configuration, you will need to use manual configuration.

NOTE

HP strongly recommends that you use Guided Configuration to initially configure each node, and for most network maintenance and updating. Use manual configuration *only* if Guided Configuration does not provide access to the configuration data you need to change.

Guided Configuration is described in Section 6, manual configuration for network links and transport are described in Sections 7 through 13, and manual configuration for network logging is described in Section 14 of this manual.

Section 5 of this manual provides a more detailed introduction to NMMGR.

Configuration Verification

After you have completed hardware installation, system configuration with SYSDUMP and network configuration with NMMGR, you will need to verify that each node is communicating correctly with other nodes on the network and that all the installed software modules are current and compatible. Utilities and tests for this software and line verification are described in Volume II, Section 2.

Network Directory

A network directory is a file containing information about other nodes in the network. All nodes with point-to-point router links must have a network directory: if an IEEE 802.3 network is part of a catenet, at least one node on the network must have a network directory. (Section 3 explains the function of the network directory in more detail; Section 14 fully describes the network directory and the commands you can use to modify this file.)

One of the tasks of both network managers and catenet administrators is to make sure that the network directories residing on all nodes in the network and catenet, respectively, are up-to-date. This means that when node information changes, and when nodes are either added or deleted, all network directories must be updated to reflect the changes. Updating can be accomplished in several ways: by using the `copy subtree` utility of NMMGR, by sending tapes of updated directories to the people responsible for maintaining a node or network (such as the node manager or network manager), or by relating the information that must change to each responsible person. Refer to Section 14 for more information about the network directory.



This section of the *NS3000/V Network Manager Reference Manual* explains concepts you will need to understand before you plan and install an NS3000 network or catenet.

This section will introduce and describe the following topics:

- **Software Components**, including NS3000/V software subsystems and configuration files.
- **Configuration concepts**, including internet and intranet routing, and the relationship of symbolic names to network addresses.
- **Network and catenet configuration and administration tasks**. Configuration tasks include the procedures required to configure software on each network node, verify that the network is functioning correctly, and start the network. Administration tasks include making sure that changes to network nodes are recorded and that changes are coordinated among all network nodes, when necessary.
- **Network design**, including guidelines to follow when designing a network or catenet.
- **Configuration worksheets**. The last section in this chapter contains worksheets that can assist you in designing a network or catenet, and that you can use to prepare for configuration with the configuration program NMMGR. The worksheet process includes the creation of a network or catenet map that shows the placement of nodes and connecting links.

SOFTWARE COMPONENTS

The following section describes the software components that make up NS3000/V services and link products.

NS3000/V Software Subsystems

The software and associated protocols that enable an NS3000 network to operate are divided into units referred to as subsystems. Separate copies of these subsystems reside on each node in the network. The following subsystems make up NS3000/V services and links:

- **Network Services.** The Network Services subsystem provides services that include Network File Transfer (NFT) and Remote File Access (RFA). The Network Services subsystem will be present on a node only if Network Services have been purchased (separately from the link) for that node.
- **Network Transport.** The Network Transport subsystem contains the protocol modules corresponding to layers 1 through 4 of the OSI model. Network Interprocess Communication (NetIPC) is part of the Network Transport subsystem.
- **Node Management Services.** The Node Management Services subsystem provides configuration file version checking, logging, and tracing. Logging enables network transactions to be "logged," or recorded, in a disc file. The recorded information can be used to assist in network troubleshooting.
- **Node Management Configurator.** The Node Management Configurator subsystem provides the software that enables you to configure an HP 3000 as a network node. This subsystem includes NMMGR, the Node Management Configurator program.
- **Link Support Services.** The Link Support Services subsystem contains two software modules: the Link Manager and the PC Link Manager. Both of these modules open, close, and otherwise control physical links. The PC Link Manager performs these functions for NS Asynchronous SERIAL Network Links; the Link Manager performs them for other NS3000/V links.
- **Communication Services (CS/3000).** CS/3000 provides some of the diagnostic and link management software required for NS3000/V links. CS/3000 is also used by DS-Compatible links.

Configuration Files

Part of the network installation process involves configuring the network using NMMGR interactive configuration software. Through the use of NMMGR, several files containing information about the node and the rest of the network to which it belongs will be created on each node. The information in these files is accessed by various network subsystems while the network is operating. It is the information provided by the configuration files that enables the network software to send and receive data in a suitable form for each node and network link, and to direct data to the correct destination nodes.

Three files can be created on each network node: NMCONFIG.PUB.SYS, NSDIR.NET.SYS, and NSCONF.NET.SYS.

NOTE

The filename NSCONF.NET.SYS is a default filename, and is the name that HP recommends that you use for this configuration file. However, a different filename can be used, as long as the file is located in the NET group of the SYS account. The NSDIR.NET.SYS file that is active, i.e., is in use when the network is running, *must* be named NSDIR.NET.SYS.

For purposes of discussion, the names NSCONF.NET.SYS and NSDIR.NET.SYS will be used to refer to these files throughout this manual.

Each of the files is described below:

NSCONF.NET.SYS. This file contains configuration information needed by the Network Transport subsystem. This information enables the system to operate as a network node. Information ranging from the amount of data buffers to allocate for certain network functions to the telephone number of a dial-up link are contained in this file. Most of the information configured via NMMGR is contained in this file.

NSDIR.NET.SYS. This file, also called a network directory, contains information that enables network software to translate node names (a node name is a symbolic ASCII-character name given to each system in the network that identifies it to the rest of the network and to network users) into protocol and address information. NSDIR.NET.SYS is actually the data file of a KSAM data file and key file pair. The key file that will be created at the same time as the data file will be named using the first 6 characters of the data file, appended with the character K. For example, if the default data file name is used, the key file will be named NSDIRK.

NMCONFIG.PUB.SYS. This file contains information needed for link level and NetIPC logging. Parameters such as what network activities to record and where to record them are provided by this file.

NOTE

Another file, called DADCONF.NET.SYS, is required to initialize NS3000/V Network Services. Refer to Section 2 for information about this file.

CONFIGURATION CONCEPTS

Before beginning network planning and configuration, you must understand certain terms and concepts that may influence your network's design and the values you enter for various configuration parameters. This section describes the most important of these terms and concepts --and those that you should understand in order to fully understand NS3000/V networks. (Additional terms not included

in this section are described in individual network configuration sections of this manual: Sections 7 through 13.)

NS Routing

Routing refers to the process used to determine the path that packets, or fragments of a message, take through a network or catenet to reach a destination node. Routing between multiple networks in the same catenet is referred to as internet routing; routing between nodes in the same network is referred to as intranet routing. The routing mechanism used by a particular network is based on its network type.

The NS Network Transport subsystem provides intranet and internet routing. However, a message's complete source-to-destination route is not determined before it is sent to its destination (unless the destination is a logically adjacent node), because each node possesses information about only the path that should be taken to the *next* node on the way to a destination.

The information about which node a packet should be directed to next is obtained by the Network Transport from the NSCONF.NET.SYS configuration file. The information in this file is derived from values configured using NMMGR. The values entered must therefore reflect the physical design of your network. (Network design is further discussed later in this chapter.)

Intranet Routing

Intranet routing involves all the processes required to route a packet from one node in a network to another node in the same network. Intranet routing can be very simple, as for an IEEE 802.3 network, or potentially very complex, as for a point-to-point router network.

For an IEEE 802.3 network, in which each node is attached to a common bus (the cable) that is shared by all the nodes, routing occurs as follows: Each node that has data to send acquires control of the bus, adds a subnet address identifying the node (called a station address) to the packet, and sends it on the bus. After the packet has been sent, the sending node relinquishes control of the bus. Each node will check every packet that is sent on the bus for a station address that matches its own, and will receive only those destined for it. Figure 3-1 illustrates an IEEE 802.3 network; note that the nodes on the network are all logically adjacent to one another.

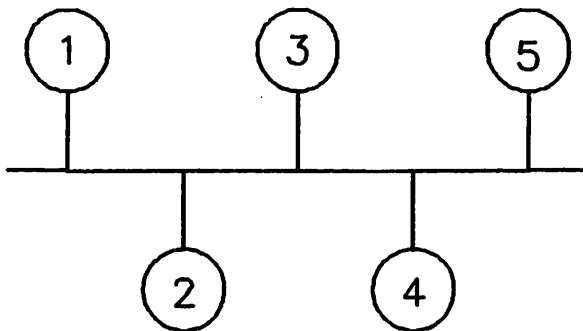


Figure 3-1. IEEE 802.3 Network

For point-to-point networks, nodes are connected to other nodes in the network via one or more point-to-point links. A route may therefore include one or more intermediate nodes through which a

packet must pass on its way to its destination. The routes to various remote nodes are configured into nodal routing tables at each node. At an intermediate node, a packet will be received and forwarded to the next node in the network based on the routing information configured at that intermediate node for the destination node. Information about more than one route to the same destination node can be configured into a node's routing table. If so, an internal algorithm selects the best possible route to the destination node. Figure 3-2 shows an example point-to-point network. Note that more than one possible route exists between nodes.

Alternate Routes. At each node, you can configure the name of the link that a packet should take to get to a given remote node. By configuring multiple alternative links to reach the same destination, you can provide several routes for packets to take to reach a destination. NMMGR allows you to specify an "entry priority" for each alternate link to indicate the order of preference for configured outbound links to the same destination.

Alternate routes can be useful if a link on the network becomes non-operational because of an intentional shut down or a link failure. Refer to "Non-Operational Links" later in this chapter for information about how alternate routes can be used to circumvent non-operational links.

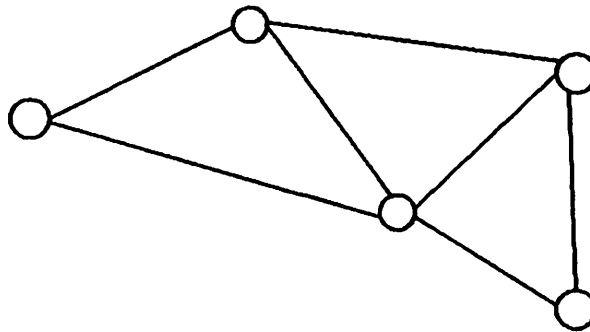


Figure 3-2. Point-to-Point Router Network

Internet Routing

Internet routing involves all the processes required to route a packet from a node on one network to a destination node on another network. Networks are connected to other networks via gateway nodes, which are nodes that are configured either as a member of multiple networks or as a gateway half in addition to another network. Internet routing is therefore concerned with which gateways and which networks a packet will pass through to reach its final destination.

Internet routing decisions are made at both the node that originates the packet and at intermediate gateways. The destination network address is checked against a table that contains an entry for each remote network in the catenet and specifies the gateway(s) on the network that can reach each remote network. Because the purpose of internet routing is to get the packet to the correct destination network, the packet will be forwarded to the appropriate gateway. This will be repeated, if necessary, until the packet reaches the gateway that is a member of the destination network. At this point, intranet routing takes over to get the packet to the correct (and final) destination node.

Symbolic Names

A name, when used in the context of NS3000/V networks, is a character string which identifies some portion or component of a network or catenet. Names, because they can be defined by the user (in this case, the Node or Network Manager) can be chosen to represent some meaningful and easily recognizable concept. For example, if you had three networks in a catenet, you could name them NET1, NET2, and NET3. Or, perhaps in your installation three nodes "belonged" to the marketing, finance, and manufacturing departments, respectively. You might choose to name them NODEMKTG, NODEFIN, and NODEMFG.

Configuration of NS3000/V networks requires that you use NMMGR to configure each node. Many of the items to be entered via NMMGR's interactive user interface (discussed in detail in Section 5) are names. The following sections describe the names that NMMGR will require you to configure.

Node Names

The node name is used to identify each system that is a node in the network or catenet. Each node name used to designate a computer in the network or catenet must be unique, although a single node can be identified by multiple names. Besides being used for configuration, node names are used in Network Services commands (for example, the :DSLIN command) and intrinsics to designate upon which node a particular networking activity is to occur. A complete node name consists of three parts, which together can be no more than 50 characters, as described in detail in the following section.

NOTE

Other HP networking documentation may use the term "computer name" instead of "node name." A computer name is the same as a node name.

Node Name Format and Assignment. Each node in the network must be assigned at least one unique node name. A fully qualified node name consists of three fields, each separated by a period:

nodename.domain.organization

When specifying node names, you must enter the delimiting periods. Each field can be up to 16 characters (alphanumeric, underscore or hyphens); the first character must be alphabetic.

Just as an MPE filename has a singular name, *filename*, and a fully qualified name, *filename.groupname.acctname*, a nodename also has a singular name, *nodename*, and a fully qualified name, *nodename.domain.organization*. The *nodename* must be unique for each node on the network. The *domain* and *organization* do not need to be unique. You might choose a unique *domain* name for each network in the catenet. Note that if the default *domain* and *organization* of all the nodes match they do not need to be specified in commands and intrinsic calls originating from nodes with the same *domain* and *organization* names. If a user does not supply domain and organization fields the fields will default to the local node's assigned domain and organization. This allows users to issue commands or intrinsics with just the single portion of the nodename, *nodename*.

HP recommends that you use some convention when assigning names; for example, all nodes in the same network could have the same domain name and all nodes in the same catenet could have the same organization name.

Multiple Node Names. A single node can be assigned more than one node name by specifying two (or more) node names in the network directory. Although the node may have multiple node names, it can have only one IP address (described in "Network Addresses" later in this section) unless it is a gateway node, which will have more one IP address configured for each network it belongs to. Using more than one node name may be useful if you need to isolate sets of network traffic received or generated by the same node. For example, if you previously had two HP 3000s but have consolidated their activities on a single, more powerful HP 3000, you might have application software that uses two node names that correspond to node names of your previous two computers. By using two node names for the single new system, you could avoid having to modify existing software to accommodate the change.

Other Names

During configuration with NMMGR, you will be asked for several other names in addition to a node name. The node name is the only name that is exchanged between nodes and used by software on remote systems; these additional names are required by only the software within the system being configured. The names described below must be composed of up to eight alphanumeric characters, and must begin with a letter.

Network Interface Name. The network interface name is used to identify the software on a node that provides an interface to a particular network. A useful convention is to name a network interface for the network to which it provides an interface. For example, if you are configuring a node as a member of a network named NET1, the name of the network interface to that network should be NET1. The network interface name is used during configuration and as part of some commands that control network operation. A node requires one network interface for each network to which it belongs, and one network interface corresponding to the software loopback function. A node's multiple interfaces are distinguishable by the use of a different network interface name for each.

During configuration, you may also be required to enter a home network name, which is simply the name of one of the node's network interfaces. A home network name refers to the network interface name that corresponds to one of the networks to which a gateway half node belongs. One of the networks to which the gateway half belongs must be designated the home network to establish a source network address for packets originating from the gateway half.

Link Name. A link name is given to each of the links connecting a node to other nodes on the same network. Links should be named according to some convention you have defined. For example, for a relatively simple network, you might choose to use the same name on different connected nodes to refer to the link which connects them. In a more complex network, you might choose to name the link by a combination of its protocol and logical device (ldev) number. For example, BSC32 might refer to a link using the BSC protocol that is assigned ldev 32 during SYSDUMP configuration.

Router Node Name, Static Neighbor Node Name, Gateway Name. Configuration sometimes requires that you specify the name of a node that belongs to a particular category. For example, a router node name is the name of a node that can be reached via one or more router links from the node being configured. A static neighbor node name is the name of a node that is on the same IEEE 802.3 network as the node being configured. A gateway name is a name that refers to a node acting as a gateway for the node being configured. These names need not be identical with the node name configured for a node; these names identify subsets of configuration data related to a particular node.

Network Addresses

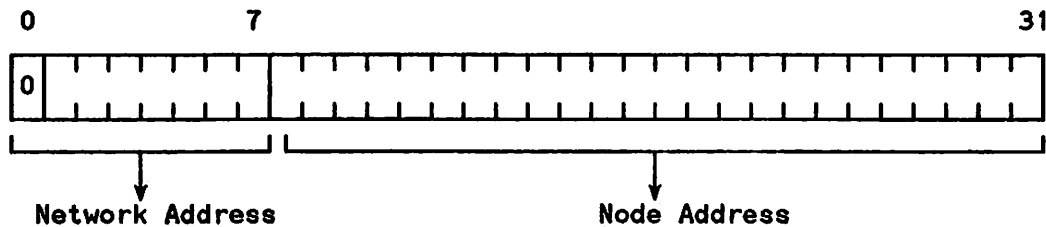
An address, in the networking sense, is a numerical identifier defined and used by a particular protocol and associated software to distinguish one node from another. Addresses of different kinds can vary in complexity depending on the need. For example, two of the protocols used by NS require addresses: the IP protocol and the IEEE 802.3 protocol. The address used by the IP protocol is hierarchical; it identifies both individual nodes and the network to which each belongs. The address used by the IEEE 802.3 protocol is not hierarchical; it provides information only about nodes in a particular IEEE 802.3 network.

IP Address Format and Assignment

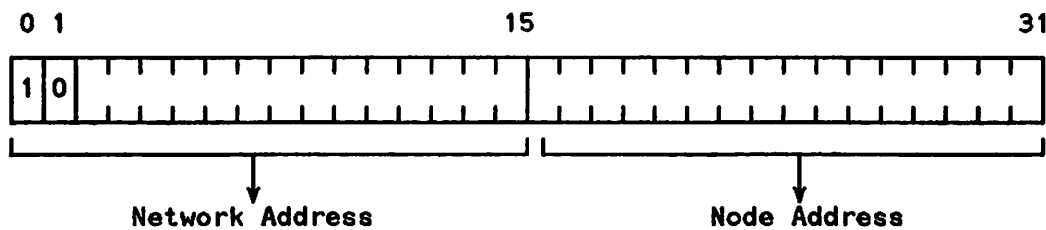
An IP address consists of two components: a network portion, which identifies the network, and a node portion, which identifies a node within a network. The terms network address and node address are commonly used to describe these two components of the IP address. Together, they uniquely identify a node within a network.

IP Address Classes. There are three IP address classes, each accommodating a different number of network and node addresses. The address classes are defined by the most significant bits of the address, as follows:

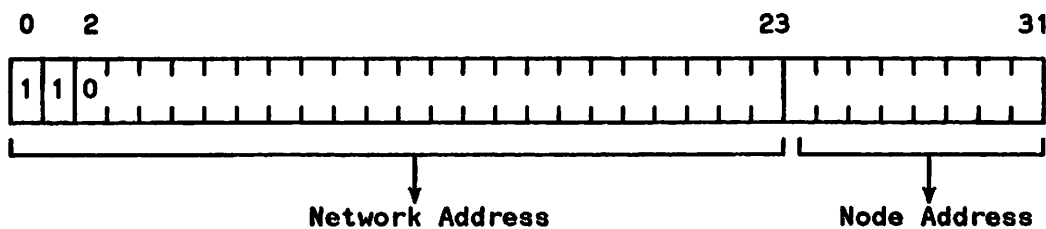
Class A--



Class B--



Class C--



The address classes can also be broken down by address ranges. IP addresses are represented in NS3000/V software by converting the bits to decimal values one octet at a time and separating each octet's decimal value by a period (.) except between the node and network portions, which are separated by a space.

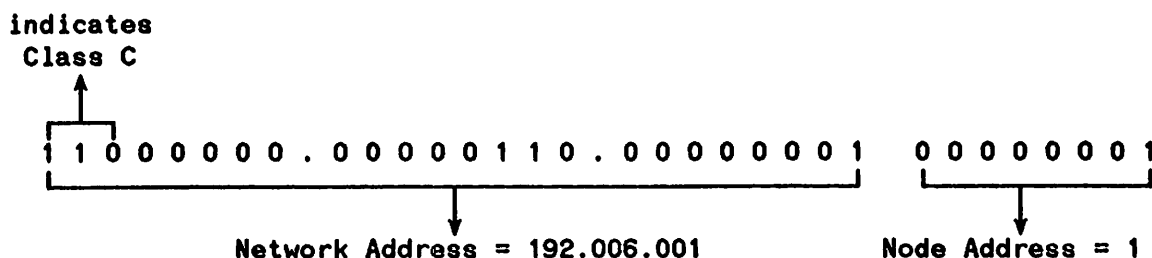
Table 3-1 lists the number of networks and nodes and the address ranges for each address class:

Table 3-1. IP Address Classes

Class	Number of Networks	Number of Nodes	Address Range
A	127	16777215	000 000.000.000 - 127 255.255.255
B	16383	65535	128.000 000.000 - 191.255 255.255
C	2097151	255	192.000.000 000 - 223.255.255 255
Reserved	--	--	224.000.000.000 - 255.255.255.255*

*Note: The address 255.255.255.255 is reserved for NS3000/V loopback. Loopback is described in Section 12.

To determine a network address and node address from an IP address, you must separate the network and node address fields. For example, the bit representation of IP address 192.006.001 001 is separated as follows:



Assigning IP Addresses. You must assign an IP address for each node on the catenet. To assign IP addresses, you must determine network and node addresses.

To determine network addresses for each network, you must first determine how many networks your catenet contains and where your network boundaries are. Each network must be assigned a unique network address. All nodes in the same network must be assigned the same network address.

HP has obtained a block of Class C addresses from the Defense Advanced Research Projects Agency (DARPA). Even if you do not anticipate connection to DARPA's ARPANET (Advanced Research Projects Agency Network), HP recommends that you obtain IP network addresses from the HP Network Administration Office (NAO) to guarantee unique network addresses. To do this, contact your HP representative or write to the NAO at the following address:

Network Administration Office, Department NET
 Information Networks Division
 Hewlett-Packard Company
 19420 Homestead Road
 Cupertino, California U.S.A. 95014
 (408) 725-8111

Do not assign any network and node addresses consisting of all 1s or all 0s. In NS3000/V software, the node address 0 is reserved for messages that are broadcast to all nodes; the address of all 1s is reserved for loopback. (Note that the 3-digit decimal address of 255 represents a byte of all 1s.) ARPA standards also reserve these addresses: all 1s signifies messages for all nodes on the network, and all 0s signifies messages for the same node that originated the message or the same network as the originating node.

Node addresses must be unique only within each network. For example, you could have a node with node address 5 in network 1 and another node with node address 5 in network 2. You can assign node addresses according to your own needs, but they must be within the ranges for the IP address class that you are using.

IEEE 802.3 Station Address Format and Assignment

An IEEE 802.3 station address is assigned to every node on an IEEE 802.3 network. When a packet is sent on the network, only the node whose station address matches the destination address in the packet receives the packet. Hewlett Packard assigns a station address to each IEEE 802.3 interface card during manufacturing. The station address is used for network addressing on the IEEE 802.3 network bus, and has the following format:

hh-hh-hh-hh-hh-hh

where *h* is a hexadecimal digit (0 - 9, A - F).

For HP 3000s, this factory-configured station address is in ROM on the LANIC interface card. You have the option of specifying a different station address by using NMMGR (refer to Section 9). Each time the card is initialized, either the factory-supplied station address or the NMMGR-configured address is activated for use on the IEEE 802.3 network.

In addition to checking the interface card, you can find out what your system's station address is by using the LANDIAG diagnostic utility. After the HELP command and LANDIAG tests 1, 2, 3 and 13 are performed, the utility displays the station address at the bottom of the display screen. Refer to the *LAN/3000 Diagnostic and Troubleshooting Guide* for information on using the LANDIAG utility. Note: Network Services and the Network Transport must be shut down before using LANDIAG.

Assigning Station Addresses. HP recommends that you use the factory-configured station address assigned to the LAN interface card. If you decide to assign your own address contact your HP representative for more information.

Address Resolution

Address resolution in NS networks refers to the mapping of node names to IP addresses and the mapping of IP addresses to subnet addresses. Two kinds of address resolution can occur on a node in an NS network: First, the destination node's nodename must be mapped to the node's IP address. Second, for some types of networks, the IP address must be mapped to a subnet address that identifies a node for the protocols used by the subnet.

Node Name to IP Address Resolution

NS3000/V routes packets throughout catenets and networks based on the internet and intranet addresses of each message's destination node. However, network users and application programs use node names to

designate the destination of a message. As a result, a method is required to map node names to their corresponding addresses.

The Network Transport uses one of three available methods to determine the addresses that correspond to a node name:

1. **From the network directory (NSDIR.NET.SYS file)** that resides on the node from which communication originates. Every node with a point-to-point link must have a network directory. This includes all nodes on router networks and any node functioning as a gateway half.
2. **By the use of the Probe protocol.** The Probe protocol can be used only on IEEE 802.3 networks.
3. **By the use of a Probe proxy server.** This method combines methods 1 and 2 listed above. A Probe proxy server is a node on an IEEE 802.3 network that possesses a network directory and is designated a Probe proxy server during configuration. Other nodes on the IEEE 802.3 network can use Probe proxy requests to obtain information contained in the network directory that may not be available elsewhere.

For each node, a choice from the above methods and the preferred order they are used can be configured with NMMGR.

Name-to-address information for each node is contained in a data structure called a path report. In addition to a node's addressing information, each path report specifies the networking protocols used on the node. When a connection is established between two nodes, the destination node's path report is obtained by one of the three methods listed above. Once a node has received another node's path report, the node receiving the information retains it so that a path report does not have to be obtained every time a connection is established with the same destination node.

The network directory. The network directory file NSDIR.NET.SYS, which you can initially create with NMMGR, contains a node's network directory. The network directory contains entries for remote nodes that each include a remote node's node name and its path report. The first time a connection is initiated from a node that has a network directory, the Network Transport software searches the NSDIR.NET.SYS file for the destination node's node name and associated path report. The path report contains the IP address(es) associated with the destination node name. Every node having a point-to-point link (every node on a router network, and every full or half gateway) must possess a network directory. However, nodes on IEEE 802.3 networks do not each require network directories. Instead, they can use the Probe protocol to obtain path reports.

The Probe Protocol. IEEE 802.3 nodes can use the Probe protocol to obtain path reports specifying the names and corresponding addresses of other nodes on the network. When a node configured to use the Probe protocol needs to establish a connection, it first multicasts a query to all the nodes on the network, requesting a response from the node whose name matches the name in the message to be sent. (Multicasting is similar to broadcasting, except that a message is sent to only a subset of nodes instead of all nodes on the network.) If the name of a node on the IEEE 802.3 network matches the destination node name, it responds to the query by sending back its path report. The node sending the message then uses this information to resolve the destination node's address, ensuring that messages arrive at the correct destination.

Probe Proxy Server Nodes. By itself, the Probe protocol can only obtain information about nodes on the same IEEE 802.3 network; to obtain information about nodes on other networks in the same catenet requires additional help from a network directory. Therefore, if an IEEE 802.3 network is part of a catenet, a network directory must reside on at least one of the IEEE 802.3 network's nodes for messages to be sent to nodes in other networks. If another node on the IEEE 802.3 network needs to establish a

connection with a destination node that belongs to a different network on the catenet, the node with the network directory can provide the sending node with addressing information about the destination node. The node on the IEEE 802.3 network that performs this function is called a Probe proxy server. In addition to possessing a network directory, the Probe proxy server must be designated as such during configuration. HP recommends that the IEEE 802.3 network's gateway node be used as the Probe proxy server. HP also recommends that you create more than one Probe proxy server on each IEEE 802.3 network so that if one of them is shut down, network directory information will still be available.

Figure 3-3 shows an IEEE 802.3 network with two Probe proxy nodes. Probe requests (illustrated by a dashed line) are sent to nodes that are configured to use the Probe protocol. Probe proxy requests (illustrated by a dotted line) are sent to nodes that are configured as Probe proxy servers. Node A can obtain a path report about node E, on another network, from nodes B or D. To send a message to node C, information is obtained from node C itself; the use of a Probe proxy server is not needed.

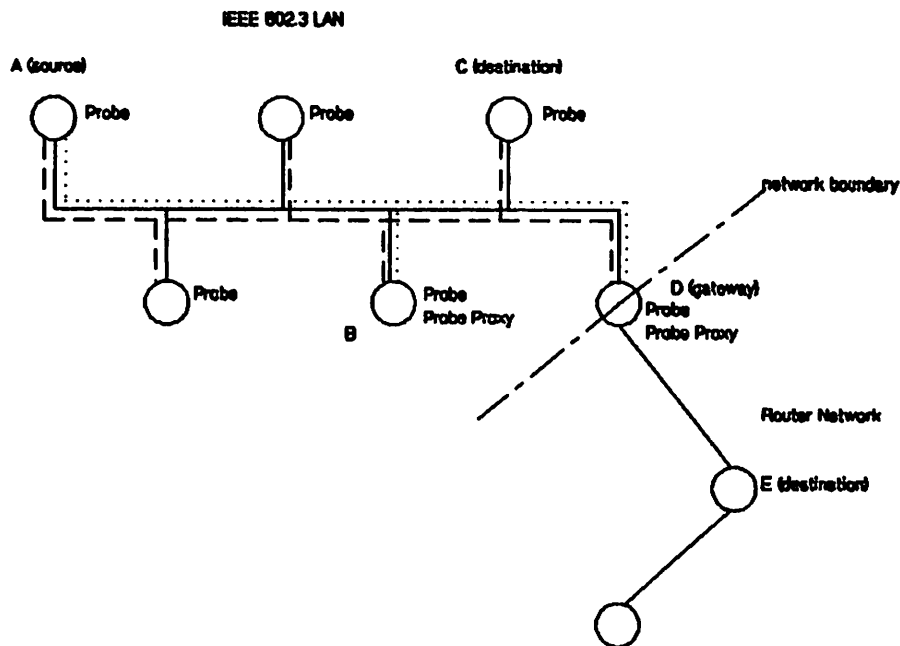


Figure 3-3. IEEE 802.3 Network Probe and Probe Proxy Requests

IP to Subnet Address Resolution

Once a packet is routed to the correct destination network, it needs to be directed to the correct destination node within that network. For router networks, the IP address is the only address needed to route the message within the router subnet. However, in IEEE 802.3 networks, the destination node's IP address must be mapped to its IEEE 802.3 address.

IEEE 802.3 Address Resolution with Probe Protocol. In addition to providing node name to IP address resolution, the Probe protocol provides IP to IEEE 802.3 address resolution. The mapping of a given IP address to an IEEE 802.3 address occurs as a result of a Probe request for address information.

IEEE 802.3 Address Resolution for Non-HP Systems. During configuration of IEEE 802.3 nodes with NMMGR, you will encounter an interactive configuration display screen that allows you to enter addressing information about other nodes on the IEEE 802.3 network. This information resides in the node's NSCONF.NET.SYS configuration file. It is only necessary to configure this screen if a remote

node on the network does not support the Probe protocol and the remote node's IEEE 802.3 address is not configured in the network directory of either the source or Probe proxy server nodes. HP computers support the Probe protocol; therefore, configuration of this information in NSCONF.NET.SYS may be required only if a non-HP node is part of the network.

Configuration Terminology

The following subsections describe concepts and terms you will encounter during configuration of a node with NMMGR. You will also need to be familiar with the concepts described when you plan your network or catenet. Use these subsections to gain general familiarity with the terms and ideas before beginning to plan or configure the network or catenet; you may also wish to use these descriptions for reference in later stages of the planning and configuration process.

General Terms

Remote Node and Local Node. The term local node usually means the node that you are configuring or to which you are logged on. A remote node is any *other* node in the catenet; that is, any node other than the local node.

Buffers. A buffer is a logical grouping of a system's memory resources used by NS3000/V. There are several kinds of NS3000/V buffers: inbound transport buffers, outbound transport buffers, and store and forward buffers. The amount of space allocated for these buffers can be specified using NMMGR.

Inbound and outbound buffers are allocated for each network interface on a node, regardless of the type of network(s) to which the node belongs. Inbound buffers hold data being received by a node until it is used by a particular protocol or a user process. Outbound buffers hold data that will be sent on a link (or through loopback) from the originating node. The number of both outbound and inbound buffers can be specified during configuration with NMMGR.

Store and forward buffers are allocated on gateway nodes (full and half) and on nodes belonging to router networks. The number of store and forward buffers can be changed (via NMMGR) to allow for tuning to achieve better network performance.

Loopback. Software loopback enables a node to communicate with itself; in other words, it allows a single node to be both the source and destination of a message. A network interface (see definition below) must be configured to provide the loopback function.

Network Interface. The term network interface refers to the software that interfaces a node to a network. On each node, one network interface is required for each network or gateway half connection, and for the software loopback function. Most nodes, therefore, require two network interfaces: one for the network the node belongs to and one for loopback. A full gateway requires a network interface for every network to which it belongs. A gateway half requires a network interface for the gateway of which it forms a part, and for the other networks to which it belongs. The term network interface is often abbreviated as "NI" throughout this manual.

Dial Link Terms

You should understand the following terms used to describe dial (also referred to as switched) links:

Direct Dial and Shared Dial. A direct dial link provides connection to a single remote system over a phone line. The telephone number dialed by the local node to reach the remote node never changes unless it is reconfigured with NMMGR. A shared dial link provides connection to more than one remote system, although to only one at a time. The link is thus *shared* by more than one remote node.

Autodial and Manual Dial. An autodial link refers to a link using automatic dialing hardware. This hardware enables a remote phone number to be dialed without requiring a user to manually dial a telephone number. Instead, the telephone number of the receiving modem is entered during a node's configuration, and when a connection must be made, the telephone number is read from the NSCONF.NET.SYS configuration file and "dialed" automatically. In contrast, a manual dial link requires human intervention; the receiving node's telephone number must be dialed at the sending node's location. NS software will display a message at the system console requesting the system operator to dial the number. Whether or not a link is autodial or manual dial depends on the capabilities of the hardware (such as the modem or any additional devices) that is used.

Note that whether a link is direct or shared dial is independent of whether the link is autodial or manual dial.

NOTE

In contrast to any dial links is a direct connect link, which does not rely on switched public telephone lines but instead depends on "hard-wired" cable or leased lines to connect one node with another. Refer to Section 1 for more details about direct connect, leased lines, and dial links for each NS3000/V link type.

Dial ID Protocol. The Dial ID protocol is a proprietary Hewlett-Packard protocol used to provide security for dial links. The protocol verifies the identity of nodes dialing in to a receiving node, and ensures that both the local and remote node have the required security access. HP computers support the Dial ID protocol; however, other computer systems may not support it. The Dial ID protocol must be disabled (during configuration) if the node being configured will be connecting to a node that does not support this protocol.

Security String. A security string is an alphanumeric ASCII character string that acts as a password for dial links. The security string is used by the Dial ID protocol. When a node attempts to connect to another node via a dial link, security strings are exchanged between the nodes. Each node checks the security string it receives against a configured list of valid security strings. If a match is found by both nodes, the link can be used. If one or both of the security strings fail this check, then the link is disconnected.

Security string checking can be disabled at any node (via configuration) if desired.

Router Network Terms

You will encounter most of the following terms during planning and configuration of a router network:

Hop Count. The term hop count is used in two ways: (1) an intranet hop count is the maximum number of intermediate nodes that lie between a source and destination node on the same router network; and (2) an internet hop count is the number of gateways that are used to route a message to its destination network. Because two partner gateway halves perform the function of a full gateway, they

are counted together as a single internet hop. Note that if no intermediate nodes lie between a source and destination, the hop count is zero.

Non-Adjacent and Adjacent. The term adjacent, when used in the context of configuring routing for a router network, refers to a node that is separated from a given node by no intermediate nodes. In other words, the adjacent node lies at the other end of a link connected to a given node. A non-adjacent node, in contrast, is a node that is separated from a given node by intermediate nodes.

Directly Connected. The term directly connected describes nodes that are members of the same network. For example, if node A is directly connected to node B, A and B must be members of the same network. Do not confuse the term "directly connected" with the term "direct connect," which describes a non-switched point-to-point link (hardwired or leased line).

Entry Priority. During configuration of router networks, you must define the route used to transmit information from the node you are configuring to the other nodes in the network. If desired, you can configure more than one route to the same node. If you do so, you can specify which of the multiple routes should be chosen first. For example, if one route has a greater number of intranet hops, you might wish to give it a lower priority (specified as a lower numerical value) than another route with fewer hops. If for some reason the route given the highest priority is not available, the message will be routed to its destination with the alternate (but lower entry priority and greater number of hops) route.

If the same value is used for all entry priorities, the Network Transport software chooses the route to be used. The choice is based on an internal algorithm that selects the best route by taking into account some of the configured characteristics of the intervening links.

Gateway Terms

You will need to understand the following terms if the node you will be configuring will be part of a catenet:

Reachable Networks. A reachable network is a network that can be accessed (with additional internet hops possibly required) by a particular gateway.

Neighbor Gateway. A neighbor gateway is a gateway node (full or half) on the same network as the node being configured.

Gateway Half. A gateway half is a node on which a gateway half network interface has been configured with NMMGR. Together, two gateway half nodes joined by the same link perform the function of a gateway, which is to connect two networks.

Gateway Half Pair. Two gateway halves connected by a gateway half link are considered a gateway half pair.

Gateway Half Link. A gateway half link is a link that joins two gateway halves. A gateway half link must be either an NS Point-to-Point 3000/V Link or an Asynchronous SERIAL Network Link.

Non-Operational Links

Network links may be non-operational because of any of the following: (1) the link was intentionally shut down with the NETCONTROL command, (2) a link failure has occurred or (3) the link has not been started. A non-operational (or "downed") link can affect the routes that messages take to reach their destinations.

Router networks can automatically reroute packets around a non-operational link. Rerouting will occur if alternate links to a destination have been configured at the nodes that are the endpoints of the non-operational (or "downed") link. This rerouting over alternate links is called automatic rerouting.

NS3000/V can also provide rerouting for internet packets. Messages reaching a gateway that are intended for a downed link (at that gateway) will be redirected to another gateway on the same network that can reach the remote network.

Router Network Automatic Rerouting

Router network automatic rerouting will reroute packets in a router network around non-operational router links. This rerouting will occur whether or not the destination node is a member of the router network.

The two nodes at the ends of a downed link will detect the fact that the link is down. If alternate links to the destination are configured at nodes that detect a downed link, the nodes will reroute packets over these alternate links. For router network rerouting, *only the nodes that detect the downed link* can select an alternate link. For messages that originate at some other node, configuration adjustments may need to be made to bypass the link that is not operating.

No immediate indication that a link is not operational will occur at other nodes (besides those directly connected by the "downed" link) on the network or catenet. However, messages will not reach their destinations and a timeout error will occur for the connection.

Alternate Links. The link that a router node uses to reach another node in the network is configured via NMMGR. If the node can use more than one link to reach another node, the link used is the link that is up with the highest value in the Entry Priority field of the Router Reachable Nodes configuration screen. The other configured links are the alternate links.

If the destination node is a member of the same network as the node that detects the downed link, the selected link is an alternate link configured for the destination node. If the destination node is not a member of the same network, the selected link is an alternate link configured for the appropriate gateway to the destination node (the local destination).

Example 1: Automatic Rerouting. In Figure 3-4, LINK1 has been configured at NODEA ("Node A") as the first link to use to reach NODEC (because LINK2 is a slower link than LINK1). LINK2 has been configured as the second link to use. At NODEB, LINK3 has been configured as the first link to use to reach NODEC, with LINK4 as the second link to use. If there is a transaction between NODEA (the source) and NODEC (the destination), the packets would be transmitted over LINK1 and LINK3. If LINK3 is down, NODEB will automatically reroute the packets over LINK4 (Figure 3-5).

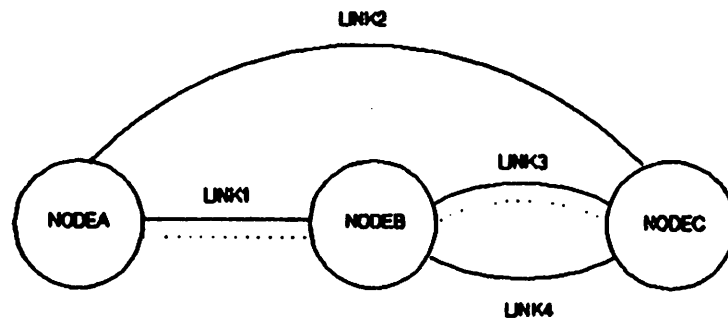


Figure 3-4. Router Network with Alternate Links

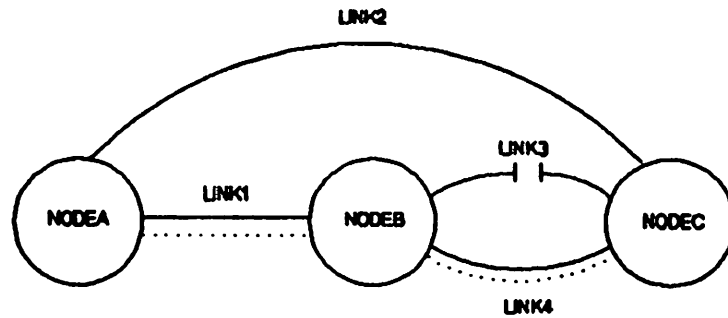


Figure 3-5. Router Network with Rerouting

Example 2: Non-Detecting Nodes. As previously noted, only the nodes that detect the downed link can select an alternate link.

If a packet is rerouted (by a node that detected a downed link) to a node that did *not* detect the failure, the node that did not detect the failure will not automatically reroute the packet over a different link than that used originally. This is because the node that did not detect the failure has no way of knowing of the downed link.

Figure 3-6 illustrates this situation. Figure 3-6 is similar to Figure 3-5, except that there is only one link between NODEB and NODEC (LINK3). Again, NODEA has LINK1 configured as the first link to use to reach NODEC, with LINK2 as the second link to use. NODEB has LINK3 configured as the primary link to use to reach NODEC, and LINK1 as a secondary link. (LINK3 has a higher number configured for its Entry Priority than LINK1.) In this network, if there is a transaction between NODEA (the source) and NODEC (the destination), and LINK3 is down, packets would not reach NODEC. Although packets will be rerouted from NODEB over LINK1 to NODEA, and NODEA could use LINK2 to reach NODEC, the packets will not be rerouted because NODEA has no knowledge of the failure of LINK3.

A variation would exist if NODEB did not have an alternate route to NODEC configured (i.e., LINK1). In this case, no automatic rerouting would occur. Packets would not be rerouted to NODEA from NODEB.

In both of the above situations, a timeout error would eventually occur for the connection. An error message indicating this would appear at NODEA, the source node.

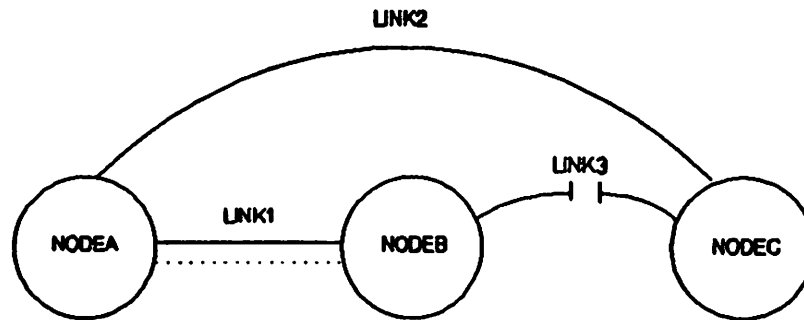


Figure 3-6. Packets from NODEA to NODEC are not rerouted.

Adjusting for Non-operational Links. If a link is either shut down via NETCONTROL or if it fails, the routing tables used by each affected intermediate node will reflect inaccurate information in that the tables will indicate that the non-operational link should be used.

To change these routing tables so that messages are not sent out over downed links, you can reconfigure the routing information entered via NMMGR. The reconfigured routes should include only those links that are operational. Use the online configuration branch of Guided Configuration to most easily make required changes.

In the above situations, (Example 2), the node manager could use the online configuration branch of NMMGR Guided Configuration and the NETCONTROL UPDATE command to change a node's router network tables. For the situation in which an alternate route to NODEC is configured at NODEB but not at NODEA, the manager could change NODEA's configuration to indicate that LINK2 should be used to reach NODEC.

For the situation in which no alternate route to NODEC is configured at NODEB, the manager could change NODEB's configuration to indicate that LINK1 should be used to reach NODEC. NODEA would also need to have LINK2 configured as the link to reach NODEC for packets from NODEB to reach NODEC.

Effect on Internet Transactions. Packets will be rerouted in a router network even if the source and destination nodes are not members of that router network.

As noted previously, if the destination node is not a member of the same network, the alternate link will be another link configured for the appropriate gateway to reach the destination node.

For example, in Figure 3-7, packets from NETX arriving at NODEA to NETZ will be rerouted around LINK3 to get to NODEC, the gateway to NETZ.

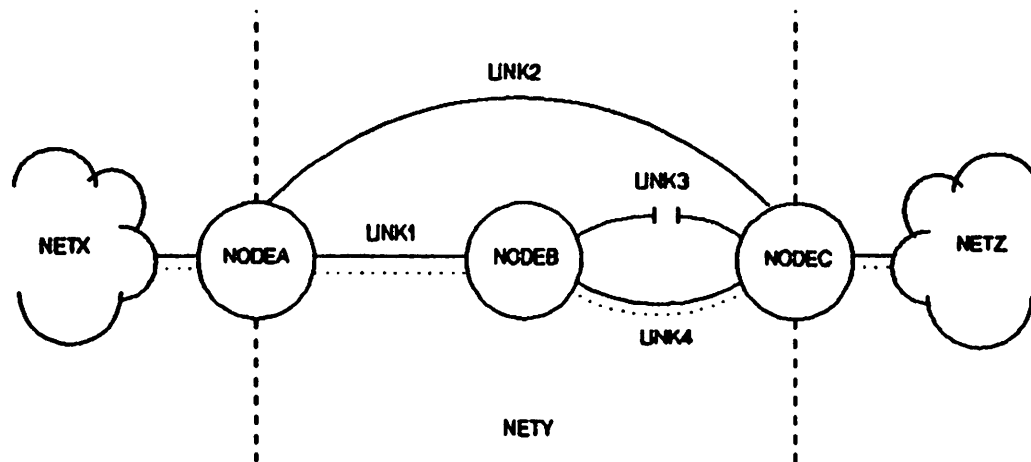


Figure 3-7. Packets forwarded through NETY are rerouted.

Router Network Automatic Rerouting Summary. In summary, router network automatic rerouting has the following characteristics:

- Only the nodes that detect the downed link can select an alternate link.
- Automatic rerouting occurs when the node (or nodes) that detects a downed link can use an alternate route to reach the destination node or appropriate gateway.
- If other nodes are affected by a downed link and have alternate links that they can use, the operator can intervene and manually change the routing table at that node.
- Packets will be rerouted in a router network even if the source and destination nodes are not members of that router network.

Internet Redirection

Internet redirection is the redirection of packets from one gateway to another gateway. If a gateway's link to a remote network is down, and the gateway's configuration file indicates another gateway on the local network that can reach the remote network, the first gateway will rebuild its internet routing table to show the other gateway as the gateway to use to reach the remote network.

This facility can be used to compensate for a gateway's downed link by redirecting packets to another gateway. If a gateway receives a packet for a remote network and its internet routing table shows another gateway (on its network) to use to reach the remote network, IP will redirect packets to the remote network through the other gateway. The other gateway is called the redirect gateway. This redirection will occur even if the redirect gateway and the source node are not on the same network.

Example 3: Internet Redirection. For an example of what happens when an internet packet is redirected, refer to Figure 3-8.

As shown, NODEC and NODEB are gateways to NETZ. At NODEB, NODEC is configured as the gateway to use to reach NETZ. NODEC is configured as a member of NETY and NETZ, and has

LINKCE configured as the link to reach NODEE. NODEC also has NODED configured as a gateway to reach NETZ.

A packet from NODEB to NODEE would take the following path:

NODEB to NODEC
NODEC to NODEE

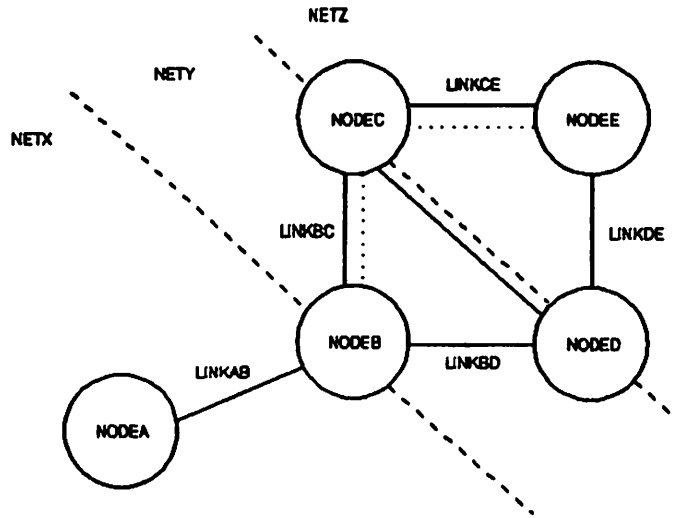


Figure 3-8. Packets from NODEB to NODEE go through NODEC.

If LINKCE goes down (Figure 3-9), NODEC will rebuild its internet routing table to show that packets to NETZ should be routed to NODED. If NODEC then receives a packet with NODEB as the source node and NODEE as the destination node, NODEC will redirect the packet to NODED. A packet from NODEB to NODEE would then take the following path:

NODEB to NODEC
NODEC to NODED
NODED to NODEE

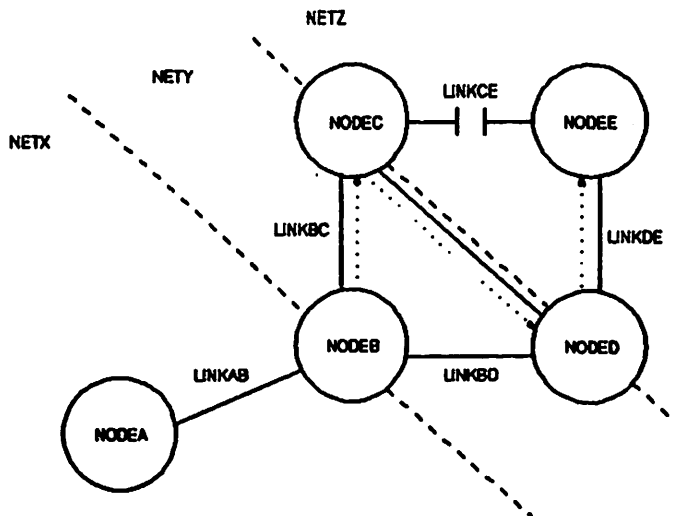


Figure 3-9. NODEC redirects packets for NODEE to NODED.

If redirected packets must go through a node that has no knowledge of the downed link, the packets may not reach the alternate gateway. For example, if the link between NODEC and NODED did not exist, packets redirected by NODEC would have to be sent to NODEB. However, NODEB has no knowledge that LINKCE is down. NODEB will therefore not forward the packets to NODED. Because no packets will ever arrive at NODEE, a timeout will eventually occur for the connection. An error message indicating this would be displayed at the source node, NODEB.

In the above situation, the node manager at NODEB could use the online configuration branch of NMMGR Guided Configuration and the NETCONTROL UPDATE command to change NODEB's internet routing tables so that NODEB will route packets for NETZ to NODED.

Redirection of Subsequent Packets on IEEE 802.3 Networks. If a gateway on an IEEE 802.3 network receives a packet that it redirects to another gateway, it also sends a message to the source node telling it to route subsequent packets for the remote network through the alternate gateway. Such a message, informing a node that all future communication should occur through another gateway, is called an ICMP (for Internet Control Message Protocol) redirect message. Redirect messages will be sent only if the source, original gateway and redirect gateway are all on the same IEEE 802.3 network.

When the source node receives the redirect message, it will alter its internet routing table to show the redirect gateway as the gateway to use to reach the remote network. Subsequent packets from the source node to the remote network will be sent directly to the redirect gateway.

Alterations to the internet routing table based on redirect messages are temporary. If any event occurs that causes that node to rebuild its internet routing table (link up, fails, link started or deleted, network interface started or shut down, NETCONTROL UPDATE command), the node will rebuild the table based on NMMGR configuration values that were read when its network interfaces were started (or the last NETCONTROL UPDATE command was entered). If, because a link is still down, a gateway sends a redirect message to the node, the node will again alter its internet routing table.

Note that the redirect gateway will be entered in the internet table even if the source node did not have the redirect gateway originally configured as a gateway.

Example 4: Redirect Messages. Refer to Figure 3-10 for an example of a redirect message being sent on an IEEE 802.3 local area network. As shown in Figure 3-10, NODEB has been configured so that a packet from NODEB to NODEE would take the following path:

NODEB to NODEC
NODEC to NODEE

If LINKCE were down, NODEC would rebuild its internet routing table so that NODED is the gateway to NETZ. If NODEC then receives a packet with NODEB as the source node and NODEE as the destination node, NODEC will redirect the packet to NODED. NODEC will also send an ICMP redirect message to NODEB. NODEB will update its routing table so that NODED is the gateway to NETZ, and will send subsequent packets to NODEE through NODED.

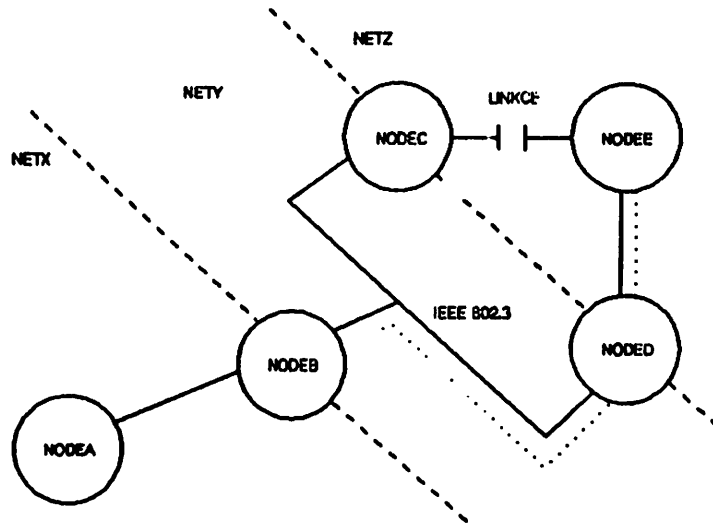


Figure 3-10. Packets from NODEB to NODEE go through NODED.

Note that ICMP redirect messages are sent only when the IP protocol determines that the source, gateway and redirect gateway node are members of the same IEEE 802.3 network. IP determines network memberships in this situation according to the IP addresses used for the transaction. If the source node has more than one IP address (it is a member of more than one network), and it must use a gateway to reach the destination node, the source node will select its IP address so that the network portion will match the network portion of the gateway's IP address.

In Figure 3-11, a packet is sent from NODEA to NODEE, and LINKCE is down. Since NODEA (the source) is not on the same network as NODEC, no redirect message would be sent. A packet from NODEA to NODEE would take the following path:

- NODEA to NODEB
- NODEB to NODEC
- NODEC to NODED
- NODED to NODEE

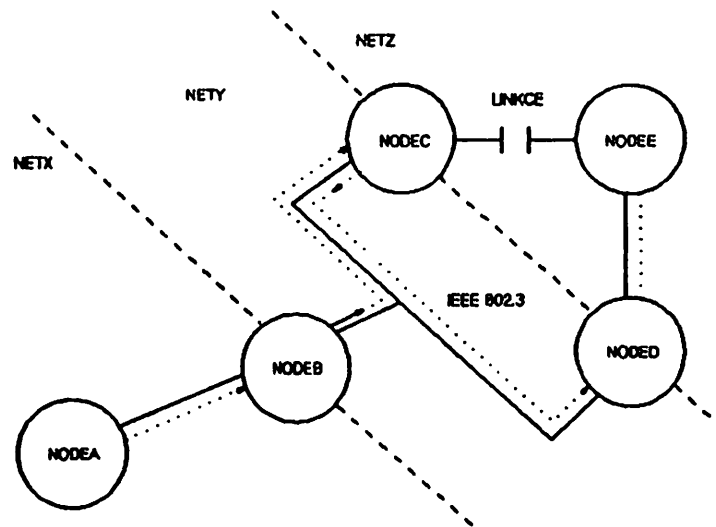


Figure 3-11. Packets from NODEA to NODEE go through NODEC and NODED.

However, once a message originating from NODEB was sent to NETZ, NODEB would receive a redirect message and NODEB would update its internet routing table so that it used NODED as the gateway to NETZ. Subsequent packets originating from either NODEA or NODEB would then be sent to NODED on their way to NETZ.

Internet Rerouting Summary. In summary, internet rerouting has the following characteristics:

- If a gateway's link to a remote network is down, and the gateway had another gateway on its network configured to the remote network, it will rebuild its internet routing table to show the other gateway as the new gateway to the remote network.
- If a gateway receives a packet for a remote network and its internet routing table shows another gateway (on its network) to use to reach the remote network, IP will redirect packets to the remote network through the other gateway (the redirect gateway). This redirection will occur even if the redirect gateway and the source node are not on the same network.
- If a gateway on an IEEE 802.3 network receives a packet that it redirects to another gateway, it also sends a redirect message to the source node if IP determines that the source, gateway and redirect gateway are all on the same IEEE 802.3 network.

NETWORK INSTALLATION AND ADMINISTRATION

Many tasks must be completed before a network or catenet is ready to operate. If there is more than one network (i.e., a catenet is being created), the catenet administrator is responsible for overseeing the completion of the tasks. If you are the catenet administrator or network manager, it is your responsibility to make sure that the configuration of network software at each node is consistent and correct and that software and hardware is correctly installed before catenet or network operation begins. If you are a node manager, it is your responsibility to make sure that the software and hardware installed and configured on your node (or nodes) is correct, and consistent with the plans for the network as determined by the network manager.

Network Planning and Configuration

This section provides an overview of the tasks that must be completed to start network or catenet operation. Details of the steps summarized here can be found in other sections of this manual.

Initial installation can be divided into six main parts:

1. Planning
2. Software and hardware installation
3. Configuration
4. Nodal validation, verification, and synchronization
5. Network startup
6. Line verification

Planning

Planning a network or catenet is an important process that must be done with care to ensure that the network meets the needs of your organization. Many factors must be taken into consideration when planning the network or catenet: for example, volume of usage over particular links, volume of non-network usage of each node, physical layout needs and limitations (such as geographical distances), and desirability of connections to non-NS3000/V nodes. These and other factors are discussed in "Network and Catenet Design" later in this chapter.

This manual contains worksheets that you can use to assist in network and catenet planning and configuration. You should already have a network design (including physical topology and types of links) in mind before you use the worksheets. However, you will need to draw a plan of the network, called a network map, before you begin filling out the worksheets. An example of a network map and specific directions for creating your own map are included in "Configuration Worksheets" later in this chapter.

Software and Hardware Installation

After you have determined the network or catenet's design, software and hardware must be installed on each node. Make sure that each node has the following hardware, as appropriate, for the particular kind of link:

- Hardware interface card(s). For NS Point-to-Point 3000/V links this is an INP; for StarLAN/3000, and ThinLAN/3000 (including ThickLAN option) links this is a LANIC; for NS Asynchronous SERIAL Network links, this is an ATP.
- Cables. For NS Point-to-Point 3000/V and NS Asynchronous SERIAL 3000/V links, this is hardware cable for whatever length necessary to reach between every pair of nodes. For ThinLAN/3000 this is .18 cm. coaxial cable; for ThickLAN this is .4 cm. coaxial cable. For StarLAN/3000, this is unshielded twisted-pair wire. If any nodes are dial (modem) links, you will need cable to connect the modem with the HP 3000.
- Modems and other dial link devices. You will need a modem for each telephone line that a node is connected to. If desired, and if it is not a function performed by your modem, you might also

need a device that performs automatic dialing (usually called an autocal unit). See Appendix B for a list of supported modems and autocal units.

- **Other hardware.** You may need additional hardware, depending upon the types of links you plan to install. For example, ThickLAN links require devices called MAUs (Media Attachment Units). Networks using StarLAN/3000 might require a device called a Bridge. Refer to the hardware installation manuals listed in the Preface of this manual for detailed hardware requirements of the type of network you are installing.

The node must have the following software installed before configuration and subsequent network startup can occur:

- The software products that are provided on MPE Fundamental Operating System (FOS) tapes
- The software provided on a subsystem tape containing NS3000/V link product software and services, if applicable.

Configuration

Network configuration tasks must be completed on each node on the network or catenet. Network configuration consists of using two utilities: SYSDUMP, which should be installed on your HP 3000, and is used for configuration of non-network hardware devices as well as network devices, and NMMGR, which is used to configure NS3000/V software.

SYSDUMP Configuration

Specifically, SYSDUMP allows you to configure:

- Logical device (LDEV) numbers to refer to hardware peripherals, including communications cards;
- Virtual terminal (VTERM) numbers to correspond to virtual terminals, software that simulates the function of terminals;
- MPE system table resources.

NMMGR Configuration

NMMGR allows you to configure items such as:

- Node names and addresses
- Link types (so that network software responds in accordance with the hardware providing the link to another node)
- Buffer sizes
- Timeout values
- Preferred point-to-point routes to get from one node to another
- Intranet and internet routes
- Network directory entries
- Probe proxy server nodes
- Logging parameters, such as which subsystems should be logged

Guided Configuration and Manual Configuration. NMMGR provides two methods of configuring a node: with Guided Configuration, or through *manual configuration*. Guided Configuration enables you to configure the network more quickly by automatically using default values for certain required configuration parameters, and by automatically bypassing certain optional configuration tasks. To accomplish any of the tasks bypassed by Guided Configuration, you will need to use manual configuration. Also, to configure the network directory, you will need to use manual configuration.

NOTE

HP strongly recommends that you use Guided Configuration to initially configure each node, and for most network maintenance and updating. Use manual configuration *only* if Guided Configuration does not provide access to the configuration data you need to change.

The defaults used by guided configuration are the defaults indicated in Sections 7 through 13 of this manual.

Manual configuration with NMMGR can be divided into five parts:

- Link configuration.
- Configuration of Network Transport parameters that must be completed for every node, regardless of link type. This is referred to as transport configuration.
- Network Interface (NI) configuration. This consists of configuring parameters used by each of the node's network interfaces. These parameters differ for different types of links, so NI configuration is separated from configuration of Network Transport items that must be configured for all link types. If a node is a gateway (either full or half), separate NI configuration is needed for each of its links (one for each network or gateway half link).
- Logging configuration. Logging configuration for each NS3000/V subsystem can be configured during this portion of network configuration tasks.
- Network directory configuration. Configuration of each node's network directory (for nodes on router networks, proxy server nodes on IEEE 802.3 networks, and for full or half gateway nodes) consists of entering node names, their IP address(es), and the protocols used on each node.

Section 5 of this manual explains how to use NMMGR. Section 6 explains how to use guided configuration; sections 7 through 13 illustrate the interface displayed when manual configuration is used. Section 14 shows and describes the interface used for configuring the network directory. Sections 6 through 14 all explain the parameters you need to configure for each configuration task.

Nodal Validation, Verification, and Synchronization

After a node's network hardware and software has been installed and it has been configured using SYSDUMP and NMMGR, certain tests need to be performed to ensure that the software and hardware are operating correctly. These tests should be performed before the Network Transport is started.

Each node manager should perform the following tests on his or her node:

- Validation of the configuration files using the NMMGR Validate Configuration File screen. This validation utility, which is part of NMMGR, is described in Section 5. It checks that certain configuration file items are correct and consistent.
- Synchronize network directories on each node. The network manager (or catenet administrator, for a multi-network catenet) should make sure that every network directory is the same. HP

recommends that you accomplish this by physically giving tapes containing copies of a master network directory to the node managers of every node that will contain a network directory. This master network directory should be configured by the network manager (or catenet administrator) on a node that is designated the Central Administrative Node--which means that it will always contain the most up-to-date version of the network directory. This node's network directory should actually be a catenet directory--it should contain entries for each node in the catenet.

If a protocol and addressing information for a particular node is missing from a network directory, messages will not be able to reach that node in cases in which their correct transmission depends on receiving information from that network directory.

NOTE

If configuration files created with a previously released version of NMMGR currently reside on your system, you must convert the files so that they are compatible with the current version of NMMGR and other Node Management Services software. A utility called NMMGRVER can convert your files; Appendix C of this Volume describes NMMGRVER and explains how to use it.

Network Startup

After the node manager has determined that the network software on each node is functioning correctly, the network can be started. To start the network, you must issue the following commands on each node:

- NETCONTROL to start the Network Transport software
- NSCONTROL to start Network Services

The syntax and use of these commands is described in Volume II, Section 1 of this manual.

Line Verification

After each node's Network Transport software has been started, the network manager (and, if applicable, the catenet administrator) should perform the line verification tests described in Volume II, Section 2 of this manual. These include:

- Start software loopback.
- Test the operation of Network Transport by performing the IPC and XPT line tests.
- Use the QuickVal utility to check for correct operation of Network Services.

- Start other network interfaces (either on this node or other nodes); use the NSLOGON diagnostic to ensure that connectivity exists between network interfaces.
- If desired, perform the IPC, XPT, and QuickVal tests to test for connectivity to remote nodes.

NETWORK AND CATENET DESIGN CONSIDERATIONS

Network and catenet design must take many factors into consideration: the desired physical location of the computers comprising the network or catenet's nodes; the volume of projected communications traffic between nodes; communications traffic patterns; and the possibility of connections to other nodes (such as those in a public data network) are just some of the criteria to consider.

These factors will affect your choice of NS network type (IEEE 802.3, router) as well as choice of specific links. You may also want to consider using DS-Compatible links for specific purposes, such as satellite or X.25 connections.

Some design decisions depend upon the capabilities of NS links. These capabilities and corresponding restrictions are described in the following sections.

Line Speed

Line speed is a measure of the rate at which data is transmitted by a physical link (usually measured in bits or kilobits per second). The maximum line speed varies among different NS links. Line speed may therefore influence your choice of link. Although line speed does not indicate the exact throughput of a particular link, it can be used on a comparative basis to indicate relative throughput. ThickLAN links have the highest line speed, at 10 megabits/second. StarLAN/3000 links have a line speed of 1 megabit/second. In general, an IEEE 802.3 link will be faster than a point-to-point router link because the bus topology provides a faster routing mechanism than a series of point-to-point hops. Among gateway half and router links, Point-to-Point 3000/V links have higher line speeds than Asynchronous SERIAL Network links due to ASNP protocol limitations. Point-to-Point links using the LAP-B protocol, which allows full-duplex transmission, are faster than links using the BSC protocol, which allows only half-duplex transmission. Links using leased lines will have a higher line speed than links using normal telephone lines.

Consult your HP representative for line speeds and the most up-to-date performance data for various links.

Geographical Location

The geographical location of the computers that will be part of your network or catenet will be an important factor in deciding both the physical topology and the kinds of links comprising the network or catenet.

If all of the nodes you want to connect are located relatively close to each other (in the same building, for example), you might choose to connect them via a ThickLAN or ThinLAN/3000 link. If you wish to connect PCs to the IEEE 802.3 network, you can use ThinLAN/3000 or StarLAN/3000 links to connect one or more PCs to an HP 3000.

Another option for nodes located in the same geographic location are hardwired (direct-connect) router links. You might wish to use a point-to-point router network if the distance between some nodes on the network will be greater than the maximum distance allowed between nodes on an IEEE 802.3 network.

If, on the other hand, you need to connect nodes that are geographically distant--for example, HP 3000s located in different cities--you might choose to connect them via a dial link. For NS dial links, you can choose either an NS Point-to-Point 3000/V or an Asynchronous SERIAL Network link.

Finally, if you need to use satellite transmission, due to the large geographical distance between nodes, or if you need to have access to other nodes on a public or private X.25 network, you might choose to use DS links.

Special Cases

The following sections describe certain design requirements for special situations, such as shared dial links, personal computers, and using non-HP 3000 minicomputers on an NS network.

Dial Links

Shared dial links have two limitations that must be considered when designing a network. First, a shared dial link cannot be used as an intermediate link in a router network. Any other kind of dial link can be used for intermediate links, but shared dial links should only be used to connect leaf nodes--that is, nodes that only receive messages targeted for themselves. Second, shared dial links cannot be used as gateway halves.

Personal Computers

Personal computers (PCs) can be used as nodes by being connected to HP 3000s with ThinLAN/3000, StarLAN/3000, and Asynchronous SERIAL Network links. PCs cannot be used as intermediate nodes in router (Asynchronous SERIAL Network link) networks. Like a shared dial link, a personal computer must be used as a node that receives only those messages targeted for itself.

Other Non-HP 3000 Nodes

Non-HP 3000 minicomputers, such as HP 1000s and HP 9000s, can operate as nodes on NS IEEE 802.3 networks. If you want to include one of these computers in your catenet, it must be part of an IEEE 802.3 network. Router networks must be composed of only HP 3000s (and PCs, if applicable).

DS-Compatible Links

DS/3000 links cannot be used as store-and-forward links on a router network. An HP 3000 can be configured to have both a DS link and an NS link; however, HP recommends that nodes with DS links configured be used as leaf nodes.

Network Interfaces and Design

The network interface (NI), the software that provides an interface between a node and a network, specifies the type and maximum number of links that can be configured for a node. Because a node's network interface(s) determine what links can be configured for the node, links are said to be configured underneath network interfaces.

Remember, there are three kinds of network interfaces (in addition to loopback):

- LAN802.3 for IEEE 802.3 networks
- Router for networks that use point-to-point routing
- Gateway half for nodes that function as gateway halves

Each HP 3000 must have at least one non-gateway half network interface configured. This network interface must be associated with the network to which the system belongs.

Number of Network Interfaces

A node can have up to eight network interfaces configured. For each network interface, the maximum number of links you can configure and the kinds of links possible are determined by the network interface type, as follows:

- A LAN802.3 network interface can have only one IEEE 802.3 link configured under it; however, each IEEE 802.3 link can support a large number of nodes. ThickLAN cable supports up to 100 nodes per segment; ThinLAN cable can be used for up to 30 nodes per segment; and each StarLAN should be used for up to 50 nodes.
- A router network interface can have up to 40 links configured under it. Router links can be NS Point-to-Point 3000/V or Asynchronous SERIAL Network links.
- A gateway half network interface can have only one link configured under it--the gateway half link. Links connecting two gateway halves can be only NS Point-to-Point 3000/V or Asynchronous SERIAL Network links.

Gateways

If more than one (non-loopback) network interface is configured on a node, the network portions of the IP addresses configured for the interfaces should differ to correspond to the multiple networks to which the node belongs.

A network can have up to 16 gateways (combined number of full gateways and gateway halves).

Full Gateways versus Gateway Halves. NS3000/V allows you to choose between connecting two networks with a full gateway, and connecting them with two gateway halves. A full gateway is a node configured as a full member of two (or more) networks. The node is considered a member of each of the networks for which it is configured.

A node that is a gateway half is configured as a member of a network and as a partner of another gateway half. A gateway half link that joins two networks connects two nodes (a gateway half pair) by a point-to-point link (NS Point-to-Point 3000/V or Asynchronous SERIAL Network link). The gateway half link and pair is not considered a network itself. Each of the paired gateway halves is configured as a member of a different network--the two networks to be connected--and as a gateway half on the same gateway half link. Together, the two gateway halves function as a full gateway.

The following subsections explain situations in which you might want to use a gateway half pair rather than a full gateway to connect networks:

Gateways Connecting Router Networks. If you need to connect two router networks, fewer catenet administrative tasks might be required if the networks are connected via two gateway halves rather than one full gateway. A full gateway must possess intranet routing information about nodes on all of the networks to which it belongs; a gateway half, in contrast, needs to possess only intranet routing information for the network to which it belongs. Making a node a gateway half therefore reduces the amount of configuration changes that must be made to it. If the change occurs to the network to which the node's partner gateway half belongs, the node's NSCONF.NET.SYS configuration file does not have to be updated. You might choose to use a gateway half link between two geographically or organizationally distanced networks for this reason, to reduce the amount of information that has to be passed between different network managers.

Gateways Connecting IEEE 802.3 Networks. IEEE 802.3 networks must use gateway halves to connect to adjacent IEEE 802.3 networks in the same catenet. This is because no more than one LAN802.3 network interface can be configured per node.

Network Boundaries

The term network boundary refers to the divisions between multiple networks. For example, you might think of two networks in the same catenet as being logically disjoint; hence divided from each other by a network boundary. Nodes in each network, of course, will have the same network address (network portion of the IP address), which will differ on the two networks. The networks will be connected by appropriate link or links; by either a gateway half link or a node acting as a full gateway.

The location of some network boundaries is sometimes dictated by the differences in link types used in two adjacent networks: for example, an IEEE 802.3 local area network must be logically disjoint from a router network. Two such networks, connected by a gateway half link or a full gateway, are separated by a network boundary.

You may wish to establish network boundaries even among links connected by the same link type so that one group of nodes is isolated from another for administrative purposes. For example, you might divide a group of nodes into two router networks instead of one network because you want two different individuals (network managers) to be responsible for each of two smaller groups of nodes. The following are other situations in which it might be useful to establish additional network boundaries:

- Situations in which you want to place nodes that will frequently communicate with each other into the same groups. Such groups might reflect your installation's organization. Separating nodes that need to communicate infrequently can result in less distance, in terms of intranet hops, between nodes that do communicate frequently, resulting in improved performance within each network.
- Situations in which the arrangement and configuration of one group of nodes is not expected to change often, and the arrangement of another group is expected to change fairly often for some extended period of time. Separating the nodes into two networks can isolate the stable nodes

from those whose configuration has to change to reflect the addition or deletion of nodes. Changes made to the frequently changing network need be reflected in additions to only the network directories on the more stable network, instead of to the NSCONF.NET.SYS configuration file for each node.

- Situations in which you want to restrict access to a group of nodes.

Network Implementation and Support Plan

Once you have designed your network or catenet, your HP representative will submit the design specifications and other information to HP as part of your Network Implementation and Support Plan (NISP). Networking consultants will review the plans for your network and inform your own HP representative of any changes that need to be made to the design for the network or catenet to operate effectively.

Network Maps and Configuration Worksheets

The remainder of this chapter consists of worksheets intended to assist you with both designing your network and preparing to configure your node. Included in the worksheets are instructions on how to construct network and catenet maps that illustrate the network and catenet's design. Creating these maps will enable you to visually check your design.

NOTE

You may wish to use copies of the network and catenet maps you submitted with your NISP for use with the worksheets, instead of redrawing them.

Once you have drawn the map, ask yourself the following questions to make sure your design adheres to the considerations mentioned above:

1. Are all of the nodes in the network within roughly 550 meters of each other?

If so, consider connecting them with ThinLAN/3000 links. The maximum cable length for segments of ThinLAN/3000 cable is 185 meters, with a maximum of three segments connected by repeaters.

2. Are all of the nodes in the network within roughly 1500 meters of each other?

If so, consider connecting them with ThickLAN (thick coaxial cable). The maximum cable length for each segment of ThickLAN coaxial cable is 500 meters, with a maximum of three segments connected by repeaters.

3. Are nodes located at remote sites? (For example, in different buildings in the same city, or in different cities?)

If so, consider installing a router network using dial links or leased lines. Choose leased lines if you have a critical need for clear transmission or if the volume of data to be transmitted is relatively large.

4. Is the set of nodes you wish to connect composed of some nodes that are in close proximity to one another (for example, in the same building) and other nodes that are geographically distanced (for example, in different buildings or different cities)?

If so, you may wish to use a combination of HP StarLAN or HP ThinLAN networks (for nodes that are located near one another) and dial links (for nodes in different buildings or cities).

5. Do you need to connect personal computers to the network?

If so, proceed to the following questions:

(a) Do you want some personal computers to communicate directly with each other without having to go through an HP 3000?

If so, consider either HP StarLAN or HP ThinLAN. Networks of personal computers can be created using HP StarLAN or HP ThinLAN links. One or more of the personal computers can also be connected to one or more HP 3000s using StarLAN/3000, an HP StarLAN Bridge, or ThinLAN/3000 links.

(b) Will you need to connect personal computers to HP 3000s over dial links (if, for example, personal computers are located at remote sites)?

If so, choose the HP SERIAL Network.

6. Will HP 9000s, HP 1000s, or other minicomputers (such as Digital Equipment VAX (TM) minicomputers) need to be part of the network?

If so, you will need to use them as nodes on a coaxial cable local area network (HP ThinLAN or its ThickLAN option).

7. Do you need access to nodes on public or private X.25 networks?

If so, consider using DS/3000 X.25 links.

8. Do you need to use satellite connections (because of distance and speed requirements)?

If so, you will need to use DS/3000 Satellite links.

9. Is a subset of nodes either geographically or organizationally distanced from another subset of nodes?

If so, you may wish to establish a network boundary between them in order to make them two separate networks joined by a full gateway or two gateway halves.

10. If you decide to connect two networks via a gateway, would it be administratively easier (and require less configuration if changes occur) to join the two networks by a gateway half link rather than a full gateway?

11. If you have decided you need an IEEE 802.3 network, do you need to connect any nodes on it with nodes that are part of another IEEE 802.3 network?

If so, one of the nodes on the IEEE 802.3 network must be a gateway half which connects to another gateway half that is a node on the remote IEEE 802.3 network.

12. If you need to use a gateway half, is the partner gateway half in the same building or further away?

If the two gateway halves are in the same building, you can use a direct connect link between them. If the two gateway halves are further away, you will need to use a dial link or leased line between them.

CONFIGURATION WORKSHEETS: TERMINOLOGY

Here are brief descriptions of some key terms used in the "Configuration Worksheets: Instructions" subsection, which follows.

catenet--A set of interconnected networks.

central administrative node--A node on a non-LAN network designated for keeping an up-to-date network directory.

full gateway--A node that belongs to more than one network and can communicate with each network to which it belongs by using store and forward. A full gateway has one IP address for each network.

gateway--A term that refers to either a full gateway or a gateway-half pair.

gateway half--A node that belongs to at least one network and also has a gateway half network interface configured. The gateway half network interface includes a point-to-point link connecting the node to another gateway half node, called a partner gateway half. Together, the gateway half partners function as a full gateway by performing store and forward over their connecting link.

gateway-half link--A term that refers to a point-to-point link connecting two gateway-half nodes.

gateway-half pair--A term that refers to two gateway half nodes connected by a point-to-point link and together functioning as partners to act as a full gateway.

internet hop count--The number of full gateways plus the number of gateway-half links that a packet must pass through in moving from one network to another.

internet routing--The routing of a packet from one network to another network.

intranet hop count--The number of intervening nodes on a router network between a source node and destination node.

intranet routing--The routing of a packet from one node to another node on the same network.

IP address--A complete IP address comprises a network address and a node address. The network address identifies a network, and the node address identifies a node within a network. IP addresses are divided into three classes. Each class accommodates a different number of network and node addresses. IP network addresses can be obtained from the HP Network Administration Office to guarantee unique network addresses. IP node addresses can be assigned according to your own needs but they must be within the ranges for the IP address class you are using.

link name--The name of a gateway-half link or a router link. The link name can contain as many as eight characters. All characters except the first can be alphanumeric; the first character must be alphabetic.

network--A group of computers connected so that they can exchange information and share resources.

network directory--A repository with connection information about all nodes in a catenet.

network name--The name of a network in your catenet. This name can contain as many as eight characters. All characters except the first can be alphanumeric; the first character must be alphabetic.

node--A computer in a network.

node name--A node name consists of three fields, each separated by a period:

node.domain.organization

When specifying a node name, you must enter the delimiting periods. Each field can contain as many as 16 characters (alphanumeric, underscore or hyphens); the first character must be alphabetic.

point-to-point link--A link connecting either two nodes in a router network or two gateway halves.

proxy server--A node on a LAN which provides network directory information to a requesting node on the same LAN.

CONFIGURATION WORKSHEETS: INSTRUCTIONS

You should use configuration worksheets to help you carefully plan your catenet and to make the NMMGR configuration process as easy as possible. HP recommends that you use all worksheets, even if you are an experienced user. The term worksheets is used loosely here and pertains to maps, tables, and sheets where you will list values you plan to configure.

Figure 1 is an overview of the worksheet process and depicts a catenet with a four-node LAN, a three-node router network, and two gateway halves that form a gateway-half pair. You will need one set of worksheets for your catenet, one set of worksheets for each network in your catenet, one set of worksheets for each gateway-half pair in your catenet, and one set of worksheets for each network interface on each node. Appendix A contains worksheets you will need. Keep the sheets in Appendix A intact, but make copies of the sheets as needed.

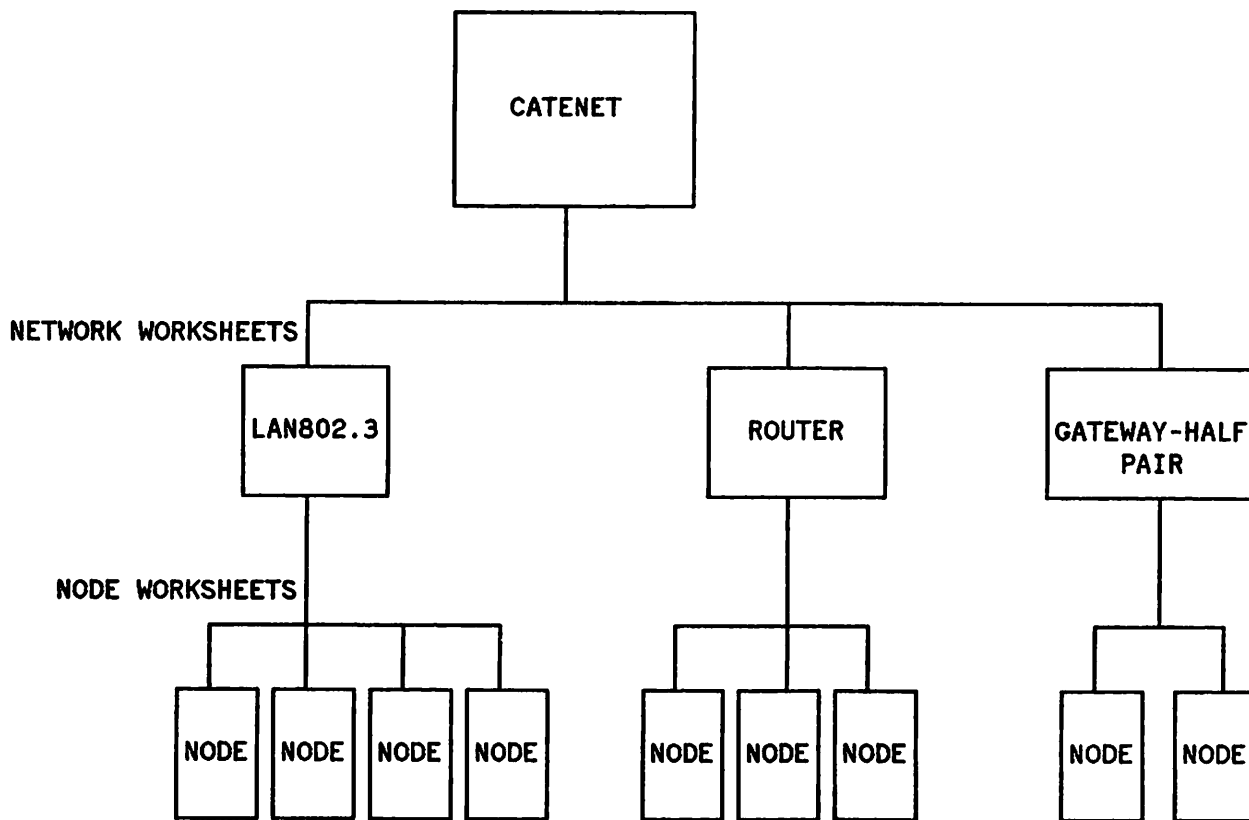


Figure 1. Overview of Worksheet Process

You should complete the catenet worksheets first because the network worksheets and gateway-half pair worksheets are derived from information on the catenet worksheets. Node worksheets are derived from information on the catenet, network and gateway-half pair worksheets.

We will illustrate the instructions that follow by completing some sample worksheets. The table numbers and figure numbers we reference will be based on an example.

Catenet Worksheets

The catenet worksheets consist of a catenet map, used to show an overview of your catenet, and a catenet table. You will take the following steps when filling out the catenet worksheets.

- Draw sketches of each network in the catenet (Catenet Map)
- Write network names, IP network addresses and network types (Catenet Map)
- Draw gateway nodes (Catenet Map)
- Indicate network boundaries (Catenet Map)
- Complete Catenet Table (Table 1)

Catenet Map

Figure 2 is an example of a catenet map. We will use this sample catenet throughout the instructions to help explain the other drawings and tables that make up the configuration worksheets.

Before you can draw your catenet map, you must know how many networks your catenet will contain, and you must know each network type (router or LAN). The catenet in our example (Figure 2) contains three networks. NET1 is a LAN, NET2 is a router network and NET3 is a LAN.

You must decide where you want your networks to be physically located and how they will be physically connected. Therefore, you must determine which nodes will be used as gateway nodes (full gateways or gateway halves) to communicate with remote networks.

Communication Between Networks

Because the main purpose of the Catenet Map is to show how the networks are connected, gateway nodes are the only nodes you should draw on the Catenet Map. All other nodes and their networks can be represented by drawing sketches of the networks, as shown in Figure 2.

In our example, Node C is a full gateway that belongs to NET1 and NET2. Nodes G and H are gateway halves that belong to NET2 and NET3, respectively. Nodes X and Y are gateway halves that belong to NET1 and NET3, respectively.

NOTE

For reasons of simplicity, we have used single letters to represent node names in our example. Actual node names must be of the form listed in the terminology subsection. As for addresses, the network portions of IP addresses used in our examples have been reserved for such use. You should not use C 192.006.001, C 192.006.250, C 192.006.251, C 192.006.252, C 192.006.253 or C 192.006.254 for your actual network addresses.

Network Boundaries

Once you have drawn your gateway nodes, you have established network boundaries.

Let us again consider our example and look at Figure 2. Because Node C in our example is a full gateway and belongs to both NET1 and NET2, the boundary between these two networks is at Node C itself. For purposes of the map, we have drawn this boundary through the middle of Node C. The boundary between NET2 and NET3 is along the gateway-half link that connects gateway nodes G and H. The boundary between NET1 and NET3 is along the gateway-half link that connects gateway nodes X and Y. Network boundaries can be depicted with dotted lines, as we have done in Figure 2.

IP Network Addresses

Each network in your catenet must have a unique IP network address. Add these IP addresses to your catenet map.

In our example, we assume that we have been assigned the Class C IP network addresses shown in Figure 2. The specific IP node addresses do not need to be shown until completion of specific parts of the network worksheets, so we will represent node portions of IP addresses with XXX in some maps and tables.

CATENET MAP

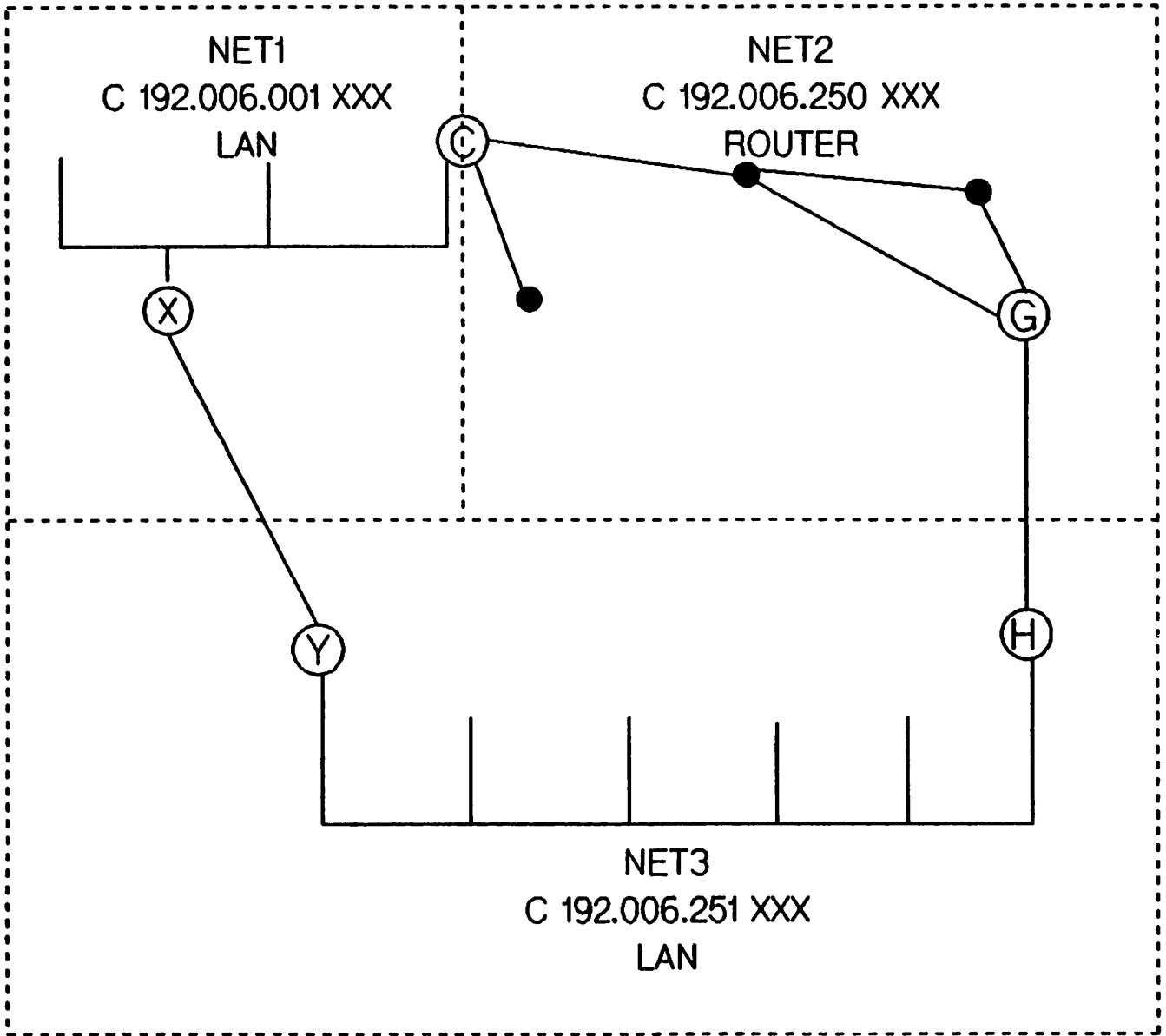


Figure 2. Catenet Map

Completing the Catenet Table

Once your catenet map contains the information just described, you are ready to complete the Catenet Table (Table 1).

The information requested for the first three columns of the Catenet Table can be taken directly from the Catenet Map, as we have done in our example. As for the Implementation Priority column, consider which networks must be operational in as little time as possible. You also may want to consider which

Network Planning and Configuration

networks will be the easiest to initiate. Analyzing these and other factors important to you, determine the order in which you plan to initiate your networks, and then enter the information in the Implementation Priority column of the Catenet Table.

When you have completed both the Catenet Map and the Catenet Table, you have finished the catenet worksheets.

TABLE 1. CATENET TABLE

NETWORK	NETWORK TYPE (LAN, ROUTER)	IP NETWORK ADDRESS	IMPLEMENTATION PRIORITY
NET1	LAN	C 192.006.001 XXX	1
NET2	ROUTER	C 192.006.250 XXX	2
NET3	LAN	C 192.006.251 XXX	3

Network Worksheets

For each network in your catenet, you are asked to draw a map of the network and to complete two tables. One table lists node-specific information, and one table lists network routing information.

You also are asked to complete worksheets for each gateway-half pair in your catenet. The worksheets for a gateway-half pair consist of a map of the gateway-half nodes and their connecting link, and a table containing information about the gateway-half network interfaces.

For our sample catenet, five sets of network worksheets need to be completed--one set for each of the two LANs, one set for the router network, and one set for each of the two gateway-half pairs.

You will take the following steps when filling out a set of network worksheets.

- Draw your map, showing all nodes and node names. (For router networks, also show all router links and link names. For a gateway-half pair, include the link name.)
- Use dotted lines on your map to indicate connected networks.
- Complete the table(s)--two for each network, one for each gateway-half pair.

LAN Network Worksheets

One set of LAN network worksheets should be used for each LAN in your catenet. The LAN network worksheets consist of a map of the LAN and two tables. One table contains information about each node on the LAN, and one table contains network-specific internet routing information. We now refer to NET1, one of the LANs in our sample catenet, to describe the LAN Network Worksheets in detail. Use the discussion of our sample LAN Network Worksheets as a guide for filling out your own LAN Network Worksheets.

LAN Network Map. Figure 3 is a drawing of the network map for NET1. The network map is a more detailed drawing of the same network shown in the Catenet Map (Figure 2). The network name, the IP network address and the network type are listed at the top of the network map. This information is derived from the Catenet Map, which should be kept available at all times.

In our example, the Catenet Map shows that nodes C and X are gateway nodes. We mark them as such on the NET1 network map and draw dotted lines to show the networks that the gateway nodes can reach. We then add the remaining NET1 nodes and their names to the network map. We also indicate that nodes C and X are proxy servers.

LAN NETWORK MAP

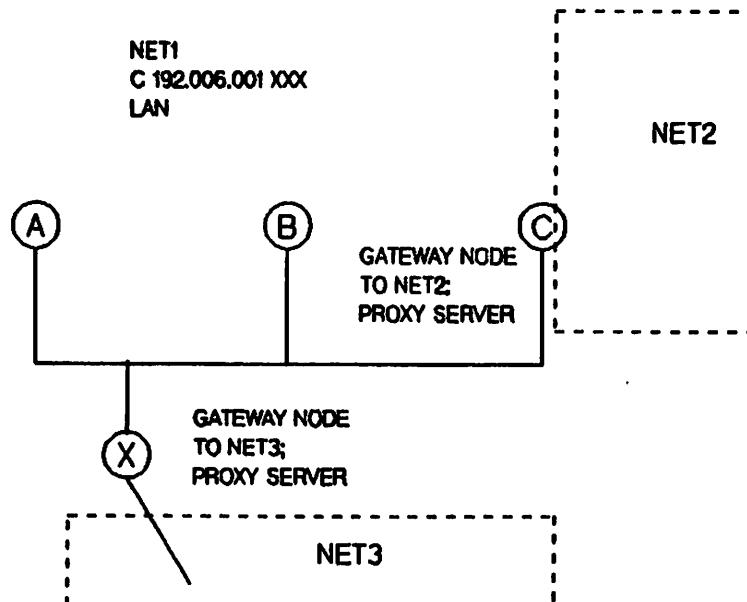


Figure 3. LAN Network Map

LAN Network Table. We refer to the LAN Network Map to fill in the LAN Network Table (Table 2). We complete the first column by listing the names of all the nodes on NET1. We then assign to each node an IP address that is unique within the network. We list only the node portions of the IP addresses because we have listed the IP network address at the top of the table. In the third column of Table 2, we indicate that nodes C and X are proxy servers. In the fourth column, we indicate that nodes C and X also are gateway nodes. For the Implementation Priority column, we rank the nodes in the order we think they should be configured.

TABLE 2. LAN NETWORK TABLE

NETWORK NAME: NET1

IP NETWORK ADDRESS: C 192.006.001 XXX

NODE NAME	IP NODE ADDRESS	PROXY SERVER (Y/N)	GATEWAY NODE (Y/N)	IMPLEMENTATION PRIORITY
A	001			3
B	002			4
C	003	YES	YES	1
X	004	YES	YES	2

Network Planning and Configuration

LAN Internet Routing Table. The purpose of the LAN Internet Routing Table (Table 3) is to list all possible networks that can be reached from each gateway node on a LAN, such as NET1 in our example.

As shown on the Catenet Map, NET1 includes two gateway nodes, C and X. We indicate in our LAN Internet Routing Table that NET1 nodes using Node C as a gateway can reach NET2 in one hop and NET3 in two hops. In the IP Node Address column of the LAN Internet Routing Table, we list the node portion of Node C's IP address.

For Node X, we list the same type of information in the LAN Internet Routing Table.

TABLE 3. LAN INTERNET ROUTING TABLE

NETWORK NAME: NET1

IP NETWORK ADDRESS: C 192.006.001 XXX

THROUGH GATEWAY NODE	IP NODE ADDRESS	DESTINATION NETWORK/ADDRESS	HOPS NEEDED TO REACH DESTINATION NETWORK
C	003	NET2/ C 192.006.250 000	1
		NET3/ C 192.006.251 000	2
X	004	NET3/ C 192.006.251 000	1
		NET2/ C 192.006.250 000	2

NOTE

For NET3, the other LAN in our sample catenet, we follow the same procedures. Figure 5 shows the network map for NET3, and tables 6 and 7 are the network and internet routing tables for NET3.

Router Network Worksheets

One set of Router Network Worksheets should be used for each router network in your catenet. The router network worksheets consist of a map of the router network and two tables. One table contains information about each node on the router network, and one table contains network-specific internet routing information. We now will refer to the router network in our sample catenet to describe the Router Network Worksheets in detail. Use the discussion of our sample Router Network Worksheets as a guide for filling out your own Router Network Worksheets.

Router Network Map. NET2 is the router network in our sample catenet. Figure 4 is a drawing of the network map for NET2. The network map is a more detailed drawing of the same network shown in the Catenet Map (Figure 2). The network name, the IP network address and the network type are listed at the top of the network map. This information is derived from the Catenet Map, which should be kept available at all times.

In our example, the Catenet Map shows that nodes C and G are gateway nodes. We mark them as such on the NET2 network map and draw dotted lines to show the networks that the gateway nodes can reach. We then add the remaining NET2 nodes and their names to the network map. We also indicate that Node G is a central administrative node.

ROUTER NETWORK MAP

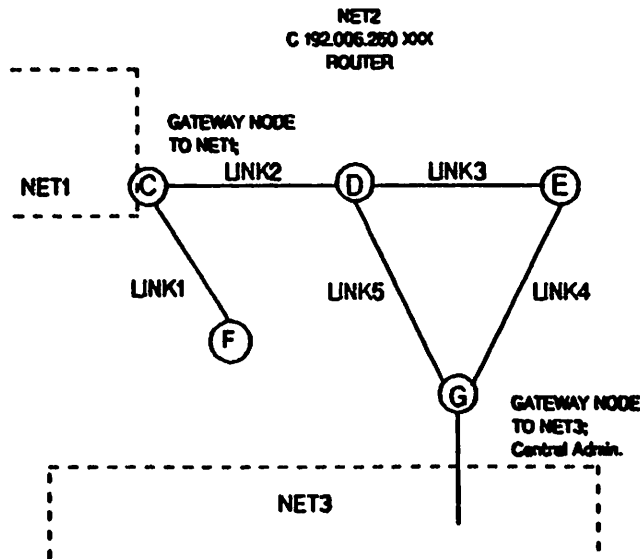


Figure 4. Router Network Map

Router Network Table. We refer to the Router Network Map to fill in the Router Network Table (Table 4). We complete the first column by listing the names of all the nodes on NET2. We then assign to each node an IP address that is unique within the network. We list only the node portions of the IP addresses because we have listed the IP network address at the top of the table. In the third column of Table 4, we indicate that Node G is a central administrative node. In the fourth column, we indicate that nodes C and G are gateway nodes. For the Implementation Priority column, we rank the nodes in the order we think they should be configured.

TABLE 4. ROUTER NETWORK TABLE

NETWORK NAME: NET2

IP NETWORK ADDRESS: C 192.006.250 XXX

NODE NAME	IP NODE ADDRESS	CENTRAL ADMIN. NODE? (Y/N)	GATEWAY NODE (Y/N)	IMPLEMENTATION PRIORITY
C	001		YES	2
D	002			3
E	003			4
F	004			5
G	005	YES	YES	1

Router Internet Routing Table. The purpose of the Router Internet Routing Table (Table 5) is to list all possible networks that can be reached from each gateway node on a router network, which is NET2 in our example.

As shown on the Catenet Map, NET2 includes two gateway nodes, C and G. We indicate in our Router Internet Routing Table that NET2 nodes using Node C as a gateway can reach NET1 in one hop and NET3 in two hops. In the IP Node Address column of the Router Internet Routing Table, we list the node portion of Node C's IP address.

For Node G, we list the same type of information in the Router Internet Routing Table.

TABLE 5. ROUTER INTERNET ROUTING TABLE

NETWORK NAME: NET2
IP NETWORK ADDRESS: C 192.006.250 XXX

THROUGH GATEWAY NODE	IP NODE ADDRESS	DESTINATION NETWORK/ADDRESS	HOPS NEEDED TO REACH DESTINATION NETWORK
C	001	NET1/ C 192.006.001 000	1
		NET3/ C 192.006.251 000	2
G	005	NET3/ C 192.006.251 000	1
		NET1/ C 192.006.001 000	2

LAN NETWORK MAP

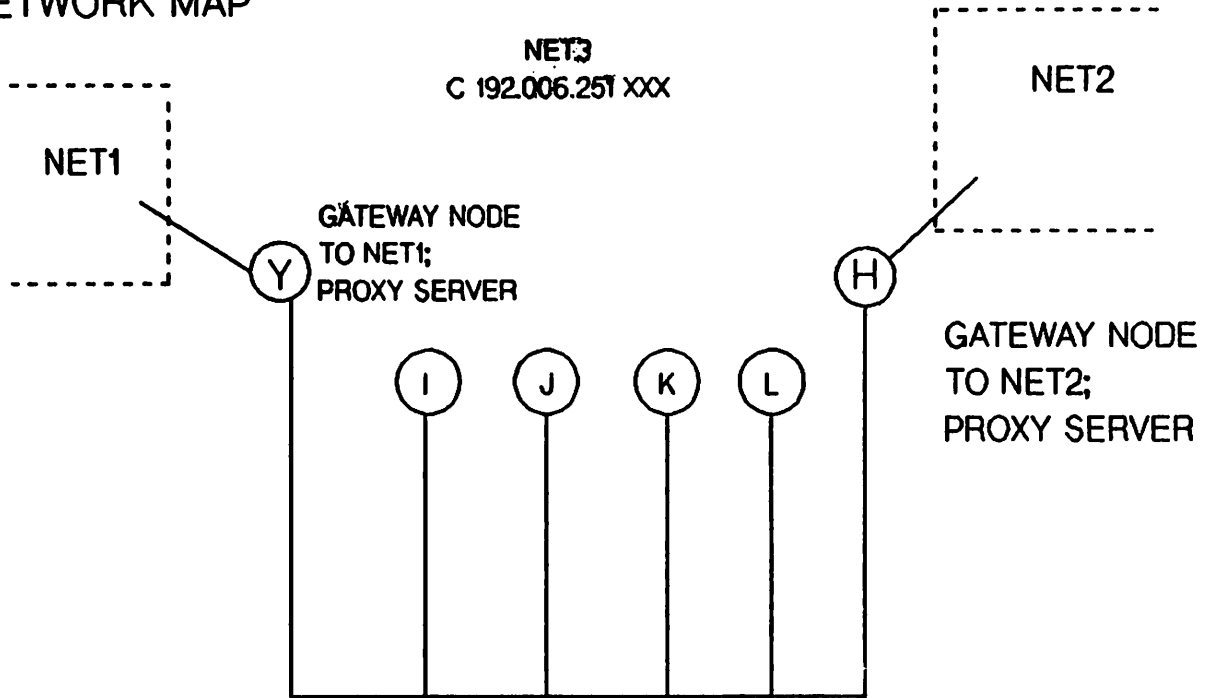


Figure 5. LAN Network Map (NET3 in example)

TABLE 6. LAN NETWORK TABLE

NETWORK NAME: NET3

IP NETWORK ADDRESS: C 192.006.251 XXX

NODE NAME	IP NODE ADDRESS	PROXY SERVER (Y/N)	GATEWAY NODE (Y/N)	IMPLEMENTATION PRIORITY
H	001	YES	YES	1
I	002			3
J	003			4
K	004			5
L	005			6
Y	006	YES	YES	2

Network Planning and Configuration

TABLE 7. LAN INTERNET ROUTING TABLE

NETWORK NAME: NET3

IP NETWORK ADDRESS: C 192.006.251 XXX

THROUGH GATEWAY NODE	IP NODE ADDRESS	DESTINATION NETWORK/ADDRESS	HOPS NEEDED TO REACH DESTINATION NETWORK
H	001	NET2/ C 192.006.250 000	1
		NET1/ C 192.006.001 000	2
Y	006	NET1/ C 192.006.001 000	1
		NET2/ C 192.006.250 000	2

Gateway-Half Pair Worksheets

One set of Gateway-Half Pair Worksheets should be used for each gateway-half pair in your catenet. The Gateway-Half Pair Worksheets consist of a map of the two gateway half nodes and their connecting link, and one table that contains information about the gateway half network interfaces. We now refer to one of the gateway-half pairs in our sample catenet to describe the Gateway-Half Pair Worksheets in more detail. Use the discussion of our sample Gateway-Half Pair Worksheets as a guide for filling out your own Gateway-Half Pair Worksheets.

Gateway Half Map. Our sample catenet contains two gateway-half pairs, as shown in our Catenet Map. One gateway-half pair is made up of nodes G and H and their connecting link, and the other gateway-half pair is made up of nodes X and Y and their connecting link. Let us focus on the G and H gateway-half pair.

Figure 6 is a drawing of this gateway-half pair. We show the two nodes and the networks to which they belong. In addition, we select a name for the link. We have decided to name the link LINKRL1.

GATEWAY HALF MAP

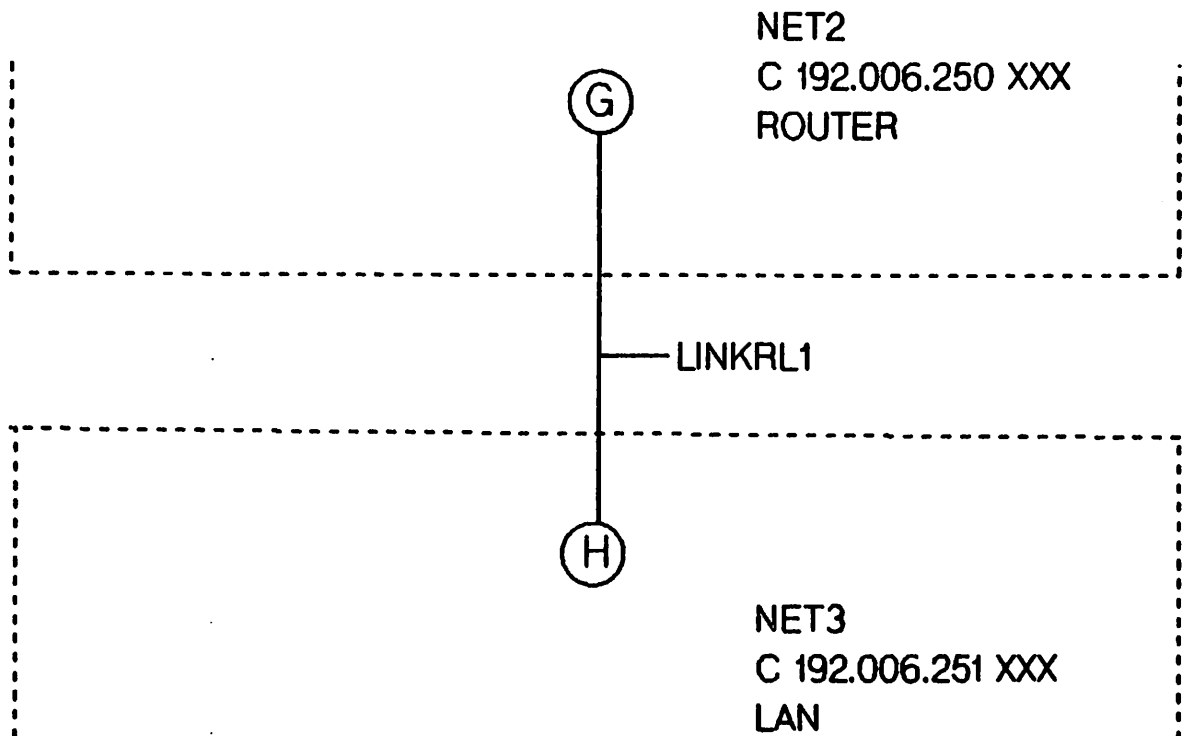


Figure 6. Gateway-Half Map

Gateway-Half Network Interface Table. This table (Table 8) is based on the map we have just discussed. We list both gateway-half nodes, the full IP addresses of the partner nodes, the connected networks, and the name of the link. Usually, the link name will be the same from the perspective of each gateway half. The reason we list the address of the partner gateway half is that the partner's address is entered during configuration of a gateway half network interface.

TABLE 8. GATEWAY-HALF NETWORK INTERFACE TABLE

NETWORK NAMES: NET2, NET3

GATEWAY NODE	FULL IP ADDRESS OF PARTNER	CONNECTED NETWORK	LINK NAME
G/NET 2	C 192.006.251 001	NET3	LINKRL1
H/NET 3	C 192.006.250 005	NET2	LINKRL1

NOTE

Figure 7 and Table 8A pertain to the other gateway-half pair in our sample catenet.

GATEWAY HALF MAP

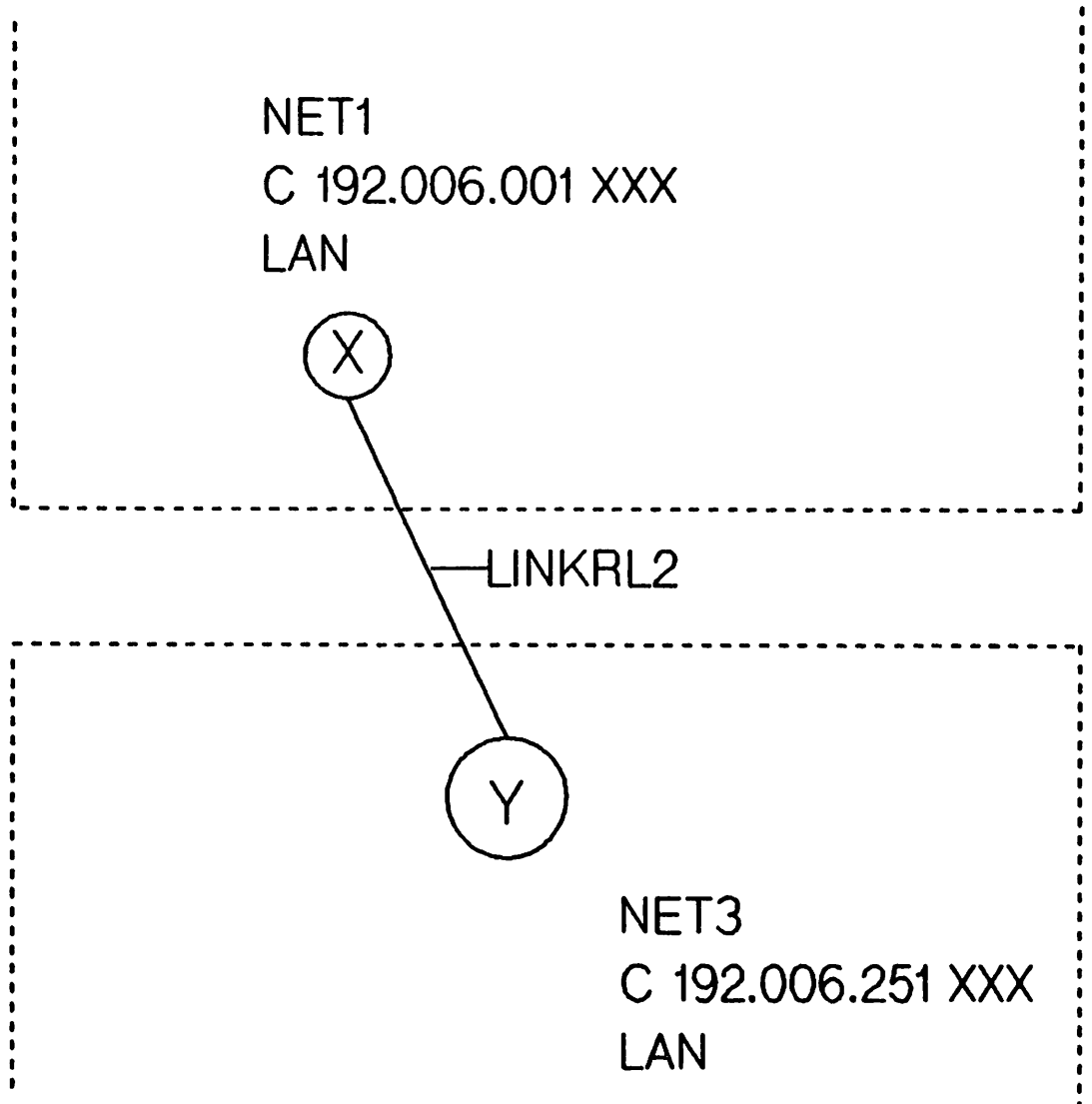


Figure 7. Gateway Half Map

TABLE 8A. GATEWAY-HALF NETWORK INTERFACE TABLE

NETWORK NAMES: NET1, NET3

GATEWAY NODE	FULL IP ADDRESS OF PARTNER	CONNECTED NETWORK	LINK NAME
X/NET 1	C 192.006.251 006	NET 3	LINKRL2
Y/NET 3	C 192.006.001 004	NET 1	LINKRL2

Node Worksheets

The main purpose of the node worksheets is to determine ahead of time the information you will need to configure during NMMGR's Guided Configuration. This information depends on the type of network to which a node belongs. Guided Configuration includes information for routing, links, and protocols.

You take the following steps when you start to complete the node worksheets.

- Fill in the necessary internet routing information (intranet routing information also for nodes on a router network).
- Determine the values for fields you will configure during Guided Configuration.
- Perform the actual Guided Configuration.

Node worksheets contain routing information, screen names, NMMGR paths, fields you will configure, and instructions on how to determine values for these required fields. The worksheets list only the fields you can configure during Guided Configuration, which allows you to configure your nodes as quickly as possible. Detailed descriptions of all fields are located in other sections. Screen names are given in uppercase letters, and the NMMGR path used to reach a screen is listed in parentheses following the screen name. Figure numbers and page numbers are also given.

We will continue to refer to our example as we discuss the node worksheets, and figure numbers and table numbers still will be based on the example. Descriptions of fields should be applicable to all situations.

NOTE

To demonstrate our example, we have filled out values on the following node-worksheet pages based on previous worksheet information. In cases where information could not be taken from previous worksheets, values have been left blank.

Network Planning and Configuration

After you choose to perform Guided Configuration, you select the **Go To NET CON** function key to perform first-time configuration of a node. You then select an NI name and press the appropriate topology function key. For NI names, use the network names on the network maps. This way, you will be able to keep track of the NI names you enter. You will then visit the Node Name Configuration Screen, shown below. (This screen is always visited during loopback guided configuration, but is visited for LAN, router, PC-router and gateway half guided configurations only if a node name has not already been configured.)

NODE NAME CONFIGURATION (NETXPORT.NODE.NAME) Fig 8-3, p. 8-5

Node Name _____

Name of the node you are configuring. Must be in the form *node.domain.organization*.

LAN Node Internet Routing

As an example of a LAN node's routing worksheet, look at Table 9. This table shows the internet routing information that we plan to configure for Node B on NET1 in our example. We see from our LAN Internet Routing Table (Table 3) that NET1 includes nodes C and X as gateway nodes. This table also shows that NET1 nodes can use Node C as a gateway to reach NET2 in one hop and NET 3 in two hops, and that Node X can be used to reach NET3 in one hop and NET2 in two hops. We decide to configure each gateway to reach both networks, which means that more than one gateway is available for Node B to reach the same remote network. We are not required to configure multiple gateways to reach the same network. It is our choice. When multiple gateways are configured, the software determines which route to use--usually the one with the fewest hop counts.

Internet routing information is not necessarily the same for all nodes on a network. Suppose we do not want Node A in NET1 ever to communicate with any node on NET3. When completing the internet routing table for Node A, we would not list NET3 as a destination network and we would not use Node X as a gateway node because it would route packets to NET3.

TABLE 9. LAN NODE INTERNET ROUTING

NODE NAME: B
 IP ADDRESS: C 192.006.001 002
 NETWORK NAME: NET1

GATEWAY NODE/IP ADDRESS	DESTINATION NETWORKS/ IP ADDRESSES	HOP COUNT
C/ C 192.006.001 003	NET2/C 192.006.250 000	1
	NET3/C 192.006.251 000	2
X/ C 192.006.001 004	NET2/C 192.006.250 000	2
	NET3/C 192.006.251 000	1

LAN CONFIGURATION SCREENS

As an example of filling out configuration fields for a LAN node, we have chosen Node B on NET1. Only information derived from previous worksheets has been filled out.

LINK CONFIGURATION (LINKCONF) Fig. 7-1, p. 7-4

Link Name _____

Assign a link name that is eight alphanumeric characters or fewer; the first character must be alphabetic.

IEEE802.3 LINK DATA (LINKCONF.*linkname*) Fig. 7-2, p. 7-6

Logical Device _____

The ldev number of the LANIC that will be configured in SYSDUMP.

PROBE PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.PROBE) Fig. 9-4, p. 9-10

Proxy Enabled N _____

Answer Y if this node will be a proxy server (will have a network directory). Refer to the LAN1 Network Map (Figure 3).

IP PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.IP) Fig. 9-3, p. 9-7

IP Address C 192.006.001 002 _____

Full IP address of the node being configured. Refer to LAN Network Table (Table 2).

Note: This page contains information for one gateway. Additional gateways need their own information, but we will focus on only one gateway for this example. During Guided Configuration, press the **Next Screen** function key when finished configuring information for a gateway. This returns you to the first screen shown on this page. If you are finished for all gateways, press the **Next Screen** key again.

LAN CONFIGURATION SCREENS (cont'd)

NEIGHBOR GATEWAYS (NETXPORT.NI.*niName*.INTERNET) Fig. 9-7, p. 9-18

Gateway Name GATEC

Assign a name (maximum eight characters) to reference a gateway that is on the network to which the node belongs. Refer to Catenet Map (Figure 2) and LAN Network Map (Figure 3).

NEIGHBOR GATEWAY REACHABLE NETWORKS (NETXPORT.NI.*niName*.INTERNET.*gatewayn*) Fig. 9-8, p. 9-19

Neighbor Gateway IP Internet Address C 192.006.001 003

Full IP address of the gateway node. Refer to LAN Network Table (Table 2).

IP Network Address

- C 192.006.250 000 (1)
- C 192.006.251 000 (2)
- (3)
- (4)

The IP addresses of all reachable networks in the catenet, through the gateway node named above. Refer to LAN Node Internet Routing Table (Table 9). We have filled in the node portion for each IP network address with zeroes because the node portion will be ignored in this field during configuration. A node portion still must be entered, however.

Hops

- 1 (1)
- 2 (2)
- (3)
- (4)

Refer to LAN Node Internet Routing Table (Table 9) for Hop Count. The numbers in parentheses correspond to the numbers regarding IP network addresses.

Router Node Routing Information

Tables 10 and 11 show routing information for Node E on NET2 in our example.

Because NET2 is a router network, intranet and internet routing information is needed. Intranet routing is shown in Table 10. Using information from the NET2 network map (Figure 4) and the Router Network Table (Table 4), we obtain the destination node names, the router link names and the IP addresses needed for completing Table 10. Let us look at some examples from Table 10. Node E can reach Node F (IP address C 192.006.250 004) by sending a packet over Link3. This is all the information needed in Node E's intranet routing table for sending packets to Node F. The reason for this is that, once the packet crosses over LINK3 and arrives at Node D, Node D will use its own intranet routing information to continue moving the packet toward its destination node.

Notice the Entry Priority column. This column becomes important when multiple link names are configured. When multiple link names are configured, the highest entry-priority number is the top-priority link. For example, we see from our Router Network Map (Figure 4) that Node E can reach Node D directly by using LINK3 and indirectly by using LINK4 and then LINK5. We decide to configure this indirect link and list it as entry priority 30 in Table 10. Unless LINK3 should go down, LINK4 will never be used because it has a lower priority number than LINK3. We are not required to configure this secondary link. It is our choice. The reason we have used priority numbers 30 and 50 in Table 10 is to allow for possible additions with higher or lower priority numbers; 50 is the default.

TABLE 10. ROUTER NODE INTRANET ROUTING TABLE

NODE NAME: E
 IP ADDRESS: C 192.006.250 003
 NETWORK NAME: NET2

DESTINATION NODE	LINK NAME	DESTINATION NODE'S IP ADDRESS	ENTRY PRIORITY
D	LINK3	002	50
D	LINK4	002	30
G	LINK4	005	50
G	LINK3	005	30
C	LINK3	001	50
F	LINK3	004	50

Now we proceed to Node E's Internet Routing Table (Table 11). Remember that Node E belongs to NET2. We see from our Router Internet Routing Table (Table 5) that NET2 includes nodes C and G as gateway nodes. This table also shows that NET2 nodes using Node C as a gateway can reach NET1 in one hop and NET3 in two hops, and that Node G can be used to reach NET3 in one hop and NET1 in two hops. We decide to configure each gateway to reach both networks, which means that more than one gateway is available for Node E to reach the same remote network. We are not required to configure multiple gateways to reach the same network. It is our choice. When multiple gateways are configured, the software determines which route to use--usually the one with the fewest hop counts.

Network Planning and Configuration

Internet routing information is not necessarily the same for all nodes on a network. Suppose we do not want Node D in NET2 ever to communicate with any node on NET3. When completing the internet routing table for Node D, we would not list NET3 as a destination network and we would not use Node G as a gateway node because it would route packets to NET3.

TABLE 11. ROUTER NODE INTERNET ROUTING

NODE NAME: E
IP ADDRESS: C 192.006.250 003
NETWORK NAME: NET2

GATEWAY NODE/IP ADDRESS	DESTINATION NETWORKS/ IP ADDRESSES	HOP COUNT
C/001	NET1/C 192.006.001 000	1
	NET3/C 192.006.251 000	2
G/005	NET1/C 192.006.001 000	2
	NET3/C 192.006.251 000	1

ROUTER CONFIGURATION SCREENS

As an example of filling out configuration fields for a router node, we have chosen Node E on NET2. Only information derived from previous worksheets has been filled out.

LINK CONFIGURATION (LINKCONF) Fig. 7-1, p. 7-4

Link Name _____ LINK3 _____

Assign a link name that is eight characters or fewer. The first character must be alphabetic. This link name corresponds to one link the node belongs to. After you have been taken to all the necessary screens for this link, Guided Configuration will bring you back to this screen to configure other links connected to this node. Refer to Router Network Map (Figure 4). When you are finished configuring the links for this node, press the **Next Screen** function key.

Type: ASNP, LAP-B or BSC Circle one.

ASNP LINK DATA (LINKCONF.*linkname*) Fig. 7-12, p. 7-27

Logical Device _____

The ldev number that will be configured in SYSDUMP.

OR

LAP-B LINK DATA (LINKCONF.*linkname*) Fig. 7-9, p. 7-19

Logical device _____

The ldev number that will be configured in SYSDUMP.

Local Mode (5=DTE, 6=DCE, 11=HP Point to Point) _____

HP recommends that you use the default, HP Point to Point. If so, both sides of the link must be configured as HP Point to Point.

OR

BISYNC LINK DATA (LINKCONF.*linkname*) Fig. 7-6, p. 7-11

Logical Device _____

The ldev number that will be configured in SYSDUMP.

ROUTER CONFIGURATION SCREENS (cont'd)

NETWORK INTERFACE LINKS (NETXPORT.NI.*niName*.LINK) Fig. 10-6, p. 10-17

Type _____

DD--Direct Dial, DC--Direct Connect, or SD--Shared Dial.

DIRECT CONNECT LINK CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 10-7, p. 10-19

No fields required to configure.

OR

ROUTER DIAL LINK CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 10-8, p. 10-21

No fields required to configure.

ROUTER NETWORK INTERFACE CONFIGURATION (NETXPORT.NI.*niName*) Fig. 10-1, p. 10-3

Network Hop Count _____ 3 _____

The greatest possible number of intermediate nodes between the two nodes farthest apart on the network. See the Router Network Map (Figure 4).

Idle Device Timeout Value (Minutes) _____

For dial links, this is the number of minutes a device can remain inactive before shutting down. A value of zero will disable the idle device timer for all devices on this network interface. (Enter 0 for Direct Connect links.)

IP PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.IP) Fig. 10-3, p. 10-8

IP Address _____ C 192.006.250 003 _____

Full IP address of the node being configured. Refer to Router Network Table (Table 4).

ROUTER CONFIGURATION SCREENS (cont'd)

Note: Mapping configuration is required for each local link the node can use to reach each remote node on the router network. Therefore, make enough copies of this sheet before you fill in any information. After configuring mapping information for one node, Guided Configuration will bring you back to the first screen on this page. Repeat the process until you have completed all mapping configuration, then press the **Next Screen** function key.

MAPPING CONFIGURATION (NETXPORT.NI.niName.MAPPING) Fig. 10-12, p. 10-30

Router Node Name D1

Assign a name (maximum eight characters) to represent a node you wish to be able to reach from your node. Refer to Router Node Intranet Routing Table (Table 10).

ROUTER REACHABLE NODES (NETXPORT.NI.niName.MAPPING.mapentry) Fig. 10-13, p. 10-32

IP Internet Address C 192.006.250 002

Full IP address of the destination node named above. Refer to Router Node Intranet Routing Table (Table 10).

Link Name LINK3

Name of the link used to reach the destination node. Must match a link name that you configured on the link configuration screen. If more than one link is required to reach the destination node, list only the first link to be used.

Adjacent (0)/ Non-adjacent (1) 0

If the destination node is not directly connected to the link just named, enter 1. Otherwise, enter 0. Refer to Router Network Map (Figure 4).

Entry Priority 50

Important when alternate local links are configured to reach a remote node. Refer to the Router Node Intranet Routing Table (Table 10). If no alternate links will be configured, use the default of 50 for the priority so that you allow for possible additions with higher or lower priority numbers.

Phone Number

The phone number of the destination node is required if the destination node is directly connected to the other end of the link and if the link is a direct dial or a shared dial link.

Gateway Half Information for Node Worksheets

As an example of the information needed for every gateway half in the catenet, look at Table 12. This table shows internet routing information for Node G, which is a gateway half on NET2. Referring to our Gateway Half Map (Figure 6) and our Gateway-Half Network Interface Table (Table 8), we indicate in Table 12 that Node H is a gateway half that is connected to Node G. We also see that we have named the gateway-half link LINKRL1. We see from our Catenet Map that, from Node G, we can reach NET1 in one hop. The reason NET3 is not included in Table 12 is that Node G can reach NET3 in zero hops. This is because Node G is a partner gateway half with Node H, and Node H is a member of NET3. Therefore, Node G is considered to be directly connected to NET3 and does not require a hop to reach NET3.

TABLE 12. GATEWAY-HALF NODE INTERNET ROUTING TABLE

NAME OF GATEWAY-HALF NODE: G
 IP ADDRESS: 192.006.250 005
 NETWORK NAME: NET2

CONNECTED GATEWAY-HALF NODE/ IP ADDRESS	GATEWAY-HALF LINK NAME	DESTINATION NETWORKS/ IP ADDRESSES	HOP COUNT
H/192.006.251 001	LINKRL1	NET1/ C 192.006.001 000	1

GATEWAY-HALF CONFIGURATION SCREENS (cont'd)

BISYNC LINK DATA (LINKCONF.*linkname*) Fig. 7-6, p. 7-11

Logical Device _____

The ldev number that will be configured in SYSDUMP.

NETWORK INTERFACE LINKS (NETXPORT.NI.*niName*.LINK) Fig. 11-6, p. 11-16

Type _____

DD--Direct Dial, or DC--Direct Connect

GATEWAY-HALF DIAL LINK CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 11-8, p. 11-19

Gateway Phone _____

The phone number of the remote gateway-half node.

Security String _____

Security String of the remote gateway-half node.

OR

DIRECT CONNECT CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 11-7, p. 11-17

No fields required to configure.

GATEWAY-HALF NETWORK INTERFACE CONFIGURATION (NETXPORT.NI.*niName*) Fig. 11-1, p. 11-3

Idle Device Timeout Value (Minutes) _____

For dial links, this is the number of minutes a device can remain inactive before shutting down. A value of zero will disable the idle device timer for all devices on this network interface. (Enter 0 for Direct Connect links.)

IP PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.IP) Fig. 11-3, p. 11-7

IP Address _____ C 192.006.251 001 _____

Full IP address of the partner gateway-half node (the node connected to the gateway half being configured). Refer to Gateway-Half Network Interface Table (Table 8).

GATEWAY-HALF CONFIGURATION SCREENS (cont'd)

NEIGHBOR GATEWAYS (NETXPORT.NI.*niName*.INTERNET) Fig. 11-9, p. 11-23

Gateway Name GATEH

Assign a name (maximum eight characters) to represent the partner gateway half whose address was just listed in the previous field. Refer to the Catenet Map (Figure 2) and Gateway-Half Link Map (Figure 6).

**NEIGHBOR GATEWAY REACHABLE NETWORKS (NETXPORT.NI.*niName*.INTERNET.*gatewayn*)
Fig. 11-10, p. 11-24**

Neighbor Gateway IP Internet Address C 192.006.251 001

Full IP address of the gateway node named above; same as the address in the IP Address field, listed previously.

IP Network Address

- C 192.006.001 (1)
- (2)
- (3)
- (4)

The IP addresses of all reachable networks in the catenet, through the gateway node named above. Refer to Gateway-Half Node Internet Routing Table (Table 12). We have filled in the node portion for each IP network address with zeroes because the node portion will be ignored in this field during configuration. A node portion still must be entered, however.

Hops

- 1 (1)
- (2)
- (3)
- (4)

Refer to Gateway-Half Node Internet Routing Table (Table 12) for Hop Count. The numbers in parentheses correspond to the numbers regarding IP network addresses.

System configuration is the means of defining to MPE all of the peripheral devices attached to the HP 3000 for the input or output of data, or I/O, as well as defining the system parameters required for operation. Each device is defined in terms of its associated software, or driver, which controls the device operation and manages the interface with MPE. Incoming data communications connections also require pseudo-devices, called virtual terminals, which consist of software to simulate the functionality of terminals. Hence, for NS3000/V and associated links, the system configuration consists of configuring the drivers associated with each device and enough virtual terminals to handle incoming data communications needs.

System configuration is accomplished by using the System Configurator (or SYSDUMP) dialogue, which you initiate with the SYSDUMP command. The information provided here is for situations where you need to change or add to that configuration because of changing circumstances at your installation. This section, therefore, begins with a detailed explanation of I/O configuration for the drivers and virtual terminals. Recommendations for the modification of system parameters are also provided. This information is followed by the SYSDUMP dialogue and the specific responses required to configure the drivers and virtual terminals needed for NS3000/V and associated links. The subsections are:

- System Configuration
 - I/O Configuration
 - Recommendations for System Parameters
- Virtual Terminal Configuration Dialogue
- LANIC Configuration Dialogue
- INP Configuration Dialogue
 - Device Driver (IOINP0)
 - Communications Drivers (IODS0 and IODSX)
- ATP (ASNP) Configuration Dialogue
- Completing the SYSDUMP Dialogue
- Configuration Examples

If you are already familiar with I/O configuration, turn to the specific dialogue for the device or virtual terminal you need to configure. For more information, or if you are making any other changes to the system configuration, refer to the *MPE V System Operation and Resource Management Reference Manual* or the *Fundamental Data Communications Handbook*.

SYSTEM CONFIGURATION

The system configuration of NS3000/V and associated links involves configuring the following:

- **Local Area Network Interface Controller (LANIC).** The LANIC is the MPE-V communications device used for the IEEE 802.3 links. You must configure the device driver, IOLAN0.
- **Intelligent Network Processor (INP).** The INP is the communications device used for NS Point-to-Point 3000/V Links, and DS-Compatible Links. You must configure the device driver (IOINP0) for each such link your node will have. For DS-Compatible links, you must also configure the communications drivers: IODS0 for the Point-to-Point links or IODSX for the X.25 and Satellite links.
- **Advanced Terminal Processor (ATP).** The ATP is a communications device that provides data transfer between HP 3000s, or between personal computers and an HP 3000, over the Asynchronous SERIAL Network Link. It consists of a System Interface Board (SIB) and at least one Asynchronous Interface Board (AIB). You must configure the device driver (HIOASNPO).
- **Virtual Terminals.** These pseudo devices are configured in pools. For NS links, the pool of virtual terminals is shared by all NS communications devices. You must configure as many IOVERMO virtual terminals as needed for concurrent access over all NS links combined.

For each DS-Compatible Point-to-Point Link, you must configure a separate pool of IODSTRM0 virtual terminals, back-referenced to the INP for that link. For each DS-Compatible X.25 and Satellite Link, a pool of IODSTRMX virtual terminals must be configured, again with each virtual terminal back-referenced to the INP corresponding to the specific link.

Note that whereas the pool of virtual terminals for NS links is shared across *all* NS links, virtual terminals configured for DS links are dedicated to a specific link corresponding to the back-referenced INP.

- **System Table Changes.** Changes may be required for NS3000/V and associated links. Recommendations are provided that you can use to check your existing configuration.

The drivers and virtual terminals are configured into MPE using the SYSDUMP dialogue. You initiate the SYSDUMP dialogue by issuing the SYSDUMP command, which requires a user with OP capability. As the questions or prompts appear on your screen, enter the appropriate replies for the desired system configuration. In all responses, Y or N can be used for YES or NO. A **(RETURN)** indicates NO or keeps the existing value. Explanations for each of the I/O configuration prompts and recommendations on modifying the system tables are provided below. If you are familiar with this information, skip ahead to the specific dialogue you need.

For any data communications subsystem to function, a compatible version of Communications Systems software (CS/3000) must be present on the system; it is presumed in this configuration description that CS/3000 is installed. Refer to Volume II, Section 2 of this manual for instructions on how to verify that the installed version of CS/3000 is the correct version needed for the operation of NS3000/V and associated links.

I/O Configuration

When you enter SYSDUMP you are asked a series of questions. Your answers provide the information required by MPE for the I/O configuration of each device as well as general system configuration.

The SYSDUMP dialogue begins as listed below. Prompts are shown on the left and recommended responses are underlined and/or explained on the right.

:SYSDUMP

ANY CHANGES?	<u>YES</u>
SYSTEM ID = HP32033v.uu.ff?	<u>RETURN</u>
MEMORY SIZE= nnnn (MIN=nnn, MAX=nnnn)?	<u>RETURN</u> (unless additional main memory has been added for the products you are configuring).
I/O CONFIGURATION CHANGES?	<u>YES</u>
LIST I/O DEVICES?	Enter <u>YES</u> to print a listing of the current I/O configuration. Enter <u>NO</u> or <u>RETURN</u> to continue. Refer to the example listing at the end of the section.
LIST CS DEVICES?	Enter <u>YES</u> to print a listing of all the CS devices currently configured. Enter <u>NO</u> or <u>RETURN</u> to continue. Refer to the example listing at the end of the section.
LIST DEVICE DEFAULTS?	<u>RETURN</u>
HIGHEST DRT= nnn (MIN=mm, MAX=ppp)?	Check to see if the value listed here as nnn is large enough to include all the data communications devices you are going to configure. INPs, LANICs, and ATP devices all use DRT numbers. Refer to their respective dialogue listings (later in this section) for more information.
LOGICAL DEVICE #?	To specify a device to be added or removed, enter the logical device number (ldev) of that device. Entering <u>0</u> or <u>RETURN</u> ends the I/O Configuration Changes procedure; the dialogue skips to the next set of prompts. Refer to "Completing the SYSDUMP Dialogue" (later in this section) for the continuation of questions after all devices have been configured.

The set of questions beginning with the LOGICAL DEVICE #? prompt is the key section of SYSDUMP dialogue for data communications devices. The dialogue for each type of device or driver is explained step-by-step later in this section.

Figure 4-1 shows an overview of the components of the Network Links that are used for I/O and therefore must be defined to MPE.

Each communications device requires a device driver to manage the device operation. Device driver names are as follows: IOLANO for the LANIC; IOINP0 for the INP; and HIOASNPO for the ATP.

System Configuration

For NS links, the device driver also handles the link-level protocol for the particular device associated with each link; no additional software driver is required. For the DS-Compatible links, however, the INP requires a separate communications driver, which must be individually configured and back-referenced to the ldev number of the INP. The communications driver IODSO handles the Bisync (BSC) protocol used by the DS-Compatible Point-to-Point Modem and Hardwired Links, while IODSX handles the LAP-B protocol used by the X.25 and Satellite links. The proper communications driver is downloaded to the INP at the time the DS-Compatible link is activated (that is, when you issue the :DSCONTROL OPEN command).

NOTE

A single INP can be used by two link products, although not concurrently. The method used to configure the same INP to be used by two or more link products (or two references in the same product) is essentially the same. Any constraints are detailed under "INP Configuration Dialogue" in this section. An example of an INP used by two NS links is described under "Configuration Examples" later in this section.

Virtual terminals are also shown in Figure 4-1. The virtual terminal driver used for communication over every NS link is IOVTERM0. If you have any DS-Compatible Links installed, the appropriate virtual terminal driver is IODSTRM0 for Point-to-Point and IODSTRMX for X.25.

There are three things to consider for virtual terminals. First, virtual terminals are configured much the same as actual terminals, although many of the parameters which apply to actual terminals are not used for virtual terminals. Second, when configuring virtual terminals, consider the maximum number of terminals supported by your node. Each virtual terminal is added to the total number of terminals already configured on the system. (Information is available from your HP representative as to the maximum number supported on your system.) Third, the number of virtual terminals you configure depends on the number of concurrent in-coming data communications requests your node normally receives. This means that you must configure a maximum number of IOVTERM0 virtual terminals for concurrent access over all NS links on your node, as well as a maximum number of IODSTRM0 and/or IODSTRMX virtual terminals for any respective DS-Compatible links installed.

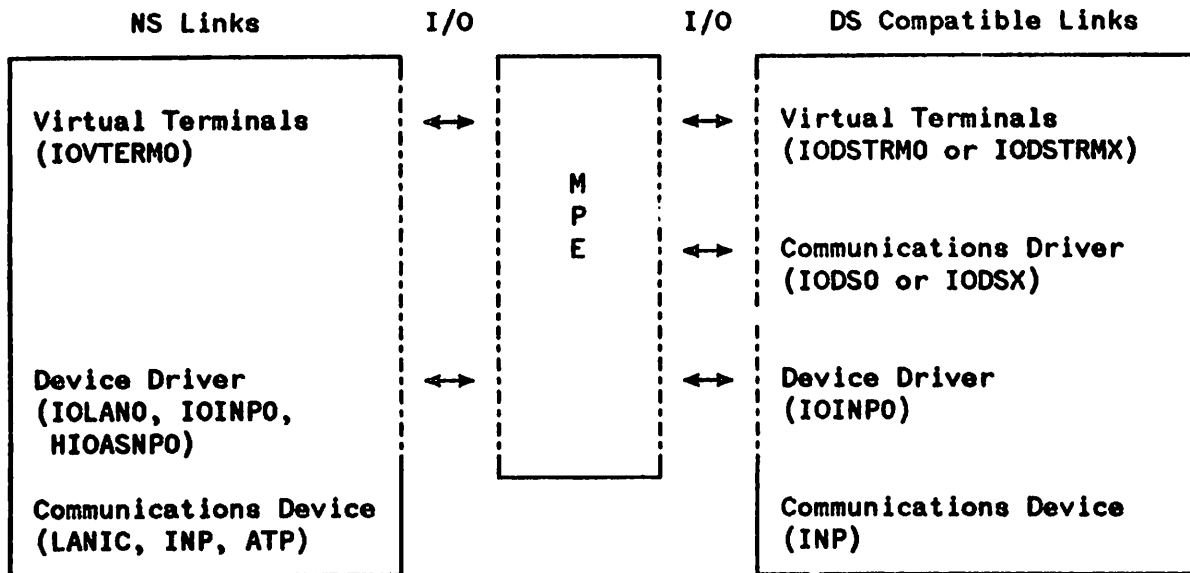


Figure 4-1. I/O Configuration for the Network Links

When configuring each of the drivers and virtual terminals, you must provide the following information:

- **LOGICAL DEVICE NUMBER.** This is the value by which MPE recognizes a particular device. You need to assign a unique logical device number, or ldev, for each device and psuedo-device you configure. The choice of ldev number is arbitrary; however, many installations follow the numbering convention that ldev numbers 1-20 are reserved for system use, with all other numbers assigned in sequence as they are needed.

NOTE

If the same INP card will be used by two different link products, it is not necessary to configure a separate IOINPO device driver for each link. When a NETCONTROL START or DSCONTROL OPEN command is attempted on a device already in use, a "DEVICE UNAVAILABLE" message will be sent to the console. Refer to Volume II, Section 1 of this manual for the proper command sequence in stopping and starting shared devices.

- **DEVICE REFERENCE TABLE (DRT) ENTRY NUMBER.** The DRT number is *only* used for the device driver. You do not enter the DRT number when configuring virtual terminals or communications drivers. Instead, you enter the ldev of the device driver preceded by a number sign (#). This is called "back-referencing" and indicates to MPE which device the virtual terminal or communications driver will use.

NOTE

For NS links, back-reference the IOVTERMO virtual terminals to the console; this allows the pool of IOVTERMO virtual terminals to be shared across all NS links. IODSTRMO and IODSTRMX virtual terminals must be back-referenced to a specific INP device driver configured as a DS link.

The DRT number is supplied by your CE and is derived from the actual hardware address of the device. During installation, the CE sets switches and jumpers on the device to correspond to that hardware address. The formula used for calculating the DRT number is included in the configuration dialogues later in this section.

- **DEVICE NAME/DEFAULTS.** Device defaults are not defined for the INP or LANIC; these prompts are not used. They are presented in the I/O configuration because many of the devices configured with MPE can be automatically configured. This means that the device configuration is created for you, without your actually having to type in values to answer some SYSDUMP dialogue questions.
- **UNIT NUMBERS.** Enter zero when configuring any of the drivers except the ATP driver (HIOASNPO); unit numbers are not used for the LANIC or INP communications devices. This is because the unit number is a hardware-dependent characteristic determined by the physical connection of a device to its controller. If there is only one device per controller, as is the case with communications devices, then a unit number of 0 is assigned.

For the ATP driver (HIOASNPO), enter a number between 0 and 95. The exact number to enter will depend on how many SIBs and AIBs are installed. Refer to the "ATP Configuration Dialogue" later in this section for details.

- **SOFTWARE CHANNEL NUMBER.** Enter zero when configuring any of the drivers. The channel number is used for other products or to deal with special configuration situations; it does not apply to NS3000/V and associated links.
- **TYPE/SUBTYPE.** Each device is assigned a device type and a subtype. In general, these numbers indicate the features the device supports and how MPE can access it. Table 4-1 describes the type and subtype for each device required by NS3000/V and associated links. The SYSDUMP dialogue may have additional prompts, depending on the type or subtype entered. The additional information requested for each type/subtype is described later in this section.
- **DRIVER NAME.** The driver is the software that serves as an interface between the device and MPE. Table 4-2 shows the names of the drivers used by each of the Network Links available with NS3000/V.

TABLE 4-1. TYPES AND SUBTYPES

Driver	Type	Subtype	Description
Virtual Terminals (IOVTERM0, IODSTRM0, IODSTRMX)	16	0	Virtual terminal. Also used for directly connected terminals with speed-sensing.
Virtual Terminal (IODSTRM0)	16	8	Allows use of block mode when connecting to a DS/1000-IV node. Checked by VPLUS/3000.
LANIC device driver (IOLAN0)	17	9	Indicates a LAN connection -- no CS configuration required.
INP device driver (IOINP0)	17	0	Indicates communication is with modems used over a switched (dial-up) line.
		1	Indicates a non-switched (leased or digital) line with a modem cable or a direct connection with a modem eliminator cable.
		3	Indicates a hardwired line, synchronous transmission.
ATP (ASNP) device driver (HIOASNPO)	42	0	Indicates a hardwired line, asynchronous transmission.
		1	Indicates communication is with modems used over a switched (dial-up) or non-switched (leased or digital) line with a modem cable. It can also be a direct connection using a modem cable.
		2	Indicates communication is with a CCITT standard modem.
Communications drivers (IODS0 and IODSX)	41	0	Indicates no data compression.
		1	Indicates data compression is enabled.

TABLE 4-2. DRIVERS REQUIRED FOR EACH NETWORK LINK

NETWORK LINKS	DRIVERS		
	Device Driver	Virtual Terminal	Communications Driver
ThickLAN HP StarLAN HP ThinLAN	IOLAN0	IOVTERMO	none
HP Serial Network	HIOASNPO	IOVTERMO	none
Point-to-Point (NS/3000)	IOINP0	IOVTERMO	none
Point-to-Point (DS/3000)	IOINP0	IODSTRM0	IODS0
X.25 Link (DS/3000)	IOINP0	IODSTRMX	IODSX

NOTE

The *DS-Compatible* X.25 Link can be used with a Packet Assembler/Disassembler (PAD). If you are using the X.25 Link with a PSN-supplied PAD or an HP 2334 Cluster Controller PAD, there are two virtual terminal drivers used instead of IODSTRMX. These are IOPAD0 for PAD to terminal connections and IOPAD1 for PAD to printer connections. Refer to the *X.25 Link for the HP 3000 Reference Manual* for information on using the X.25 Link with a PAD.

- **DEVICE CLASSES.** The IOVTERMO virtual terminal driver uses the device class designator VTERM to define a pool of virtual terminals available for use over NS3000/V links. Because of this, you *must* enter VTERM as the device class for each IOVTERMO virtual terminal that you configure. Additional device class names are allowed.

The device drivers for the NS3000/V Links do not have any special considerations as to the device class. Any device class designator configured for the device drivers IOLAN0, IOINP0, or HIOASNPO can be used in commands or intrinsics which allow device class designators.

For the DS-Compatible Links, you can configure the device class for the device driver IOINP0, the IODSTRM0 and IODSTRMX virtual terminals, and the communications driver IODS0. These configured device class designators are used in certain commands and intrinsics, including DSCONTROL and DSLINE, when any member of a group of devices can be referenced.

The exception is the IODSX communications driver used by the DS-Compatible X.25 and Satellite Links. It is recommended that device class not be configured and that users or programmers use X.25 nodenames whenever a *dsdevice* parameter is required in a command or

intrinsic. If you do configure device class designators for IODSX, *do not use X.25 nodenames as the device class designators*. The X.25 nodenames referred to are those defined in the Remote Node (RN) Table as part of the network configuration of the DS-Compatible X.25 and Satellite Links. The RN Table is configured with the NETCONF utility and stored in a TurboIMAGE data base. To find out what X.25 nodenames are configured on your node, issue the following command:

```
:RUN NETCONF.PUB.SYS
```

```
>LIST
```

A listing of all configured X.25 nodenames is displayed. Refer to the *X.25 Link for the HP 3000 Reference Manual* for information on DS/3000 X.25 and Satellite network configuration.

Type 16, Subtype 0, 8 -- Virtual Terminals

Additional information required for each virtual terminal for either subtype:

- **TERMINAL TYPE OR DESCRIPTOR FILE NAME.** Enter zero; virtual terminals do not use terminal types. The terminal type, or termtyp, refers to the HP assigned numbers used to classify actual terminals based on their characteristics. The descriptor filename is used to specify a user-created termtyp, as described in the *Workstation Configurator Reference Manual*.
- **SPEED IN CHARACTERS PER SECOND.** Enter zero; virtual terminals do not use this item. The speed refers to the fact that for actual terminals you must enter the transmission speed.
- **RECORD WIDTH.** Enter 40 for virtual terminals. This is a decimal value which specifies words, not bytes. While virtual terminals are not bound by the physical constraints of CRTs, many applications do not distinguish between virtual and actual terminals and expect data in the standard terminal record width of 40 words (80 characters).
- **OUTPUT DEVICE.** Enter the value used for the logical device number. You must specify a corresponding output device if a device is used to initiate jobs or sessions.
- **MODE.** Each device may have five modes: job/session accepting, data accepting, interactive, duplicative, and spooled. Configure the virtual terminal in accordance with its intended use, normally: job/session - YES; data - NO; interactive - YES; duplicative - YES; spooled - NO.
- **AUTO REPLY.** Press RETURN. This is not used for virtual terminals. It enables automatic replies to any tape requests.

Type 17, Subtype 9 -- LANIC Driver

No further information (in addition to ldev, type, subtype, and driver name) is required in SYSDUMP. Refer to Network Configuration in Section 5.

Type 17, Subtype 0, 1, 3 -- INP Driver

Additional information required for the INP for all three subtypes:

- **RECEIVE TIME OUT.** For NS Point-to-Point Links, enter **(RETURN)**; the default value will be overridden by NMMGR. For DS-Compatible Point-to-Point Links, use the default value of 20 by entering **(RETURN)**. This means that the INP waits 20 seconds for data to be received from the remote, following a transmission. *Do not enter 0.* This timeout is not used for the DS-Compatible X.25 and Satellite Links.
- **LOCAL TIME OUT.** For NS Point-to-Point Links, enter **(RETURN)**; the default value will be overridden by NMMGR. For the DS-Compatible Links, use the default of 60 seconds. This timeout refers to the length of time the INP allows between completion of one I/O request and the initiation of the next one. This is used by the INP to determine if the HP 3000 is responding; if not, the INP will close the link gracefully. The range is 5-900; entering 0 disables the timer.
- **CONNECT TIME OUT.** For NS Point-to-Point 3000/V links enter **(RETURN)**, and the default will be overridden by NMMGR. For the DS-Compatible Links you should enter 300 for Subtype 0; enter 120 for Subtype 1 and 3. This means that the local node waits the configured number of seconds after one attempt to make a physical connection to a remote node. It applies to the manipulation of the control lines across the DTE/DCE interface rather than a protocol exchange. Do not use the default of 900; the range is 60-900; entering 0 disables the timer. Under most conditions, you do not need to adjust these timeout values. However, if the timeout is not sufficient, CS/3000 displays an error.
- **TRANSMISSION MODE.** For NS Point-to-Point Links, enter zero; any value entered here will be overridden by NMMGR. For DS-Compatible Links, interpret this question as asking you:

"Is the INP a full-duplex (0) or half-duplex device (1)?"

Since the INP is full-duplex, capable of transmitting and receiving simultaneously, the usual response is 0 for full-duplex. However, if you are connecting the INP to a half-duplex modem or to a DS/3000 node using the Synchronous Single Line Controller (SSLC) communications device you need to enter 1 for half-duplex.

Configure the INP to operate in full duplex if the communications link provides two simultaneous main channels, one for transmit and one for receive. This is usually the case in one of the following:

- A leased line with four-wire, point-to-point installation.
- A dial network with two lines (four-wire equivalent).
- A dial network with Wide Band Service.
- Any direct connect cable between two INPs.
- A dial network or a 2-wire leased line with a special 2-wire full duplex modem. Typically these operate at 1200 bps (bits per second).

Configure the communications interface to operate in half duplex if your communications link does not provide two simultaneous main channels, one for transmit and one for receive. This is usually the case in the following:

- A dial network with a half duplex type modem that uses a single line. Usually this is a 2400 or 4800 bps modem.
- A connection to a DS/3000 node that is an HP 3000 Series II or III using a SSLC communications device.

Your response must agree with the remote system's configuration and with the characteristics of the communications line.

- **SPEED CHANGEABLE/TRANSMISSION SPEED.** The speed of the INP is changeable. For NS links, you *must* enter YES to the SPEED CHANGEABLE? prompt. Any value you enter for TRANSMISSION SPEED will be overridden by NMMGR. (Refer to Section 7 for details.)

For DS-Compatible links, the value you enter is determined by whether the INP is used for a hardwired or modem connection, and the characteristics of the communications line. If you are configuring an INP connection to a modem (Subtype 0 or 1), first determine if the modem has internal clocking signals. If so, the transmission speed is ignored, although you need to enter some value. This allows modems of different speeds to be used without reconfiguration. If the modem does not provide internal clocking signals you need to determine the correct speed for the modem. Enter that value.

If you are configuring an INP hardwired connection (Subtype 3) you need to specify a line speed appropriate for the connection. The speed you specify becomes the default. For Subtype 3 you can also specify that the speed is changeable, which is recommended. This allows the Operator to override the default by including the speed parameter in the DSCONTROL command. (Refer to Volume II, Section 1 of this manual for details on the DSCONTROL command.)

Note that the value you enter for transmission speed is in *bytes*, not *bits*, per second. For example, 4800 bits/second must be entered as 600 bytes/second. The possible values are 150, 300, 600, 900, 1200, 2400, 3600, 4800, 7000. Your response must agree with the configuration of the remote node and with the characteristics of the communications line.

- **BUFFER SIZE.** For NS links, enter 1024; any value entered here will be overridden by NMMGR.

For DS-Compatible Point-to-Point Links, the buffer size must be between 304 and 1024 words. For best performance, the maximum size of 1024 is recommended. The size of this buffer determines the maximum amount of data that can be sent or received in a single physical transmission over the line. Note that although large buffer sizes increase transmission efficiency, they also use up memory space. (In cases where noisy phone lines contribute to high transmission error rates, a smaller buffer size may increase efficiency by reducing the error rate.) Match buffer sizes for sender and receiver whenever possible, since the effective buffer size that can be utilized is the smaller of the two.

The configured buffer size can be overridden by the first user to issue a DSLINE command (with the `LINEBUF=buffer_size` parameter) after the line is initialized. Once overridden, the buffer size cannot be changed again until the first user (and any subsequent users) has closed the connection. Refer to the *NS3000/V User/Programmer Reference Manual* for information on DSLINE.

For DS-Compatible X.25 and Satellite Links, any value entered here is ignored. The buffer size used for the line is calculated depending on the packet size defined in the network configuration (using the NETCONF utility). Refer to the *X.25 Link for the HP 3000 Reference Manual* for information on X.25 and satellite network configuration.

System Configuration

- **DRIVER CHANGES.** Press **RETURN**.
- **DRIVER OPTIONS.** Enter zero.

For Subtype 1, which means the connection is over a nonswitched line with modem cable or modem eliminator cable, the following additional information is needed:

- **DUAL/HALF SPEED.** This is to establish if the modem used for this connection operates at single or dual speed. Many European modems operate with dual speeds. If you are using a dual speed modem, you are also asked if the modem is to operate at half or full speed. Answer in accordance with the features available on the modem used for the connection.

For Subtype 0, which means the connection is over modems used with a switched line, the following additional information is needed:

- **DIAL FACILITY.** The INP20B has auto-dial capability. If you are using this feature, you enter the ldev of the INP. Otherwise, answer whether the modem requires manual dial-up or not.
- **ANSWER FACILITY/AUTOMATIC ANSWER.** This refers to modems that can answer incoming calls, manually or automatically. Answer in accordance with the features available on the modem used for the connection.
- **PHONELIST/PHONE NUMBER.** If you answer that you want to list a phone number, you can supply one number, usually a frequently dialed number, to be used as the default when the line is opened. If you configured auto-dial, you must enter a phone number. The phone number is entered as a string of numbers and hyphens, up to a maximum of 30 characters. The following special characters may also be part of the phone number:
 - / Separator used for automatic call units that have a second dial tone detect.
 - E Optional end-of-number indicator.
 - D One-second delay. Used for European modems and automatic call units that require built-in delays.
 - # Defined by the local telephone system.
 - * Defined by the local telephone system.
- **LOCAL/REMOTE ID SEQUENCE.** For NS Point-to-Point Links, enter **RETURN** because this information is provided through NMMGR in the form of "security strings." Local/remote ID sequences configured for DS point-to-point links are ignored by NMMGR. ID sequences are not used for DS X.25 and Satellite Links. Local/remote ID sequences are used with DS point-to-point links as part of the DSLINE command. For more information, see the DS manuals listed in the Preface of this manual.

This additional information for Subtype 0 is necessary due to the complexity of establishing a connection using a dial-up modem. The typical sequence of steps is as follows:

1. The user issues a DSLINE command. Refer to the *NS3000/V User/Programmer Reference Manual* for information on this command.

2. The command contains a phone number (PHNUM). If not, the phone number supplied during system configuration is used.
3. Without auto-dial, the phone number is displayed at the console; the Operator dials the number at the modem and then enters YES at the console. The keyboard of the user terminal is disabled until the Operator responds. With auto-dial, meaning the INP or the modem has auto-dial and the line is configured for auto-dial, the number is dialed immediately.

Notice that the configured phone numbers are used as defaults; users may or may not supply the required numbers as parameters on the command used to request the connection. It is strongly recommended that you configure default phone numbers for any dial-up lines installed on your node. If neither defaults nor supplied values are available then the remote connection cannot be made successfully. This means that the INP and the terminal are tied up during the length of time configured for the connect timeout.

Type 41, Subtype 0, 1 -- Communications Drivers

Additional information required for the communications drivers for both subtypes:

- **RECORD WIDTH.** Enter 128 for communications drivers. This is a decimal value which must be specified in words, not bytes.
- **OUTPUT DEVICE.** Enter 0.
- **MODE.** Each device may have five modes: job/session accepting, data accepting, interactive, duplicative, and spooled. Configure the communications driver in accordance with its intended use, normally: job/session - YES; data - NO; interactive - YES; duplicative - YES; spooled - NO.
- **AUTO REPLY.** Press RETURN. This is not used for communications drivers. It enables automatic replies to any tape requests.

The configured subtype establishes the default data compression for the line, where subtype 0 is no compression and subtype 1 is compression enabled. Compression is allowed only if both nodes are capable of performing compression. The default established during configuration can be overridden with the DSCONTROL used to open the line by specifying COMP or NOCOMP, as described in Section 1, Commands, in Volume II of this manual set.

On a non-exclusive line, a user can specify data compression without affecting any other users of that line. This is done by specifying COMP or NOCOMP on the DSLINE command, as described in the *NS3000/V User/Programmer Reference Manual*. Note that the default for DSLINE is NOCOMP. If you configure the line for data compression you need to notify users to specify COMP. Otherwise, the configured default is always overridden by the default on the DSLINE command.

Compression can increase throughput by reducing redundancy in the data, which results in a reduction in the number of characters being transmitted over the link. The compression technique compresses any occurrence of three or more consecutive characters. Obviously, the savings depends on the amount of redundancy in the files, which may vary significantly. Source or listing files may be compressed by as much as 75 percent, but a savings of 25 percent is more usual. The savings also depends on the system load. Using compression and decompression increases the system overhead at both ends of the link.

The decision on whether to use compression or not depends on the communications link data rate, system load, and the amount of redundancy in the data being transmitted. Often a test of relative throughput with normal system load and typical data provides an indication of the benefits of using compression.

Type 42, Subtype 0, 1, 2 -- ATP Devices

Additional information is required for each device used by the ASNP driver:

NOTE

These values will be overwritten by information in the configuration file as specified through NMMGR.

- **RECORD WIDTH.** Enter 40 for ATP devices. This is a decimal value expressed in words, not bytes.
- **OUTPUT DEVICE.** Enter 0.
- **MODE.** Each device may have five modes: job/session accepting, data accepting, interactive, duplicative, and spooled. Press **RETURN** for each of the five modes.
- **AUTO REPLY.** Press **RETURN**. This is not used for ATP devices. It enables automatic replies to tape requests.

The configured subtype (0, 1, or 2) indicates the type of line and modem being used on the ports associated with this device driver.

NOTE

For the Asynchronous SERIAL Network Link, you must also configure as many virtual terminals (IOVTERM0) as will access the HP 3000 concurrently over this link. These are in addition to those virtual terminals configured for any other NS links. Remember to back-reference IOVTERM0 virtual terminals to the console.

Recommendations for System Parameters

Before configuring and activating NS3000/V services and links, check the limits on your system tables.

Since DS/3000 is included with NS3000/V, the additional table resources for NS3000/V depend on whether you already have DS/3000 on the system. Similarly, since the node management services provided with NS3000/V link products are also provided with the SNA Link, the additional table resources depend on whether you already have the SNA Link on the system.

The following guidelines indicate the *additional* entries needed in the Code Segment Table (CST), Data Segment Table (DST), Process Control Block Table (PCB), and I/O Queue Table (IOQ). An explanation of the items shown in *italics* follows the list of guidelines. Refer to "Configuration Examples" later in this section for some practical examples.

One or more NS3000/V Link Products:

CST: 26
 DST: $10 + (1.2 * \textit{NumConn})$
 PCB: 3
 IOQ: 0

If you do not already have products using Node Management Services:

CST: 7
 DST: $14 + (12 * \textit{NumLinks})$
 PCB: $4 + \textit{NumLinks}$
 IOQ: 0

For each Network Interface configured:

CST: 0
 DST: $\textit{NumBuff}/40$
 PCB: 0
 IOQ: 0

For each concurrently active NS link device:

CST: 0
 DST: 0
 PCB: 0
 IOQ: $2 + \textit{NumReads} + \textit{NumWrites}$

NS3000/V Services or the OfficeShare family of products (Asynchronous SERIAL Network Link, ThinLAN/3000 Link, or StarLAN/3000 Link):

CST: 10
 DST: $7 + (3 * \textit{NumConn})$
 PCB: $1 + \textit{NumConn}$
 IOQ: 0

System Configuration

If you do not already have DS/3000:

CST: 10
DST: 2 + (3 * NumLinks) + NumPads&Terms + NumSess + NumDSLlines
PCB: NumLinks
IOQ: 5 + NumSess

Note that in the case of DST and PCB entries, additional entries are used for active traces and for active users of node management services (NMMGR, NMDUMP, NMMAINT, NMMGRVER).

NOTE

The number of PCB entries should never be less than $(NumConn/2) + 4$.

An explanation of the items shown above in italics follows:

- *NumConn* is the number of TCP connections. The maximum number of TCP connections is configured through NMMGR on the Network Transport TCP screen (*Maximum Number of Connections*). You may want to use the maximum value for *NumConn* when calculating table entries in order to ensure that sufficient resources will always be available. The HP default value for the maximum number of connections is 128.
- *NumBuff* is the number of buffers used by each Network Interface.

For the LOOPBACK NI, *NumBuff* is simply the value configured in the Loopback Network Interface data screen (*Number of Buffers*). The NMMGR default value is 256.

For the 802.3, Router and Gateway NIs, *NumBuff* is calculated by the addition of the two buffer values in the Network Interface data screens (*Number of Inbound Buffers* and *Number of Outbound Buffers*) added to the *Number of Buffers* in the LINKCONF data screen. The NMMGR default for inbound buffers and outbound buffers is 256 for the 802.3, Router and Gateway NIs.

The default number of buffers for each link is as follows:

<u>Link</u>	<u>Number of Buffers</u>
802.3	42
LAP-B	12
BSC	12
ASNP	20

For an 802.3 link, only one link is configured. Using the defaults, the *Numbuff* would be:

Number of Inbound Buffers + Number of Outbound Buffers + Number of Buffers (for the 802.3 link)

256 + 256 + 42 = 554 buffers

NumBuff for a Router NI with two associated LAP-B links would be:

*Number of Inbound Buffers + Number of Outbound Buffers +
Number of Buffers (for first LAP-B link) +
Number of Buffers (for the second LAP-B link)*

Using the default values, this would be:

$$256 + 256 + 50 + 50 = 612 \text{ buffers}$$

- *NumReads* and *NumWrites* are the number of outstanding reads and the number of outstanding writes, respectively. Both are configured through NMMGR in the LINKCONF IEEE 802.3 and ASNIP data screens (*Maximum Outstanding Reads* and *Maximum Outstanding Writes*).

The NMMGR default values for each link are:

<u>Link</u>	<u>Maximum outstanding Reads</u>	<u>Maximum outstanding Writes</u>
802.3	16	7
ASNIP	5	5
BSC	3 (not configurable)	3 (not configurable)
LAP-B	3 (not configurable)	3 (not configurable)

For BSC and LAP-B use the value 3 for both the number of outstanding reads and writes in the SYSDUMP dialogue.

- *NumLinks* is the maximum number of links concurrently open.
- *NumPads&Terms* is the maximum number of pads and virtual terminal devices.
- *NumSess* is the average number of jobs or sessions using DS/3000.
- *NumDSLlines* is the average number of open DS lines on the system.

In addition to the above, the following are recommended for NS3000/V services and links:

System Table Microcode: The Expanded System Table Microcode is required.

Memory: A minimum of two megabytes of memory is required.

System Configuration

Virtual Memory: If you use the default number of TCP connections, 128, configure 60K sectors of virtual memory. If the number of TCP connections is more than or less than 128, use the following table to estimate the total virtual memory required for the system. These figures take into account the requirements of MPE, the transport, and the network services.

In the following table, Sectors takes into account one NI plus one loopback NI. For each additional NI, add in the amount listed under Sectors per Additional NIs.

<u>Number of Connections</u>	<u>Sectors</u>	<u>Sectors for Each Additional NI</u>
64	35K	1.2K
128	60K	2.5K
512	200K	10.0K
1024	400K	20.0K

Maximum Extra Data Segment Size: Increase to 32764 words.

Interrupt Control Stack: Configure the maximum value for your system.

VIRTUAL TERMINAL CONFIGURATION DIALOGUE

For more information on virtual terminal configuration, refer to I/O Configuration earlier in this section. In the dialogue below, prompts are shown on the left, and recommended responses are underlined and/or explained on the right.

LOGICAL DEVICE #?	To specify a device to be added or removed, enter the logical device number (ldev) of that device.
	Entering <u>0</u> or <u>RETURN</u> ends the I/O Configuration Changes procedure; the dialogue skips to the next set of prompts, shown later under "Completing the SYSDUMP Dialogue."
DEVICE NAME?	<u>RETURN</u>
DRT #?	For any of the IEEE 802.3 links, the Asynchronous SERIAL Network Link, or the NS3000/V Point-to-Point Link (all of which use the IOVTERM0 virtual terminal), enter the ldev number of the console preceded by a number sign (#). For DS-Compatible links, which use IODSTRM0 or IODSTRMX virtual terminals, you must enter the ldev number of the corresponding INP preceded by a number sign (#). To remove a device, enter <u>0</u> ; the dialogue returns to the LOGICAL DEVICE #? prompt.
UNIT #?	<u>0</u>
SOFTWARE CHANNEL #?	<u>0</u>
TYPE?	<u>16</u>
SUBTYPE?	Enter <u>0</u> in all cases <i>except</i> when connecting a DS-Compatible Link to a DS/1000-IV node, in which case enter <u>8</u> . Subtype <u>8</u> is checked by VPLUS/3000.
ENTER [TERM TYPE #], [DESCRIPTOR FILENAME] ?	<u>0</u>
SPEED IN CHARACTERS PER SECOND?	Enter <u>0</u> for virtual terminals. Default: 240.
RECORD WIDTH?	<u>40</u>
OUTPUT DEVICE?	Enter the same ldev as the LOGICAL DEVICE # requested above.
ACCEPT JOBS/SESSIONS?	<u>YES</u>
ACCEPT DATA?	<u>NO</u>

System Configuration

INTERACTIVE? YES

DUPLICATIVE? YES

INITIALLY SPOOLED? NO

AUTO REPLY? NO

DRIVER NAME? Enter the appropriate name:

IOVTERM0 virtual terminal for: IEEE 802.3 Link,
NS Point-to-Point 3000/V Link,
Asynchronous SERIAL Network Link

IODSTRM0 virtual terminal for: Point-to-Point
Modem or Hardwired Link (DS-Compatible)

IODSTRMX virtual terminal for: X.25 or Satellite
Link (DS-Compatible)

DEVICE CLASSES? For all NS links, enter device class **VTERM** for each configured **IOVTERM0** virtual terminal. Additional device class names are allowed.

For the virtual terminals used with the DS-Compatible Links, enter a list containing a device class name (up to eight alphanumeric characters, beginning with a letter). Class names are separated from each other by commas. Note that **VTERM** and other class names that are reserved for system devices are not permitted.

LOGICAL DEVICE #? If all I/O configuration is complete, press **(RETURN)** and the I/O configuration portion of the **SYSDUMP** dialogue will end. Subsequent prompts in the dialogue are discussed under "Completing the **SYSDUMP** Dialogue" later in this section. If I/O configuration is not yet complete, enter a logical device number and repeat the above configuration procedure (or one of the other procedures listed on the following pages).

LANIC CONFIGURATION DIALOGUE

For more information on LANIC configuration, refer to I/O Configuration earlier in this section, or to the *LANIC Installation and Service Manual*. In the dialogue below, prompts are shown on the left, and recommended responses are underlined and/or explained on the right.

LOGICAL DEVICE #? To specify a device to be added or removed, enter the logical device number (ldev) of that device.

Entering 0 or (RETURN) ends the I/O Configuration Changes procedure; the dialogue skips to the next set of prompts, shown later under "Completing the SYSDUMP Dialogue."

DEVICE NAME? (RETURN)

DRT #? To add a device, enter its DRT entry number. This number is supplied by your C.E. The formula used to calculate the DRT number from the hardware address is:

$$(IMB\# * 128) + (channel\# * 8) + device\#$$

To remove a device, enter 0; the dialogue returns to the LOGICAL DEVICE #? prompt.

UNIT #? 0

SOFTWARE CHANNEL #? 0

TYPE? 17

SUBTYPE? 9

DRIVER NAME? IOLANO

DEVICE CLASSES? Enter a list containing a device class name (up to eight alphanumeric characters, beginning with a letter). Class names are separated from each other by commas.

LOGICAL DEVICE #? If all I/O configuration is complete, press (RETURN) and the I/O configuration portion of the SYSDUMP dialogue will end. Subsequent prompts in the dialogue are discussed under "Completing the SYSDUMP Dialogue" later in this section. If I/O configuration is not yet complete, enter a logical device number and repeat the above configuration procedure (or one of the other procedures in this section).

INP CONFIGURATION DIALOGUE

For more information on INP configuration, refer to I/O Configuration earlier in this section, or to the *INP Installation and Service Manual*.

Device Driver (IOINPO)

In the dialogue below, prompts are shown on the left, and recommended responses are underlined and/or explained on the right.

LOGICAL DEVICE #? To specify a device to be added or removed, enter the logical device number (ldev) of that device.

Entering 0 or **(RETURN)** ends the I/O Configuration Changes procedure; the dialogue skips to the next set of prompts.

DEVICE NAME? **(RETURN)**

DRT #? To add a device, enter its DRT entry number. This number is supplied by your C.E. The formula used to calculate the DRT number from the hardware address is:

$$(IMB\# * 128) + (channel\# * 8) + device\#$$

To remove a device, enter 0; the dialogue returns to the LOGICAL DEVICE #? prompt.

UNIT #? 0

SOFTWARE CHANNEL #? 0

TYPE? 17

SUBTYPE? For NS links, any value is overridden by NMMGR. For DS-Compatible links, 0, 1, or 3 where:

- 0 = switched line with modem
- 1 = non-switched line with modem cable or direct connection using modem eliminator cable
- 3 = hardwired line, synchronous transmission

RECEIVE TIMEOUT? **(RETURN)**

Default: 20 (Do not enter 0.) For NS links, this default is overridden by NMMGR.

LOCAL TIMEOUT? **(RETURN)**

Default: 20. For NS links, this default is overridden by NMMGR.

Range: 5-900 seconds; 0 disables the timer.

CONNECT TIMEOUT?	For NS links, enter <u>RETURN</u> (the default value is overridden by NMMGR). For DS-Compatible links, enter <u>300</u> for Subtype 0; <u>120</u> for Subtype 1 and 3.
	Default: 900
	Range: 60-900 seconds; 0 disables the timer.
DIAL FACILITY? (Subtype 0 only)	Enter the ldev number of the INP if the AUTO DIAL feature is used. Enter <u>YES</u> if manual dial-up is required. Enter <u>NO</u> if no dial facility is required.
ANSWER FACILITY? (Subtype 0 only)	Enter <u>YES</u> if the local modem can answer calls, either manually or automatically. Enter <u>NO</u> if it cannot. A NO response causes the next step to be skipped.
AUTOMATIC ANSWER? (Subtype 0 only)	Enter <u>YES</u> if the local modem can automatically answer calls. Enter <u>NO</u> if manual answering is required.
DUAL SPEED? (Subtype 1 only)	Enter <u>YES</u> if the local modem is dual speed (European models). Enter <u>NO</u> if it is single speed. A NO response causes the next step to be skipped.
HALF SPEED? (Subtype 1 only)	Enter <u>YES</u> if the local modem is to operate at half speed. Enter <u>NO</u> if it is to operate at full speed.
SPEED CHANGEABLE?	For all NS Point-to-Point 3000/V Links, you must enter <u>YES</u> . For DS-Compatible links, you must enter <u>YES</u> to allow the speed of the line to be changeable with the DSCONTROL command. Enter <u>NO</u> for fixed line speed.
TRANSMISSION SPEED?	Enter the transmission speed of the line in characters per second (Bit Rate/8). (For NS links, this value is overridden by NMMGR.) Default: The speed specified is ignored for connections with modems that provide internal clocking signals. For all other connections, the speed you specify becomes the default. (Note also that for NS links, this default is overridden by NMMGR.) Speeds: 150, 300, 600, 900, 1200, 2400, 4800, 7000
TRANSMISSION MODE?	Enter <u>0</u> for full-duplex or <u>1</u> for half-duplex. (For NS links, always enter 0.)
PREFERRED BUFFER SIZE?	<u>1024</u> words. (For NS links, this value is overridden by NMMGR.)
DRIVER CHANGEABLE?	<u>NO</u>
DRIVER OPTIONS?	<u>0</u>
DRIVER NAME?	<u>IOINPO</u>

System Configuration

- PHONELIST?**
(Subtype 0 only) Enter YES to enter a phone number -- required for auto-dial. A NO response causes the next step to be skipped.
- PHONE NUMBER?**
(Subtype 0 only) Enter the phone number.

Up to 30 characters are allowed, consisting of a string of numbers, hyphens, and special characters (/, E, D, #, *).
- LOCAL ID SEQUENCE?**
(Subtype 0 only) For NS Point-to-Point Dial links, this information is configured through NMMGR as security strings, press RETURN.
For a DS point-to-point link, enter a valid local ID sequence or press RETURN for a null ID sequence.
- REMOTE ID SEQUENCE?**
(Subtype 0 only) For NS Point-to-Point Dial links, this information is configured through NMMGR as security strings, press RETURN.
For a DS point-to-point link, enter a valid remote ID sequence or press RETURN for a null ID sequence.
- DEVICE CLASSES?** Enter a list containing a device class name (up to eight alphanumeric characters, beginning with a letter). Class names are separated from each other by commas.
- LOGICAL DEVICE #?** If all I/O configuration is complete, press RETURN and the I/O configuration portion of the SYSDUMP dialogue will end. Subsequent prompts in the dialogue are discussed under "Completing the SYSDUMP Dialogue" later in this section. If I/O configuration is not yet complete, enter a logical device number and repeat the above configuration procedure (or one of the other procedures in this section).

Communications Drivers (IODS0 and IODSX)

In the dialogue below, prompts are shown on the left, and recommended responses are underlined and/or explained on the right.

LOGICAL DEVICE #?	To specify a device to be added or removed, enter the logical device number (ldev) of that device.
	Entering <u>0</u> or <u>RETURN</u> ends the I/O Configuration Changes procedure; the dialogue skips to the next set of prompts, shown later under "Completing the SYSDUMP Dialogue."
DEVICE NAME?	<u>RETURN</u>
DRT #?	You must assign the ldev number of the corresponding INP preceded by a number sign (#).
UNIT #?	<u>0</u>
SOFTWARE CHANNEL #?	<u>0</u>
TYPE?	<u>41</u>
SUBTYPE?	Enter <u>0</u> for No data compression or <u>1</u> for data compression.
RECORD WIDTH?	<u>128</u>
OUTPUT DEVICE?	For a communications driver, enter <u>0</u> .
ACCEPT JOBS/SESSIONS?	<u>YES</u>
ACCEPT DATA?	<u>NO</u>
INTERACTIVE?	<u>YES</u>
DUPLICATIVE?	<u>YES</u>
INITIALLY SPOOLED?	<u>NO</u>
AUTO REPLY?	<u>NO</u>
DRIVER NAME?	Enter the appropriate name: <u>IODS0</u> : Point-to-Point communications driver <u>IODSX</u> : X.25 and Satellite communications driver
DEVICE CLASSES?	Enter a list containing a device class name (up to eight alphanumeric characters, beginning with a letter). Class names are separated from each other by commas.

System Configuration

LOGICAL DEVICE #?

If all I/O configuration is complete, press **RETURN** and the I/O configuration portion of the SYSDUMP dialogue will end. Subsequent prompts in the dialogue are discussed under "Completing the SYSDUMP Dialogue" later in this section. If I/O configuration is not yet complete, enter a logical device number and repeat the above configuration procedure (or one of the other procedures in this section).

ATP CONFIGURATION DIALOGUE

For more information on ATP (ASNP) configuration, refer to I/O Configuration earlier in this section.

In the dialogue below, prompts are shown on the left, and recommended responses are underlined and/or explained on the right. Do not configure your remote support ATP port as an Asynchronous SERIAL Network Link.

LOGICAL DEVICE #?

To specify a device to be added or removed, enter the logical device number (ldev) of that device.

Entering 0 or **(RETURN)** ends the I/O Configuration Changes procedure; the dialogue skips to the next set of prompts.

DEVICE NAME?

(RETURN)

DRT #?

To add a device, enter its DRT entry number. For the ASNP driver, enter the DRT number that results from the following formula, making sure that the number you enter is less than or equal to the current highest allowable DRT number.

For Series 6x/70: $(\text{IMB\#} * 128) + (\text{channel\#} * 8)$

For Series 39/58: $(\text{channel\#} * 8)$

The channel number is the number set on the SIB's thumbwheel switch. For Series 6x and 70, the first ATP is channel number 1, the second is 4, and additional ATPs are channel numbers greater than 4. The ATP's Device number is always 0 and is not included in the formula. (The SIB always returns Device number 0 to the IMB.) The first IMB number is 0, the second is 1, and so on.

For Series 37, Micro 3000, Micro 3000 XE: $(\text{channel\#} * 8)$

For the ATP37, the channel number is the number of the slot in the cabinet where the ATP37 board is placed. The first ATP37 is channel number 1, and a maximum of four ATP37 boards are allowed. The ATP's Device number is always 0 but is not included in the formula.

NOTE

Another way to find the DRT number of the ATP is by giving a "yes" response to the IOMAP prompt during system startup.

To remove a device, enter 0; the dialogue returns to the LOGICAL DEVICE #? prompt.

System Configuration

UNIT #? 0 - 95 for ATP. Unit numbers 0 through 11 correspond to ports 0 through 11 on AIB number zero, unit numbers 12 through 23 correspond to ports 0 through 11 on AIB number one, and so on.

0 - 7 for ATP37. Unit numbers 0 through 7 correspond to ports 0 through 7.

SOFTWARE CHANNEL #? 0

TYPE? 42

SUBTYPE? 0, 1, or 2, where

0 = hardwired direct connection

1 = switched or non-switched line with modem cable or direct connection with modem cable

2 = line with a CCITT standard modem

NOTE

These subtypes will be overwritten by information in the network configuration file as specified through NMMGR.

ENTER [TERM TYPE #],
[DESCRIPTOR FILENAME] ? 0

SPEED IN CHARACTERS
PER SECOND? 0

RECORD WIDTH? 40

OUTPUT DEVICE? 0

ACCEPT JOBS/SESSIONS? RETURN

ACCEPT DATA? RETURN

INTERACTIVE? RETURN

DUPLICATIVE? RETURN

INITIALLY SPOOLED? RETURN

AUTO REPLY? RETURN

DRIVER NAME? HIOASNPO

DEVICE CLASSES?

Any non-reserved device class names are allowed, up to eight alphanumeric characters each (beginning with a letter), separated by a comma.

LOGICAL DEVICE #?

If all I/O configuration is complete, press **RETURN** and the I/O configuration portion of the SYSDUMP dialogue will end. Subsequent prompts in the dialogue are discussed under "Completing the SYSDUMP Dialogue" on the following page. If I/O configuration is not yet complete, enter a logical device number and repeat the above configuration procedure (or one of the other procedures in this section).

NOTE

For the Asynchronous SERIAL Network Link, you must also configure as many virtual terminals (IOVTERM0) as will access the HP 3000 concurrently over this link. These are in addition to those virtual terminals configured for any other NS links. Remember that all IOVTERM0 virtual terminals should be back-referenced to the console.

COMPLETING THE SYSDUMP DIALOGUE

After all I/O Configuration Changes are complete, the dialogue proceeds as shown below. Refer to the "Recommendations for System Parameters" earlier in this section to check if any other changes are required.

- LOGICAL DEVICE #?
- MAX # OF OPENED SPOOLFILES
= *nnn* (MIN=*nn*, MAX=*nnn*)?
- LIST OF I/O DEVICES? Enter YES to print a listing of the new I/O device configuration.
- LIST CS DEVICES? Enter YES to list the characteristics of the new CS device configuration.
- TERMINAL TYPE CHANGES?
- CLASS CHANGES?
- LIST I/O DEVICES?
- ADDITIONAL DRIVER CHANGES?
- I/O CONFIGURATION CHANGES?
- SYSTEM TABLE CHANGES? YES
- CST = *nnn* (MIN=*mm*,
MAX=*pppp*)? Increase the number listed here as *nnn* to match the number of additional CST entries needed (calculated earlier in this section under "System Parameters").
- EXTENDED CST = *nnnn* (MIN=
mm, MAX=*pppp*)?
- DST = *nnnn* (MIN=*mm*,
MAX= *pppp*)? Increase the number listed here as *nnnn* to match the number of additional DST entries needed (calculated earlier in this section under "System Parameters").
- PCB = *nnn* (MIN=*mm*,
MAX=*pppp*)? Increase the number listed here as *nnn* to match the number of additional PCB entries needed (calculated earlier in this section under "System Parameters").
- I/O QUEUE = *nnn* (MIN=*mm*,
MAX=*pppp*)? Increase the number listed here as *nnn* to match the number of additional I/O Queue entries needed (calculated earlier in this section under "System Parameters").
- DISC REQUEST QUEUE = *nnn*
(MIN=*mm*, MAX=*ppp*)?
- TERMINAL BUFFERS PER PORT =
n (MIN=*m*, MAX=*pp*)?

SYSTEM BUFFERS = *nn* (MIN=*m*, MAX=*ppp*)?

SWAP TABLE = *nnnn* (MIN=*mmm*, MAX=*pppp*)?

PRIMARY MESSAGE TABLE = *nnn* (MIN=*mm*, MAX=*pppp*)?

SECONDARY MESSAGE TABLE = *nn* (MIN=*mm*, MAX=*pppp*)?

SPECIAL REQUEST TABLE = *nnn* (MIN=*mm*, MAX=*pppp*)?

ICS = *nnnn* (MIN=*mmm*, MAX=*pppp*)? Increase the current value, listed here as *nnnn*, to the maximum value, listed here as *pppp*.

LOADER SEGMENT TABLE = *nnnnnn* (MIN=*mmmm*, MAX=*ppppp*)?

UCOP REQUEST QUEUE = *nnn* (MIN=*m*, MAX=*pppp*)?

TIMER REQUEST QUEUE = *nnn* (MIN=*m*, MAX=*pppp*)?

BREAKPOINT TABLE = *nn* (MIN=*m*, MAX=*pppp*)?

MAX NUMBER OF USER LOGGING PROCESSES = *nn* (MIN=*m*, MAX=*pp*)?

MAX NUMBER OF USERS PER LOGGING PROCESS = *nnn* (MIN=*m*, MAX=*ppp*)?

MISC CONFIGURATION CHANGES?

LOGGING CHANGES?

DISC ALLOCATION CHANGES? YES

MAX DIRECTORY SIZE (SECTORS) = *nnnn* (MIN=*mmmm*, MAX=*ppppp*, USED=*qqqq*)?

LIST VOLUME TABLE?

DELETE VOLUME?

ADD VOLUME?

System Configuration

LIST VOLUME CHANGES?

VIRTUAL MEMORY CHANGES? YES

LIST VIRTUAL DEVICE ALLOCATION? (If you respond YES, each volume is listed with its ldev and current virtual memory allocation.)

ENTER VOLUME NAME , SIZE IN KILOSECTORS (MAX = *nnn*)? At least 30 additional sectors need to be allocated to virtual memory for NS products.

VIRTUAL MEMORY CHANGES?

MAX # OF SPOOLFILE KILOSECTORS = *nnnn* (MIN=0, MAX=*nnnnnn*)?

OF SECTORS PER SPOOLFILE EXTENT = *nnnn* (MIN=*nnnn*, MAX=*ppppp*)?

SCHEDULING CHANGES?

SEGMENT LIMIT CHANGES? YES

MAX # OF CONCURRENT RUNNING PROGRAMS = *nn* (MIN=1, MAX=*nnnn*)?

MAX CODE SEGMENT SIZE = *nnnnn* (MIN=*nnnnn*, MAX= *ppppp*)?

MAX # OF SEGMENTS/PROCESS = *nn* (MIN=1, MAX=*nnnn*)?

MAX STACK SIZE = *nnnnn* (MIN=*nnnn*, MAX=*ppppp*)?

MAX EXTRA DATA SEGMENT SIZE = *nnnnn* (MIN=0, MAX=*nnnnnn*)? 32764

MAX # OF EXTRA DATA SEGMENTS /PROCESS = *nnn* (MIN=0, MAX=*nnnn*)?

STD STACK SIZE = *nnnn* (MIN=*nnnn*, MAX=*pppp*)?

SYSTEM PROGRAM CHANGES?

SYSTEM SL CHANGES?

ENTER DUMP DATE? Enter the appropriate response from the four possible listed here:

1) RETURN Copies the modified MPE. When this copy is used to COLDSTART the system, the account structure and all files remain intact.

2) mm/dd/yy where mm/dd/yy is some date in the future. Copies the modified MPE and the current accounting, but no files.

3) mm/dd/yy where mm/dd/yy is usually the date of the most recent system backup. Copies the modified MPE, the current accounting structure, and any files that were changed on or since the specified date.

4) 0 Copies the entire system (MPE, the current accounting structure and all files).

ENTER DUMP FILE SUBSETS?

Press RETURN, or enter a filename or series of filenames. (Example: @.PUB.SYS)

LIST FILES DUMPED?

YES or NO

The console operator must now use the =REPLY command to assign the magnetic tape drive on which you have arranged for a tape reel to be mounted.

After the SYSDUMP is complete, the tape produced should be used to COLDSTART the system. During COLDSTART, the existing I/O device configuration is replaced with the new one from your SYSDUMP tape. Refer to the *MPE V System Operation and Resource Management Reference Manual*.

CONFIGURATION EXAMPLES

The following examples illustrate possible configurations for nodes with multiple NIs and multiple link products installed. For each example, please refer to Figure 4-3, which shows a simplified catenet.

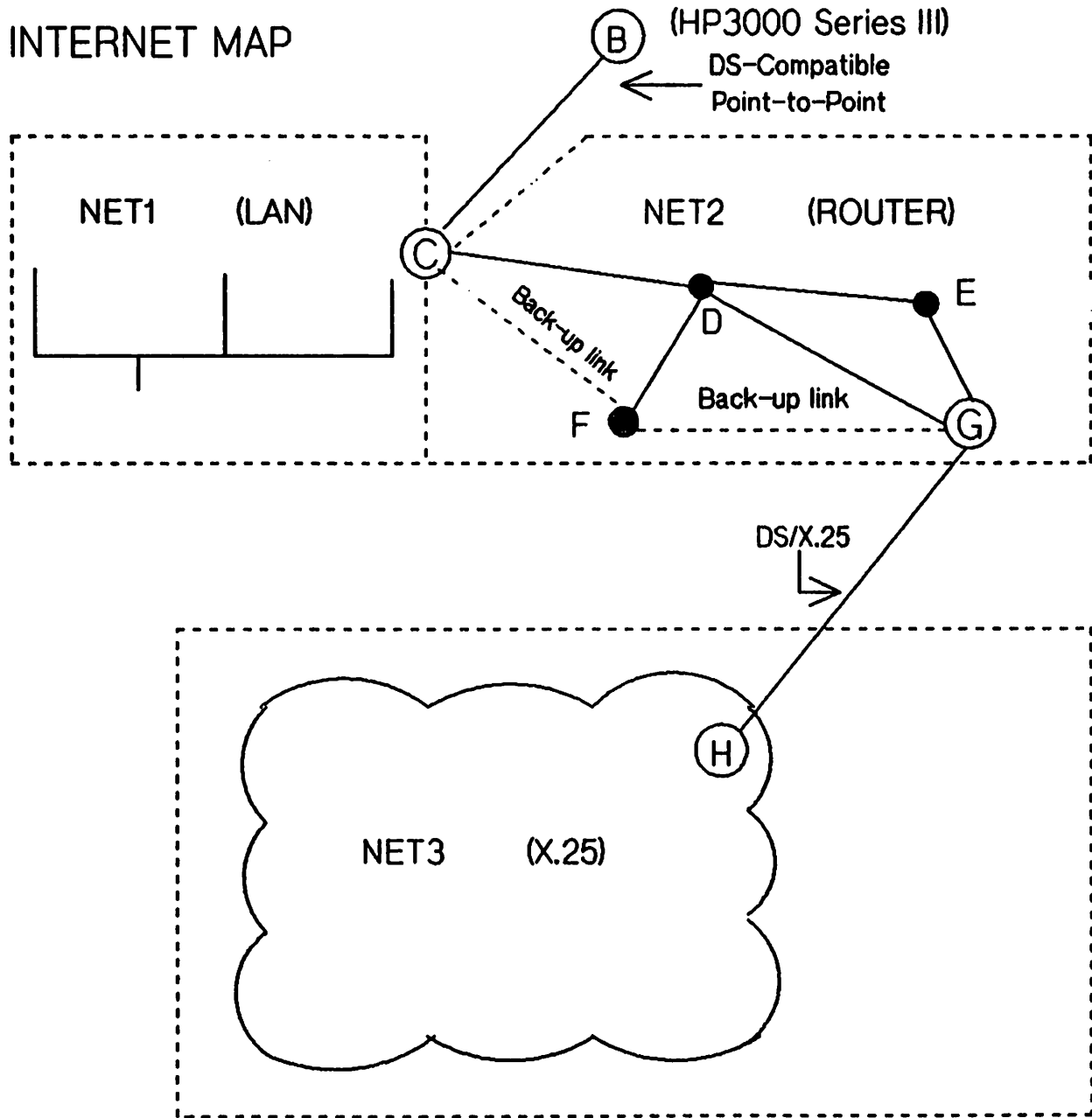


Figure 4.3 Example Network

Example 1

This example shows a SYSDUMP listing of the I/O devices on Node C in Figure 4-3. Node C is a full gateway between a LAN (Net 1) and a Router Network (Net 2). Node C has NS3000/V installed, with the following link products: ThinLAN/3000 Link, NS Point-to-Point 3000/V Link, and one DS-Compatible Point-to-Point Modem Link to an HP 3000 Series III (Node B).

Either of the INPs configured can be used as back-up NS links to Node F. Note that I/O configuration in SYSDUMP does not indicate which devices are shared. In this example, the DEVICE CLASS field has been used to indicate possible shared links. Alternatively, an INP configured for an existing DS-compatible link could be used as an NS point-to-point link, but not at the same time. The SYSDUMP items you must verify for consistency from DS to NS are described in Appendix E, DS vs NS INP Configuration.

```

LIST I/O DEVICES? Y
LOG DRT U  C T SUB_
DEV #  N  H Y TYPE  TERMINAL  REC   OUTPUT  MODE   DRIVER  DEVICE
#      I  A P      TYPE SPEED  WIDTH  DEV      DEVICES
      T  N E
1   25  0  0  0  9                128    0          *HIOMDSC1 SYSDISC
2   26  0  0  3  8                128    0          HIOMDSC2 SPOOL
3   155 0  0  3  8                128    0          HIOMDSC2 SPOOL
6   90  0  0  32 13               66     0          S        HIOCIRRO LP
7   145 0  0  24 0                128    0          HIOTAPE0 TAPE
8   145 1  0  24 0                128    0          HIOTAPE0 TAPE
10  73  2  0  24 0                128    PP        JA      HIOTAPE0 JOBTAPE
14  167 0  0  32 8                66     0          S        HIOPPRTO PP
20  8   0  0  16 0   10   960   40    20   JAID   HIOTERM1 ATPTERM
21  8   1  0  16 0   10   960   40    21   JAID   HIOTERM1 ATPTERM
.
.   (configured terminals, ldev 22-99, not shown)
.
100 8   80 0  16 0   10   960   40    22   JAID   HIOTERM1 ATPTERM
109 48  0  0  17 9                0     0          IOLANO  LANIC
110 41  0  0  17 0                0     0          IOINPO  INP
.
.
111#110 0  0  41 0                128    0          I        IODSO   NODEB
112#110 0  0  16 0   0    240   40    112  JAID   IODSTRM0 DSTERM
113#110 0  0  16 0   0    240   40    113  JAID   IODSTRM0 DSTERM
114#110 0  0  16 0   0    240   40    114  JAID   IODSTRM0 DSTERM
115#110 0  0  16 0   0    240   40    115  JAID   IODSTRM0 DSTERM

```

System Configuration

120	42	0	0	17	3	0	0	IOINPO	INP	TONODED	TONODEF
121#20	0	0	16	0	0	240	40	121	J ID	IOVTERMO	VTERM
122#20	0	0	16	0	0	240	40	122	J ID	IOVTERMO	VTERM
123#20	0	0	16	0	0	240	40	123	J ID	IOVTERMO	VTERM
124#20	0	0	16	0	0	240	40	124	J ID	IOVTERMO	VTERM
125#20	0	0	16	0	0	240	40	125	J ID	IOVTERMO	VTERM
126#20	0	0	16	0	0	240	40	126	J ID	IOVTERMO	VTERM
127#20	0	0	16	0	0	240	40	127	J ID	IOVTERMO	VTERM
128#20	0	0	16	0	0	240	40	128	J ID	IOVTERMO	VTERM
129#20	0	0	16	0	0	240	40	129	J ID	IOVTERMO	VTERM
130#20	0	0	16	0	0	240	40	130	J ID	IOVTERMO	VTERM
131#20	0	0	16	0	0	240	40	131	J ID	IOVTERMO	VTERM
132#20	0	0	16	0	0	240	40	132	J ID	IOVTERMO	VTERM
133#20	0	0	16	0	0	240	40	133	J ID	IOVTERMO	VTERM
134#20	0	0	16	0	0	240	40	134	J ID	IOVTERMO	VTERM
135#20	0	0	16	0	0	240	40	135	J ID	IOVTERMO	VTERM
136#20	0	0	16	0	0	240	40	136	J ID	IOVTERMO	VTERM
137#20	0	0	16	0	0	240	40	137	J ID	IOVTERMO	VTERM
138#20	0	0	16	0	0	240	40	138	J ID	IOVTERMO	VTERM
139#20	0	0	16	0	0	240	40	139	J ID	IOVTERMO	VTERM

The preceding thirteen columns display the following information:

- LOG DEV # -- Logical device number.
 - The ldev numbers for the INP devices are 110 and 120. The first INP, ldev 110, is used by a DS-Compatible link to a Series III (Node B in our sample catenet). Ldev 111 is the associated IODS0 communications driver for this INP. There are also four IODSTRM0 virtual terminals for this INP, configured as ldev numbers 112-115, and back-referenced to ldev 110.
 - The second INP, ldev 120, is used by an NS Point-to-Point Link to Node D and requires no separate communications driver.
 - The ldev number for the LANIC in this example is 109.
 - The ldev numbers for the pool of virtual terminals shared by the NS links are 121-139. Note that these virtual terminals are each back-referenced to the console.
- DRT # -- Device Reference Table (DRT) number. The DRT number for the LANIC is 48. The DRT numbers for the INP devices are 41 and 42. The communications driver (IODS0) and the virtual terminals (IODSTRM0 and IOVTERMO) display the ldev number of the appropriate device, preceded by a #, in place of the DRT number.
- UNIT and CHAN -- Device Unit Number and Hardware Channel Number. Channel number is unused and always set to 0; unit number is unused and set to 0 except in the case of ports configured for an ATP. (Refer to Example 2 for the way unit number is used with the NS Asynchronous 3000/V Link.)

- **TYPE and SUBTYPE -- Device Type and Subtype** The LANIC is configured as type 17, subtype 9. The INP device used for a NS link is configured as type 17, subtype 3; the INP used for a switched modem connection is configured as type 17, subtype 0. The communications driver (IODSO) is configured as type 41, subtype 0, which means a default of no data compression. All the terminals and virtual terminals are configured as type 16, subtype 0.
- **TERMINAL TYPE and SPEED -- Terminal Type and Speed.** These columns only apply to terminals.
- **REC WIDTH -- Record Width.** This value is expressed in words. The virtual terminals are configured at 40; the communications driver is configured at 128. For INPs and the LANIC, the record width is set to zero.
- **OUTPUT DEV -- Corresponding Output Device.** Notice that the virtual terminals all have their ldev number entered as their corresponding output device.
- **MODE -- Device Mode.**
- **DRIVER NAME -- Device Driver Name.**
- **DEVICE CLASSES -- Device Classes.** As required, all the IOVTERM0 virtual terminals are configured with device class VTERM.

CS Device Listing

The SYSDUMP listing of CS devices on Node C would show the following:

```
LIST CS DEVICES? Y
LDN PM PRT LCL TC RV LCL CON MODE TRANSMIT TM BUFFER D DRIVER
MOD TMOUT TMOUT TMOUT SPEED SIZE C OPTIONS
109 0 X X X 0 0 0 0 0 0 N 0
110 0 X X X 20 60 120 C 7000 0 1024 N 0
120 0 X X X 20 60 120 C 7000 0 1024 N 0
```

The CS listing provides information primarily on the INP configuration, which is described earlier in this section. Specifying subtype 9 for the LANIC skips the CS prompts in the SYSDUMP dialogue; the values for the LANIC (ldev number 109) are set to zero in the CS listing. The headings for the fourteen columns of information are:

- LDN -- Logical Device Number.
- PM -- Port Mask.
- PRT -- Protocol.
- LCL MOD -- Local Mode.
- TC -- Transmission Code.
- RV TMOUT -- Receive Timeout.
- LCL TMOUT -- Local Timeout.
- CON TMOUT -- Connect Timeout.
- MODE -- Mode.
- TRANSMIT SPEED -- Transmit Speed.
- TM -- Transmission Mode.
- BUFFER SIZE -- Buffer Size.
- DC -- Driver Changable.
- DRIVER OPTIONS -- Driver Options.

Example 2

This example shows a SYSDUMP listing for the I/O devices on Node G in Figure 4-3. Node G is a member of the Router Network, Net 2, and forms a gateway half node between Net 2 and Net 3. Node G has NS3000/V installed, with the following links products: NS Point-to-Point 3000/V, NS Aynchronous 3000/V Link, and one DS-Compatible link for support of PAD terminals in the X.25 network.

Either of the INPs configured can be used as back-up NS links to Node F. Note that I/O configuration in SYSDUMP does not indicate which devices are shared. In this example, the DEVICE CLASS field has been used to indicate possible shared links. Alternatively, an INP configured for an existing DS-compatible link could be used as an NS point-to-point link, but not at the same time. The SYSDUMP items you must verify for consistency from DS to NS are described in Appendix E, DS vs NS INP Configuration.

```

LIST I/O DEVICES? Y
LOG DRT U C T SUB_
DEV # N H Y TYPE  TERMINAL  REC   OUTPUT  MODE   DRIVER  DEVICE
#      I A P      TYPE SPEED WIDTH  DEV
1  25  0  0  0  9          128    0          *HIOMDSC1 SYSDISC
2  26  0  0  3  8          128    0          HIOMDSC2 SPOOL
3  155 0  0  3  8          128    0          HIOMDSC2 SPOOL
6  90  0  0  32 13         66     0          S        HIOCIRRO LP
7  145 0  0  24 0          128    0          HIOTAPE0 TAPE
8  145 1  0  24 0          128    0          HIOTAPE0 TAPE
10 73  2  0  24 0          128    0          PP       JA     HIOTAPE0 JOBTAPE
14 167 0  0  32 8          66     0          S        HIOPRTO PP
20 8   0  0  16 0   10   960   40     20    JAID   HIOTERM1 ATPTERM
21 8   1  0  16 0   10   960   40     21    JAID   HIOTERM1 ATPTERM
.
.   (configured terminals, ldev 22-99, not shown)
.
100 8  80  0  16 0   10   960   40     22    JAID   HIOTERM1 ATPTERM
110 41 0  0  17 3          0       0       IOINPO  INP
111#20 0  0  16 0   0    240   40     111    J ID   IOVTERMO VTERM
112#20 0  0  16 0   0    240   40     112    J ID   IOVTERMO VTERM
113#20 0  0  16 0   0    240   40     113    J ID   IOVTERMO VTERM
114#20 0  0  16 0   0    240   40     114    J ID   IOVTERMO VTERM
115#20 0  0  16 0   0    240   40     115    J ID   IOVTERMO VTERM
116#20 0  0  16 0   0    240   40     116    J ID   IOVTERMO VTERM
117#20 0  0  16 0   0    240   40     117    J ID   IOVTERMO VTERM
118#20 0  0  16 0   0    240   40     118    J ID   IOVTERMO VTERM

```

System Configuration

119#20	0	0	16	0	0	240	40	119	J	ID	IOVTERMO	VTERM
130 43	0	0	17	1			0	0			IOINPO	INP
												TONODEH
131#130	0	0	41	0			128	0			IODSX	X25
132#130	0	0	16	0	??	??	40	132	J	ID	IOPADO	PADTERM
133#130	0	0	16	0	??	??	40	133	J	ID	IOPADO	PADTERM
134#130	0	0	16	0	??	??	40	134	J	ID	IOPADO	PADTERM
135#130	0	0	16	0	??	??	40	135	J	ID	IOPADO	PADTERM
136#130	0	0	16	0	??	??	40	136	J	ID	IOPADO	PADTERM
												TONODEF
150	8	84	0	42	0		40	0			HIOASNPO	RASP
												TONODEE

The preceding thirteen columns display the following information:

- **LOG DEV #** -- Logical device number.
 - The ldev numbers for the INP devices are 110 and 130. The first INP, ldev 110, is used by an NS Point-to-Point Link to Node D in Net 2.
 - The second INP, ldev 130, is used by a DS-Compatible X.25 Link for communication with PAD terminals in Net 3 through node H. Ldev number 131 is the required communications driver (IODSX) associated with this INP. Five IOPADO virtual terminals, ldev's 132-136, are also back-referenced to this INP.
 - The ldev number for the ATP in this example is 150. This ATP is used by an Asynchronous Link to Node E.
 - The ldev number for the pool of virtual terminals shared by the NS links are 111-119. Note that these virtual terminals are back-referenced to the console.
- **DRT #** -- Device Reference Table (DRT) number. The DRT number for the ATP device is 8. DRT numbers for the INP devices are 41 and 43. The communications driver (IODSX) and the virtual terminals (IOVTERMO and IOPADO) display the ldev number of the appropriate device, preceded by a #, in place of the DRT number.
- **UNIT and CHAN** -- Device Unit Number and Hardware Channel Number. Channel numbers are unused and are set to 0; unit numbers are unused and are set to 0, except in the case of ports configured for the ATP. Units 0 through 11 correspond to ports 0 through 11 on AIB 0, unit numbers 12 through 23 correspond to ports 0 through 11 on AIB 1, and so on. In our example, the ATP driver (HIOASNPO) is configured as unit 84 (port 0 of AIB 7).
- **TYPE and SUBTYPE** -- Device Type and Subtype. The ATP is configured as type 42, Subtype 0. INP devices used for NS links are configured as type 17, subtype 3; the INP used for a switched modem connection is configured as type 17, subtype 0. The communications driver (IODSX) is configured as type 41, subtype 0, which means a default of no data compression. All terminals and virtual terminals are configured as type 16, subtype 0.
- **TERMINAL TYPE and SPEED** -- Terminal Type and Speed. These columns only apply to terminals.
- **REC WIDTH** -- Record Width. This value is expressed in words. The virtual terminals are configured at 40; the communications driver is configured at 128. For INPs the record width is set to zero.

- OUTPUT DEV -- Corresponding Output Device. Notice that the virtual terminals all have their ldev number entered as their corresponding output device.
- MODE -- Device Mode.
- DRIVER NAME -- Device Driver Name.
- DEVICE CLASSES -- Device Classes. As required, all the IOVTERMO virtual terminals are configured with device class VTERM.

CS Device Listing

The SYSDUMP listing of CS devices on Node G would show the following:

```
LIST CS DEVICES? Y
LDN PM PRT LCL TC RV LCL CON MODE TRANSMIT TM BUFFER D DRIVER
MOD TMOU1 TMOU2 SPEED SIZE C OPTIONS
110 0 X X X 20 60 120 C 7000 0 1024 N 0
130 0 X X X 20 60 120 C 7000 0 1024 N 0
```

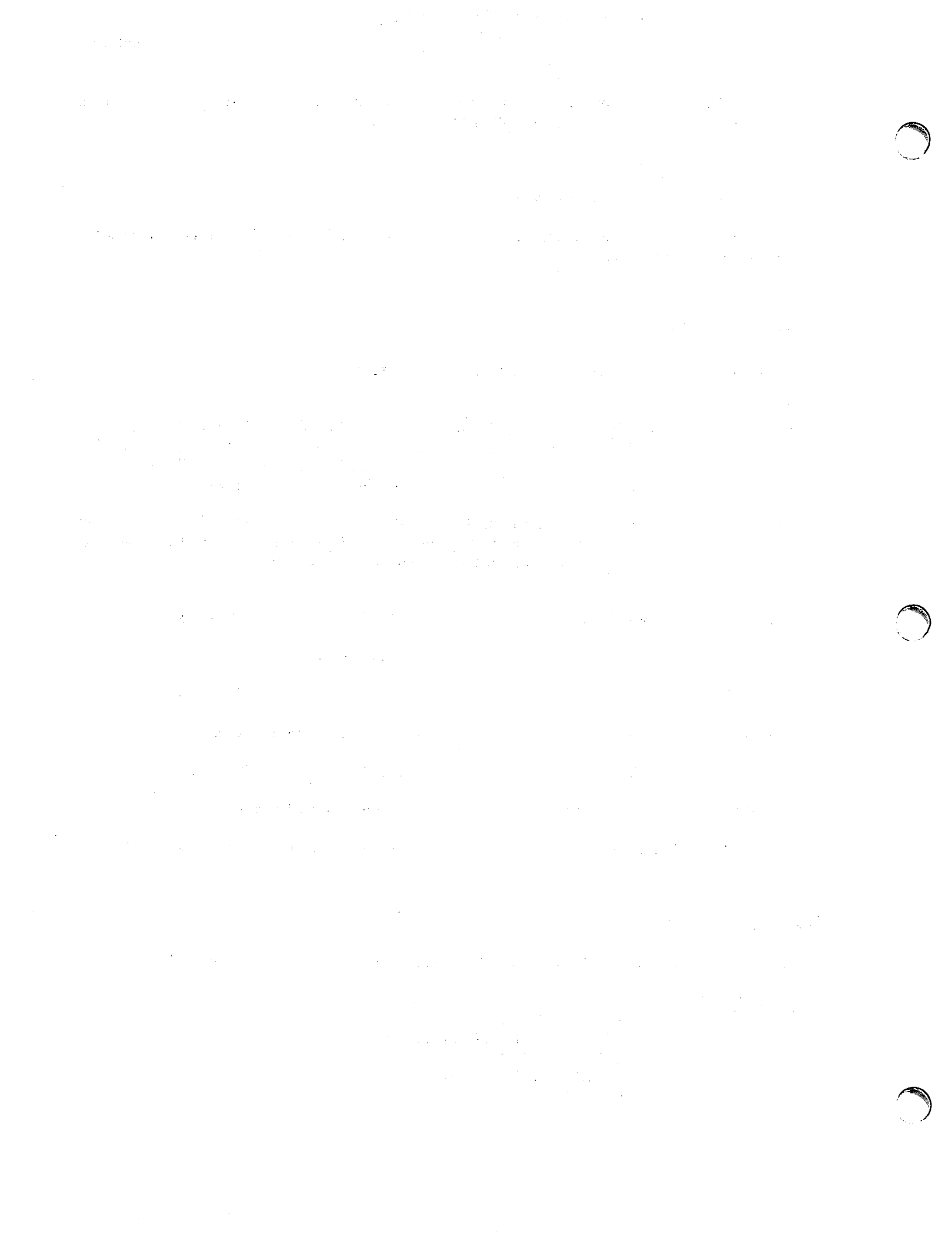
The CS listing provides information primarily on the INP devices. Information on the ATP does not appear in this listing. However, status information about the ATP is displayed when the :SHOWCOM command is entered. The headings for the fourteen columns of information are:

- LDN -- Logical Device Number.
- PM -- Port Mask.
- PRT -- Protocol.
- LCL MOD -- Local Mode.
- TC -- Transmission Code.
- RV TMOU -- Receive Timeout.
- LCL TMOU -- Local Timeout.
- CON TMOU -- Connect Timeout.
- MODE -- Mode.
- TRANSMIT SPEED -- Transmit Speed.
- TM -- Transmission Mode.
- BUFFER SIZE -- Buffer Size.
- DC -- Driver Changable.
- DRIVER OPTIONS -- Driver Options.

SHOWCOM Listing

The following is a sample listing of the MPE SHOWCOM command when used for the above ATP:

```
:SHOWCOM 150
LDN - 150
MESSAGES SENT 391680 MESSAGES RECVD 270.89
LAST RECOVERABLE ERROR 0
LAST IRRECOVERABLE ERROR 0
LINE IS CONNECTED
```

This section describes the operation of the Node Management Services Configurator (NMMGR), a utility program that provides a series of VPLUS/3000 block-mode screens to display and accept configuration information. The data entered into these configuration screens are stored in a configuration file, which is a data file with a hierarchical structure and MPE file code NCONF. The configuration information is used for initializing the NS3000 network transport.

Configuration is divided into three parts:

- Defining the operating parameters required for the Link Services subsystem.
- Defining the operating parameters required for the Network Transport subsystem.
- Enabling/disabling logging classes for each of the NMS subsystems of NS3000/V and NS3000/V links.

NMMGR includes utility screens that enable you to perform such tasks as compressing and expanding a configuration file, printing a listing of the data entered, and displaying errors.

This section contains the following subsections:

- Getting Started with NMMGR
 - The Open Configuration/Directory File Screen
 - The Main Menu Screen
 - Getting Help
 - NMMGR Screen Structure
 - Configuration Files
- Using NMMGR Configuration Screens
 - General Operation of Screens
 - Menu Screens
 - Select Screens
 - Data Screens

The NMS Configurator (NMMGR)

- Using NMMGR Utility Screens
 - Output Configuration File
 - Compress Configuration File
 - Validate Configuration File
 - The Configuration Subtree Copy Screen
 - The Error Information Screen
- Copying Configuration Data
- Making Configuration Changes

For field descriptions of configuration screens, refer to Sections 7 through 13. Section 7 describes the link configuration screens. Section 8 describes the network transport configuration screens that apply to all network interface types (LAN, router, gateway half and loopback). You should read Section 8 before proceeding to the next four sections (9 through 12). Each of these four sections is devoted to the network transport configuration screens of one network interface type. Section 13 describes the logging configuration screens.

Section 6 describes how guided configuration operates. Section 14 describes the Network Directory, including how to create and modify network directory files.

This section describes how to create and modify regular configuration files.

GETTING STARTED WITH NMMGR

You must have MPE Node Manager (NM) or Network Administrator (NA) capability to run NMMGR. Enter the following command in response to an MPE prompt:

```
:RUN NMMGR.PUB.SYS
```

After MPE accepts the run command, NMMGR displays the following message:

```
NMS Configuration Manager 32098-20012 A.02.00 (C) Hewlett Packard Co. 1986
```

NMMGR then clears the terminal screen and displays the Open Configuration/Directory File screen (Figure 5-1). The Open Configuration/Directory File screen enables you to specify a configuration file or network directory file to open or create. Specifying a configuration file name and pressing the **Open Config** or the **Create Config** key takes you to the Main Menu screen. The Main Menu (Figure 5-2) allows you to proceed to either manual configuration, utility screens, or guided configuration.

The Open Configuration/Directory File Screen

After you open or create a configuration file using the Open Configuration/Directory File screen, the file is directly accessed, and any changes you make are immediately written to the file.

If you create a configuration file for a new network, your configuration takes effect when the network is brought up for the first time. You can modify routing information for an existing configuration without bringing down the network by using the Update branch of guided configuration, followed by the NETCONTROL UPDATE command. To activate or deactivate configured links without bringing down the network, you can use the NETCONTROL ADDLINK and NETCONTROL DELLINK commands. These three commands can be issued from the MPE prompt and are the only means of modifying a configuration while the transport is active. These commands are fully described in Volume II, Section 1.

NOTE

For recommendations on making configuration changes, refer to the "Making Configuration Changes" subsection later in this section.

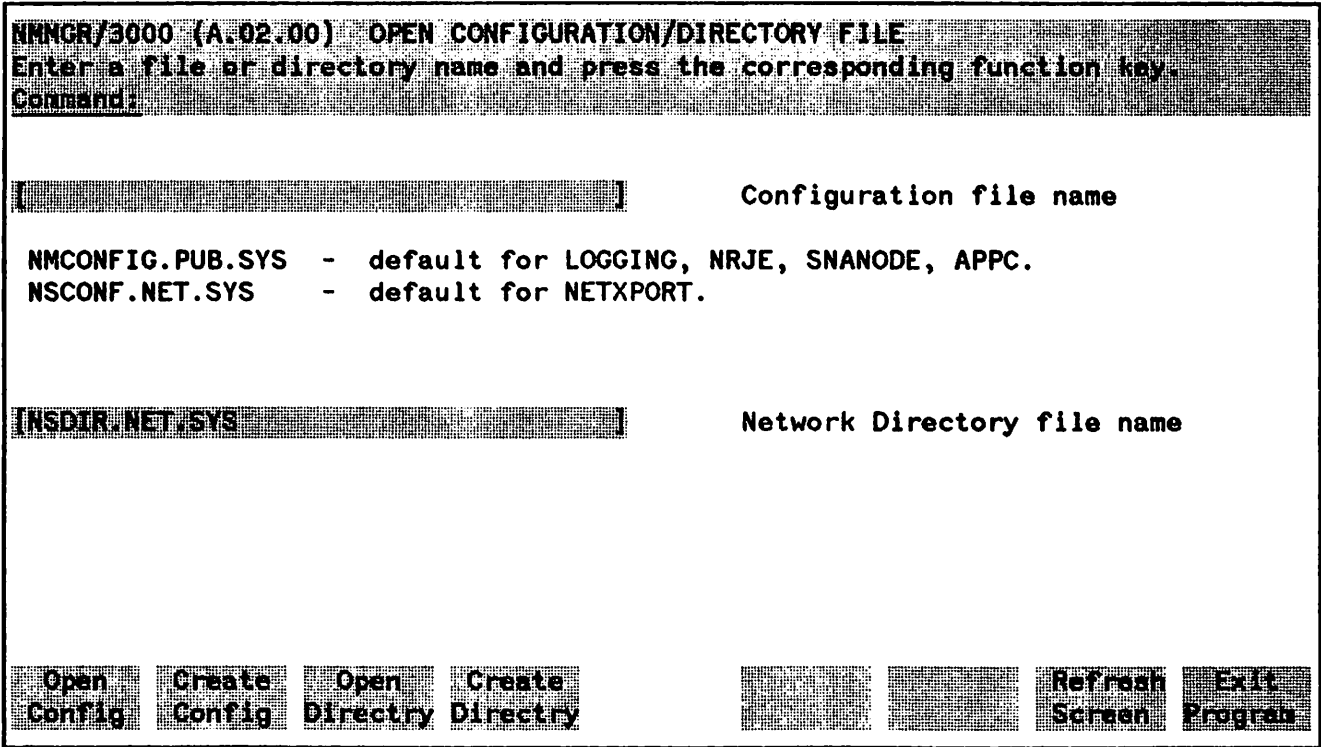


Figure 5-1. Open Configuration/Directory File Screen

The NMS Configurator (NMMGR)

At the top of each screen is a header, which identifies the version number of the NMMGR program and the screen name. In Figure 5-1, the version number is A.02.00 and the screen name is OPEN CONFIGURATION/DIRECTORY FILE. The fields labeled Configuration file name and Network Directory file name are used to specify the configuration/network directory file to be created or modified. The bottom of each screen includes function key labels, which identify the functions that NMMGR assigns to keys **F1** through **F9** on your terminal. These functions vary from screen to screen. The function keys of the Open Configuration/Directory File screen are described in Table 5-1. If the labels are blank, the function keys are unused.

TABLE 5-1. FUNCTION KEYS FOR THE OPEN CONFIGURATION/DIRECTORY FILE SCREEN

Key	Function	Description
F1	Open Config	This key opens an existing configuration file, named in the Configuration file name field. The file must already exist.
F2	Create Config	This key creates a new configuration file, named in the Configuration file name field. The file must not already exist.
F3	Open Directory	This key opens an existing network directory file, named in the Network Directory file name field. The file must already exist.
F4	Create Directory	This key creates a new Network Directory file, named in the Network Directory file name field. The file must not already exist.
F7	Refresh Screen	This key refreshes the current screen to its default or original data. This key is described in more detail later in this section.
F9	Exit Program	This key exits NMMGR. If you have an open configuration file, NMMGR closes it. Any modifications made while the file was open are saved.

NOTE

An NMMGR screen is 24 lines long. If your terminal screen is longer than 24 lines, the NMMGR labels appear to be four lines tall with blank labels on the bottom two lines. These lines are blank because the functions assigned by NMMGR clear any existing functions. Any user-defined functions are saved and are restored after exiting NMMGR.

Specifying the Configuration File Name

Three configuration files are required for the operation of NS3000/V Network Services and NS3000/V link products. Two of them are created with NMMGR, and are described below.

- One configuration file is used to define the link configuration and Network Transport configuration. This file must reside in the NET group of the SYS account. HP recommends that you name the file NSCONF which is the file name that the Network Transport looks for at initiation if one is not specified. This file is also used to define the logging configuration for the Network Transport subsystem.
- The other required configuration file defines the logging configuration for the Network Services, NetIPC, and the NMS Link Services. This second file must be named NMCONFIG.PUB.SYS.

The third configuration file is named DADCONF.NET.SYS, and is necessary for the operation of Network Services. For more information on DADCONF.NET.SYS, refer to Section 2, "Network Management."

CAUTION

NMCONFIG.PUB.SYS is also required for the following HP-to-IBM data communications products: SNA Link, SNA IMF, SNA NRJE, and LU 6.2 Base. If you have one or more of these products installed, this file is in use and *must not be modified while the HP-to-IBM products are active*. If you use the logging configuration recommended by HP, it should not be necessary to modify this file. Only the logging information of NMCONFIG.PUB.SYS is used by NS3000/V services and link products. However, if you do need to modify logging, make sure that the file is not in use, and exercise great care not to modify any of the configuration specifications used for the HP-to-IBM products. Refer to the *SNA Link Services Reference Manual* for information on the configuration of HP-to-IBM products.

A sample configuration file, NMSAMP1.PUB.SYS, is supplied with NS3000/V links. This file shows you the recommended values for the NMCONFIG.PUB.SYS configuration file, used to configure NMS logging for the Network Services, Network Interprocess Communication, and Link Support Services subsystems. The values in this file are set to optimize performance of NS3000/V and NS3000/V links during normal operation. HP recommends that you do not change the values specified in this sample file, except on the advice of your HP representative.

Also supplied is the file SAMPCONF.NET.SYS, an example of the file NSCONF.NET.SYS (or *filename*.NET.SYS). The contents of SAMPCONF.NET.SYS correspond to Node G of the example catenet described in the "Configuration Worksheets" portion of Section 3. This example file is to be used only as a reference and not as a base for building your own file. To see the contents of SAMPCONF.NET.SYS, simply run NMMGR, enter the file name in the Configuration file name field of the Open Configuration/Directory File screen, and press the **Open Config** function key.

Opening or Creating the Configuration File

Enter the name of the configuration file that you want to work on and press () **Open Config** if it is an existing file, or () **Create Config** if it is a new file. NMMGR qualifies the file name with your logon group and account if you do not specify the group or account.

NMMGR performs the following checks before creating or opening the specified configuration file:

- NMMGR checks the appropriate MPE file security specifications.
- If you pressed () **Open Config** NMMGR checks that the file specified exists and that it is a configuration file (file code NCONF).

If currently accessing a different configuration file, NMMGR closes the file before opening the specified configuration file. If the specified configuration file fails one of the checks listed above, an error message is displayed in the line immediately below the screen title. For more detailed information on an error encountered, use the Error Information screen, described later in this section.

The Main Menu Screen

Once the configuration file is successfully opened or created, NMMGR displays the second screen, the Main Menu screen (Figure 5-2). As indicated by the three choices on the main menu, the NMMGR screens have been divided into three distinct groups of screens. The configuration screens are arranged hierarchically, with a structure that corresponds to the configuration file structure. Use the screens to examine or modify a configuration file.

```

NMMGR/3000 (A.01.00) MAIN
Select the next screen and press the corresponding function key.
Command:

CONFIGURATION - Modify or examine a Configuration file.
UTILITY       - Configuration file Utility functions(output,compress,validate).
GUIDED CONFIG - Guided Configuration of subsystems.

File: filename.group.acct

Go To CONFIG  Go To UTILITY  Go To GUIDED  Refresh Screen  Prior Screen

```

Figure 5-2. Main Menu Screen

The function key **F1** **Go To CONFIG** allows you to proceed to any configuration screen. An overview and descriptions of the features of each screen can be found in sections 7 through 13.

The **F2** **Go To UTILITY** key allows you to access the utility screens. Use the utility screens to compress, output and validate a configuration file, and to copy a portion of it to another configuration file.

The **F3** **Go To GUIDED** key takes you to Guided Configuration. This function guides you through the screens used to configure a node in a network subsystem. Guided Configuration is described in detail in Section 6. Because guided configuration is faster than manual configuration, you should use guided configuration whenever possible.

Getting Help

NMMGR provides an online help function. You can use this function to obtain information about screens, commands, and other topics pertaining to NMMGR. You can access the help function from the command line of any screen.

- Enter HELP from the command line to bring up help text for the current screen, including all field descriptions for the screen.

- Enter **HELP** and either a keyword or a keyword with a qualifier to bring up help text about a specific topic, not necessarily the current screen. The topics fall into four main categories, all of which are keywords. These are **OVERVIEW**, **ROADMAP**, **COMMANDS**, and **MAINT**.

If you enter **HELP OVERVIEW** you will see a brief explanation of the operation of **NMMGR**.

If you enter **HELP ROADMAP** you will receive a map of the screen structure of **NMMGR**. You will also receive a list of additional keywords, consisting of the subsystems supported by **NMMGR**. Each of these subsystem names, such as **LINKCONF**, can be used as a qualifier to obtain a map of the screens pertaining to the listed subsystem. A qualifier, which also is considered a keyword, must follow the main keyword with a comma separating the two keywords. For example, if you wanted to see a map of **LINKCONF** screens, you would enter **HELP ROADMAP, LINKCONF** in the command window. Every screen name shown in these screen maps is a keyword of its own, and can be used with the **HELP** command and the **FIELDS** qualifier. For example, if you wanted to see field descriptions for the screen called **LAN**, you would enter **HELP LAN, FIELDS** in the command window.

If you enter **HELP COMMANDS** you will obtain a list of commands available from within the **VPLUS** interface. For information about a specific command, enter the name of the command as a keyword following the word **HELP** in the command window.

If you enter **HELP MAINT** you will see a list of commands available within maintenance mode. For information about a specific command, enter the name of the command as a keyword following the word **HELP** in the command window. If you do obtain information about a specific command, the help text will list any qualifiers, such as **PARMS**, **OPERATION**, **EXAMPLE**, and **ALL**. You then could enter the command again, this time followed by a comma and a qualifier, to obtain even further information.

- Enter a question mark (?) from the command line to put you in help mode. In this mode, you can browse through various topics until you terminate help mode by typing "end", "exit", or ":". Terminating help mode returns you to the screen you entered from.

NMMGR Screen Structure

Figure 5-3 shows the screen structure of **NMMGR** used to define the network configuration of **NS3000/V** and **NS3000/V** links. *This is a subset of the complete **NMMGR** screen structure, which includes screens for other HP data communications products.* The Open Configuration/Directory File screen is shown at the top of the screen structure because it is the first screen displayed when you run **NMMGR**.

In Figure 5-3, the function key used to reach each screen below the Main Menu is listed in the top part of the screen's box. To keep Figure 5-3 easy to follow, not all lower-level screens are shown. Where screens exist at any level beneath a box but are not shown, the section number of this volume is listed as a reference to these other screens. How to proceed from screen to screen is described in more detail under "General Operation of Screens" later in this section.

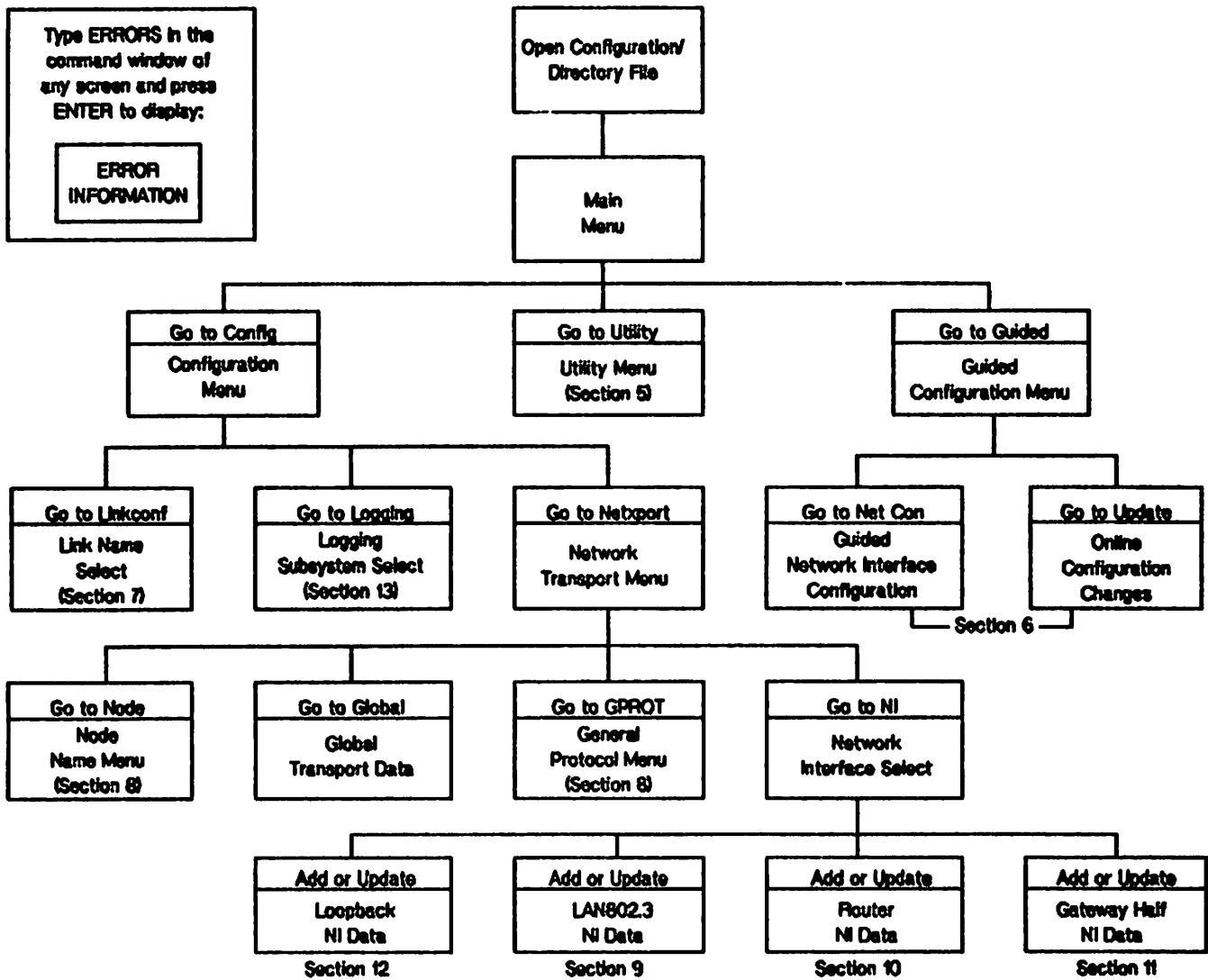


Figure 5-3. NMMGR Screen Structure

Configuration Files

NMMGR is used to create and modify configuration files. Configuration files are data files with a hierarchical structure which are file code NCONF. They are created with 2048 32-byte records. The hierarchical structure, called a template, is provided by NMMGR when the configuration file is created. Figure 5-4 shows the configuration file template used for NS3000/V network configuration. Note that this is only a subset of the complete configuration file template provided with NMMGR; templates are provided for other HP data communications products, and for the other NI types available with NS3000/V.

The template defines groups of information, called cells, with identifiers of up to eight characters. The cells are arranged in a hierarchical structure. When the configuration file is created, some of the cells, called fixed cells, are already identified. In Figure 5-4, uppercase letters denote fixed cells, such as LINKCONF.

The NMS Configurator (NMMGR)

Other cells, called **select cells**, need identifiers specified for one or more items that are associated with the cell. In Figure 5-4, select cells are shaded. The maximum number of items for each select cell is shown in square brackets. For example, the number 8 is shown next to the cell called **SUB[8]** in Figure 5-4. This means you can configure as many as eight logging classes for **CLAS[8]**, which is the select cell below **SUB[8]**. You use select screens, described later, to specify identifiers. Thus, the template can be thought of as a framework that determines the overall structure of the configuration file.

Each cell in the template corresponds to a configuration screen. The hierarchical structure of the configuration file is provided so that any screen can be accessed by defining its path in the template. A path is a sequential list of the identifiers used to reach a specific screen. Paths are described in more detail later in this section.

Data is stored in the configuration file in data records. These data records are associated with the appropriate identifiers for the cells marked with an asterisk in Figure 5-4. When the configuration file is created, its structure is established by the template, but its data records are empty. You use data screens, described later, to create or modify data records in the configuration file.

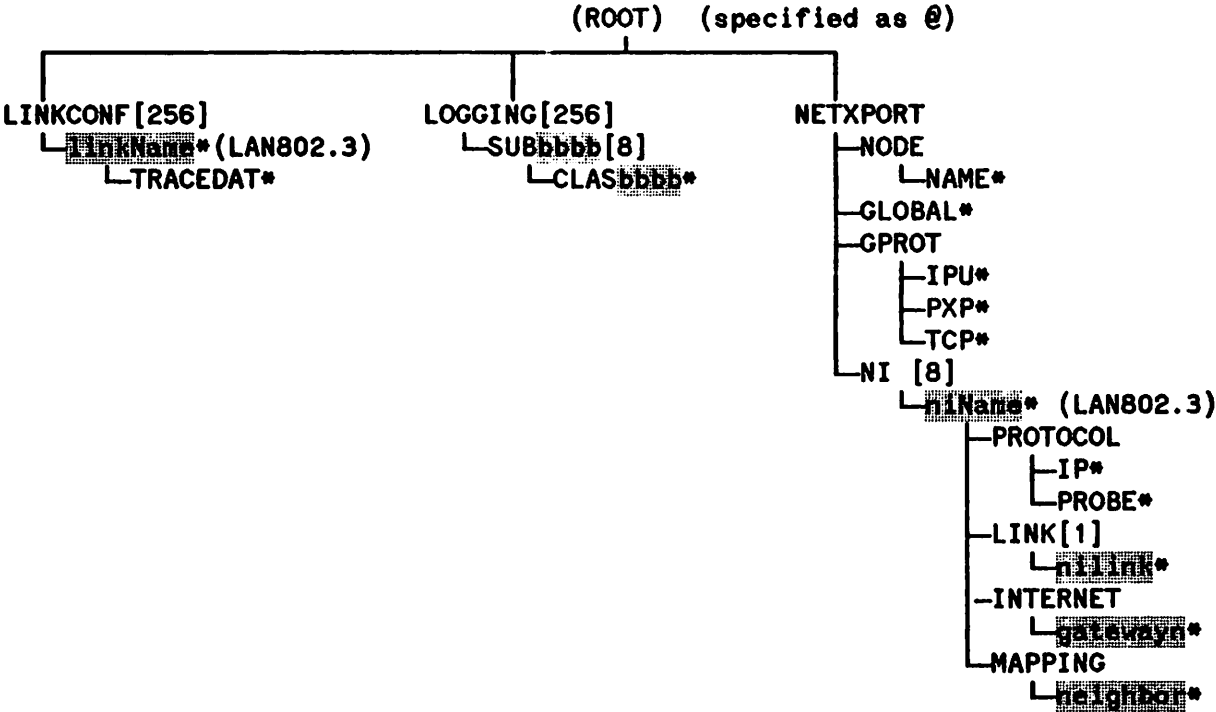


Figure 5-4. Example of a LAN Configuration File Template

* Cell with data record

USING NMMGR CONFIGURATION SCREENS

From the Main Menu screen you can proceed to the menu used to access the screens for manual configuration. Press **Go To CONFIG** at the Main Menu screen to display the Configuration screen (Figure 5-5).

```
NMMGR/3000 (A.01.00) CONFIGURATION
Select the next screen and press the corresponding function key.
Command:

Path:

LINKCONF - Configure LINK MANAGER Subsystem.
LOGGING  - Configure LOGGING for all Subsystems.
NRJE     - Configure NRJE Subsystem.
SNANODE  - Configure SNA Subsystem.
NETXPORT - Configure NETWORK TRANSPORT Subsystem.
APPC     - Configure APPC Subsystem.

File: filename.group.acct

Go To Go To Go To Go To Go To Go To Refresh Prior
LINKCONF LOGGING NRJE SNANODE NETXPORT APPC Screen Screen
```

Figure 5-5. The Configuration Screen

General Operation of Screens

Figure 5-6 shows a generalized NMMGR screen that illustrates the common features of all configuration screens. It also indicates the features that vary depending on the type of screen. An NMMGR configuration screen can be classified as one of three types:

- Menu screen
- Select screen
- Data screen

Menu screens show the fixed cells available on the path below your current level as you traverse the NMMGR screens. Select screens are used to specify identifiers for the select cells of the configuration file. Data screens are used to enter data into the data records associated with cells in the configuration file. The layout of the fields and the labels of the first six function keys (labeled **function** in Figure

5-6) are different for the three types of screens. The rest of the features (except the data flag), shown in Figure 5-6 and described below, are common to all three screen types.

NMMGR/3000 (A.02.00) SCREEN TITLE HERE				Data: Y			
Describes action required at this screen. Also used to display error messages.							
Command:							
Path: LEVEL1.userselect.LEVEL3							
Layout and function keys (1-6) depend on the type of screen:							
<ul style="list-style-type: none"> - Data Fields and definitions for DATA screens - Menu choices for MENU screens - Name select fields for SELECT screens. 							
File: filename.group.acct							
function	function	function	function	function	function	Refresh Screen	Print Screen

Figure 5-6. A Typical NMMGR Configuration Screen

The Header and Message Lines

The top line of each NMMGR screen is the header, which identifies the NMMGR version number (A.02.00) and the screen title. Below the header is the message field, where NMMGR prints errors, warnings, prompts, and other messages.

Data Flag

On data screens only, the header line also contains the Data Flag, which is shown as **Data:** followed by **Y** in Figure 5-6. A **Y** indicates that the data record has been created for that cell of the configuration file; an **N** indicates that the data record has not been created. You *must* check the data flag to know if the data record has been created. *No data is entered into the configuration file until the data record is created.* Refer to "Data Screens" later in this section.

Path Name

The path name is shown on each configuration screen in the **Path:** field. The path name for each screen consists of all the cell identifiers (separated by periods) between the root and the specific cell in a configuration file. The NMMGR screen structure is similar to the configuration file structure. The root

The NMS Configurator (NMMGR)

of the configuration file template (Figure 5-4) corresponds to the Configuration Menu in the NMMGR screen structure (Figure 5-3). Therefore, a path name corresponds to both a cell in a configuration file and an NMMGR screen. In Figure 5-6, the path name is shown as LEVEL1.userselect.LEVEL3; where LEVEL1 and LEVEL3 indicate fixed cell identifiers and userselect indicates a select cell identifier.

File Name

NMMGR displays the name of the configuration file that you are working on in the area called **File:** at the bottom of each screen. This name is shown as filename.group.acct in Figure 5-6; in practice, the actual file name entered in the Open Configuration/Directory File screen is displayed. Note that the file name is not a field; to change your working file, you must use the Open Configuration/Directory File screen.

Command Window and the Enter Key

Each screen includes a field labeled **Command:** below the message line. This field, called the command window, is displayed in half-bright inverse video. NMMGR accepts three types of commands:

- NMMGR commands
- MPE commands
- NMMGR path commands (Direct Path Branching and Brother Branching)

You can type any of the accepted types of commands in the command window and press **ENTER** to execute the command.

NMMGR Commands. NMMGR provides commands that transfer you to other screens or perform specific functions. Refer to Table 5-3 for a list of the NMMGR commands. NMMGR recognizes the unambiguous prefix of any command in Table 5-3. For example, you can enter ER to transfer to the Error Information screen; you cannot enter E because you might mean EXIT, not ERRORS. The optional portions of the commands are indicated by brackets.

MPE Commands. You can enter any programmatically executable MPE command in the command window and preface it with a colon. For example, suppose you want to see if a configuration file is active before you access it. You are already running NMMGR. You could enter the MPE command:

```
Command: :LISTF NSCONF.NET.SYS.2
```

in the command window and press **ENTER**. Your terminal screen is cleared and the information is displayed. When MPE is finished processing your command, NMMGR prompts you to press **RETURN** to return to the screen interface. You can process only one MPE command at a time.

NMMGR Path Commands. NMMGR provides two path commands that allow you to transfer freely among configuration screens that have path names: direct path branching and brother branching.

Direct path branching allows you to enter *@pathname* in a command window to transfer to the screen addressed by the path name. Look at the template in Figure 5-4 and find the cell called NAME, near the upper-right corner of the template. This cell corresponds to a data screen called the Node Name Configuration screen. To transfer to this screen, you would type the *pathname*, preceded by an @, in the command window of any screen. The command window would look like:

Command: NETXPORT.NODE.NAME

After pressing **(ENTER)**, the Node Name Configuration screen would be displayed.

Path names can include both fixed cells and user-specified cell identifiers. In order to use direct path branching, you must be familiar with the structure of the configuration file for your node. You use an output utility, described later, to provide a tree structure of your file. You must know all cell identifiers to specify a correct path name.

Brother Branching. Configuration screens that share a common parent screen are referred to as brothers. If you are working in a screen with one or more brothers, you can use the **NEXT** command to transfer to the next brother screen. This feature is called brother branching.

Look again at the template in Figure 5-4. Notice that the cell **NETXPORT** in the upper right-hand corner has four children (referred to by their path names): **NETXPORT.NODE**, **NETXPORT.GLOBAL**, **NETXPORT.GPROT**, and **NETXPORT.NI**. These four screens are brothers. To transfer to **NETXPORT.GLOBAL** from **NETXPORT.NODE**, you would simply type **next** on the command line and press **(ENTER)**. The command would look like this:

Command: NEXT

After pressing **(ENTER)**, the **NETXPORT.GLOBAL** screen would be displayed. Typing **NEXT** on the command line of the **NETXPORT.GLOBAL** screen and pressing **(ENTER)** would transfer you to **NETXPORT.GPROT**. You could use the same command to transfer from **NETXPORT.GPROT** to **NETXPORT.NI**.

The screens are visited in the order their names appear on the parent screen. Typing **NEXT** at the command line will transfer you to the next brother as long as one exists. If you try to transfer from the last brother screen to the first, you will receive an error message telling you that there are no more brother screens to transfer to.

TABLE 5-3. NMMGR COMMANDS

NMMGR Command	Action
:MPECommand	Execute <i>MPECommand</i> . <i>MPECommand</i> must be a programmatically executable MPE command.
COM[PRESS]	Transfer to Compress screen.
CON[FIGURATION] or @	Transfer to Configuration screen.
COP[YSUB]	Transfer to Configuration Subtree Copy screen.
ER[RORS]	Brings up Error Information screen.
EX[IT]	Exit from NMMGR.
H[ELP] or ?	Calls up help function. (Refer to "Getting Help" subsection earlier)
M[AIN]	Transfer to Main Menu screen.
NEX[T]	Transfer to brother screen. (Refer to the subsection "NMMGR Path Commands" earlier)
NET[DIR]	Transfer to Network Directory Main screen. Refer to Section 14 for more information.
NIG[UIDE]	Transfer to Guided Network Interface Configuration screen. Refer to Section 6 for more information.
NIU[PDATE]	Transfer to Guided Network Update Configuration Screen. Refer to Section 6 for more information.
NM[MGRCMD]	Transfer to maintenance mode interface. Refer to Section 14 for more information.
OP[EN]	Transfer to Open Configuration/Directory File screen.
OU[TPUT]	Transfer to Output Configuration File screen.

TABLE 5-3. NMMGR COMMANDS (cont.)

NMMGR Command	Action
P[RIOR]	Same as pressing Prior Screen . See explanation below.
Q[UIT]	Exit from NMMGR (Same as EXIT.)
R[EFRESH]	Same as pressing Refresh Screen . See explanation below.
S[TOP]	Stop Guided Configuration Process. Refer to Section 6 for more information.
S[U]B[GUIDE]	Transfer to Guided Configuration of Subsystem screen.
U[TILITY]	Transfer to Utility screen.
V[A]LIDATE]	Transfer to Validate Configuration File screen.
V[E]R[SION]	Display version information.

Screen Fields

You enter data or item names into the appropriate fields in data screens or select screens. You can enter information only into "unprotected" fields; the rest of the screen is protected against modification. If your terminal has the required capability, the unprotected fields are easy to identify because they are shown in half-bright inverse video and appear grey. All half-bright inverse video fields are unprotected fields, with the exception of the header and function key labels. Full-bright inverse video fields, which appear white, are used for display-only information.

On terminals without half-bright inverse video capability, unprotected fields are displayed in full-bright inverse video and appear white. For screens with more than one unprotected field, the cursor automatically moves to the next unprotected field when you reach the end of the present field, or if you press **TAB**.

Generally, you use the **TAB** key to step through the fields from the top of the screen to the bottom. For the reverse, the keys to use depend on the type of terminal -- use the **SHIFT** **TAB** keys for HP 262X terminals, use the **CONTROL** **TAB** keys for HP 264X terminals. A convenient method of positioning the cursor at the **Command** window is to home the cursor (press the key on your terminal with the diagonal arrow). For more information, consult your terminal reference manual.

Prior Screen Key

The **Prior Screen** key displays the screen most recently displayed before the current one. In order to show the correct screen, NMMGR maintains a prior screen list, which is a sequential list of the screens that have been displayed. Pressing the **Prior Screen** key displays the most recent screen in the prior screen list, and removes that screen from the list. The most recent screen in the list is the screen that was visited just prior to the current screen, with three exceptions:

- When you display the Error Information screen, NMMGR does not put this screen in your prior screen list. Thus, pressing **Prior Screen** never transfers you to the Error Information screen, even if it was the latest screen you displayed.
- After reaching the Validate screen in guided configuration, the prior screen becomes the screen with which you began the guided configuration.
- If you use the command window to return to a screen already visited, NMMGR drops from the prior-screen list any screens that you visited after this screen. For example, suppose you run NMMGR; NMMGR displays the Open Configuration/Directory File screen. The prior-screen list is empty. You open a file and NMMGR displays the Main Menu screen. The prior-screen list now contains:

Open Configuration/Directory File

You then display the Configuration screen, and the prior-screen list contains:

Main Menu
Open Configuration/Directory File

with the latest screen on top.

You then display the Link Configuration (select) screen, and the prior-screen list contains:

Configuration
Main Menu
Open Configuration/Directory File

You then display an associated Link Configuration data screen and the prior-screen list contains:

Link Configuration (select)
Configuration
Main Menu
Open Configuration/Directory File

If you then use the command window to transfer to the Main Menu screen, NMMGR truncates the prior-screen list so that it contains only:

Open Configuration/Directory File

Now, if you press **Prior Screen**, NMMGR transfers you to the Open Configuration/Directory File screen.

The Error Information screen, described later, does not include a **Prior Screen** key. Instead, it contains a key labeled **Leave Errors**, also described later.

NOTE

During Guided Configuration, this key is labeled **Next Screen** and performs a different function.

Refresh Screen Key

All screens include a **Refresh Screen** key (**F7**). You can use this key to redisplay a screen with current configuration file data. A common use of **Refresh Screen** is to "clean up" a screen after a TELL message or other interference has appeared on it. Because NMMGR uses VPLUS/3000 screens, you must press **Refresh Screen** after a terminal hard reset is performed and after a terminal power failure.

CAUTION

If you make changes to a *select* screen and press **Refresh Screen** before pressing **Update** or one of the other function keys, the identifier that you entered is cleared and is not entered into the configuration file. As for a *data* screen, any changes not saved with **Update Data** cause a warning to be displayed in the message line. If you ignore the warning and press **Refresh Screen** again or a function key other than **Update Data**, the data is not written to the configuration file.

Menu Screens

Menu screens, such as the Main Menu screen in Figure 5-2, allow you to select an NMMGR function. In the Main Menu screen, for example, three functions are available.

The text in the middle of menu screens describes the functions of the screens to which you can transfer. Select a screen by pressing the corresponding function key. The function keys available on menu screens are shown in Table 5-4.

TABLE 5-4. MENU SCREEN FUNCTION KEYS

Key	Function
Go To Function	Transfers you to the next screen "below" the current screen. Labels are dependent on specific screen.
Refresh Screen	Redisplays screen with current configuration file data.
Prior Screen	Displays the most recent screen in the prior-screen list. Refer to the earlier description of this key for examples.

Select Screens

Select screens allow you to select identifiers to add, delete, update or rename. Some select screens also include a field where you must specify the type of identifier you are selecting. Figure 5-7 is an example of such a select screen. You must specify a network interface type in addition to a network interface name. Some of the screens that follow such a select screen depend on the type of network interface you select.

```

NMMGR/3000 (X.05.06) NETWORK INTERFACE CONFIGURATION
Type in name of item to Update, Delete, or Rename; or Add a new item
Command:

Path: NETXPORT.NI

Network Interface Name      Type : LOOP, LAN802.3,
New Name                    ROUTER, GATEHALF
                             (if new)

          Configured Network Interfaces

Name      Type      Name      Type      Name      Type

[ ]       [ ]       [ ]       [ ]       [ ]       [ ]

File: filename.NET.SYS

Next Page  Prev Page  Delete  Rename  Add  Update  Refresh Screen  Prior Screen
    
```

Figure 5-7. Select Screen

In this screen, the select field is labeled:

Network Interface Name

Item names can contain as many as eight alphanumeric characters, and the first character must be alphabetic. NMMGR does not differentiate between uppercase and lowercase letters when you enter item names; it upshifts all letters in item names and stores them in uppercase letters.

The type field in this screen is labeled:

LOOP, LAN802.3,
Type : ROUTER, GATEHALF
(if new)

To delete or update an identifier, enter the name of the item in the select field and press the appropriate function key. To add, enter the name of the item and its type and press **Add**. Refer to Table 5-5 for a list of function keys for select screens. If you press **Add** or **Update**, NMMGR transfers you either to a data screen so that you can enter or update configuration data for that item, or to another select screen so that you can further specify what you want to configure. If you press **Delete**, NMMGR asks you to press **Delete** again to confirm. If you do, NMMGR deletes the item specified in the select field and any data associated with it from the configuration file. NMMGR then confirms that you have deleted the item by printing the following message in the message field:

Item deleted.

Below the select field is the rename field. In Figure 5-7, the rename field is:

New name

To rename an item, enter the name of the item in the select field and enter the new name in the rename field; then press the **Rename** key. NMMGR confirms that you have renamed the item by printing the following message in the message field:

Item renamed.

TABLE 5-5. SELECT SCREEN FUNCTION KEYS

Key	Function
Next Page	Displays the next set of items.
Prev Page	Displays the previous set of items.
Delete	When pressed twice in succession (to confirm deletion), deletes the item specified in the select field. NMMGR deletes the item and any data associated with it from the configuration file.
Rename	Renames the item specified in the select field with the name specified in the rename field.
Add	Adds an item to the configuration file, with the name specified in the select field. Transfers you either to a data-entry screen so you can enter configuration information for the item, or to a select screen "below" the current screen.
Update	Transfers you either to a data-entry screen so you can update configuration information about the item specified in the select field, or to a select screen "below" the current screen.
Refresh Screen	Redisplays the screen with current configuration file data.
Prior Screen	Displays the most recent screen in the prior-screen list. Refer to the earlier description of this key.

The lower half of a select screen displays, in alphabetical order, names of items that are currently configured in the file. If your configuration file contains more items than can be displayed in one screen, you can display the next set by pressing **Next Page**. To display the previous set, press **Prev Page**.

The maximum number of items possible for a select cell is 256, but some have lower limits--such as 8 for the Logging Configuration class select cells (CLASbbb).

Data Screens

Data screens are used to configure data records for items that require data. The cells in Figure 5-4 that have data records associated with them are denoted with asterisks. Data-entry screens allow you to enter configuration data into unprotected fields. Figure 5-8 is an example of a data-entry screen.

You must press **Update Data** to create a data record. The data flag in the upper-right corner of each data screen is set to **Y** only when a data record has been created. Otherwise, the flag is set to **N**. Before a data record is created, any values displayed in the data fields are only recommendations -- they are not yet part of the configuration file.

```

NMMGR/3000 (X.05.06)  ROUTER NETWORK INTERFACE CONFIGURATION      Data: N
When Data Flag is 'N', press "Update Data" to create the data record.
Command:

Path: NETXPORT.NI.niName

[256]  Number Of Inbound Buffers
[256]  Number Of Outbound Buffers
[100]  Number Of Routing Table Entries
      Network Hop Count
      Idle Device Timeout Value (Minutes)
          0 = Timer Disabled For All Devices

File: filename.NET.SYS

Go To  Go To  Go To  Go To  Update  Refresh  Prior
PROTOCOL LINK  INTERNET MAPPING  Data  Screen  Screen
    
```

Figure 5-8. Data-entry screen

The **Update Data** key is used to add or update information in a data record. The **(ENTER)** key can also be used to update the data record if the command line is blank. NMMGR confirms that you have updated the configuration file by printing the following message in the message field:

Configuration data updated.

The NMS Configurator (NMMGR)

If you enter data in a field and then try to transfer to another screen (by pressing a function key or by using the command window) before pressing **Update Data**, NMMGR prints:

Warning: Screen changed. Use UPDATE to save data. (NMGRWARN7)

This warning cautions you against unintentionally leaving a data screen before you have updated the configuration file. If you decide you do not want to update the configuration file with the data on the screen, you can ignore the warning and repeat the action to transfer to another screen.











If you enter the wrong type of data in any field and try to update the configuration file, NMMGR prints an error message corresponding to the first field with invalid data, highlights and underlines the fields with invalid data, and positions the cursor at the first field with invalid data. For example, suppose you enter an alphabetic character in a location that must contain an integer. When you try to update the file, NMMGR may print:

The field can contain only digits.

The **Refresh Screen** key redisplay a data screen, and shows its current configuration file data. Suppose you have changed some values on a data screen, but then decide to modify these values before actually entering them into the configuration file. Press **Refresh Screen**. NMMGR will warn you that the screen has changed since you last updated it. Press **Refresh Screen** again; NMMGR refreshes the screen and shows its current configuration file data.

Refer to Table 5-6 for a list of function keys for data-entry screens.

TABLE 5-6. DATA SCREEN FUNCTION KEYS

Key	Function
	Transfers you to the next screen "below" the current screen. Labels are screen specific.
	Displays the next set of items.
	Displays the previous set of items.
	Displays the first set of items. (Function available for Neighbor Gateway Reachable Networks Screen.)
	Displays the last set of items. (Function available for Neighbor Gateway Reachable Networks Screen.)
	Condenses the current set of items. (Function available for Neighbor Gateway Reachable Networks Screen.)
	Writes screen data to configuration file. This key <i>must</i> be used to create or update the data record.
	Redisplays screen with current configuration file data.
	Displays the most recent screen in the prior-screen list. Refer to the earlier description of this key.
	Appears on some screens; removes data configured on the screen from the configuration file.

USING NMMGR UTILITY SCREENS

The Utility Screen (Figure 5-9) is a menu screen from which you can transfer to the Output, Compress, Validate, or Configuration Subtree Copy screens. To display the Utility Screen, you can select **Go To UTILITY** at the Main Menu screen, or you can type UTILITY in the command window of any screen and press **ENTER**.

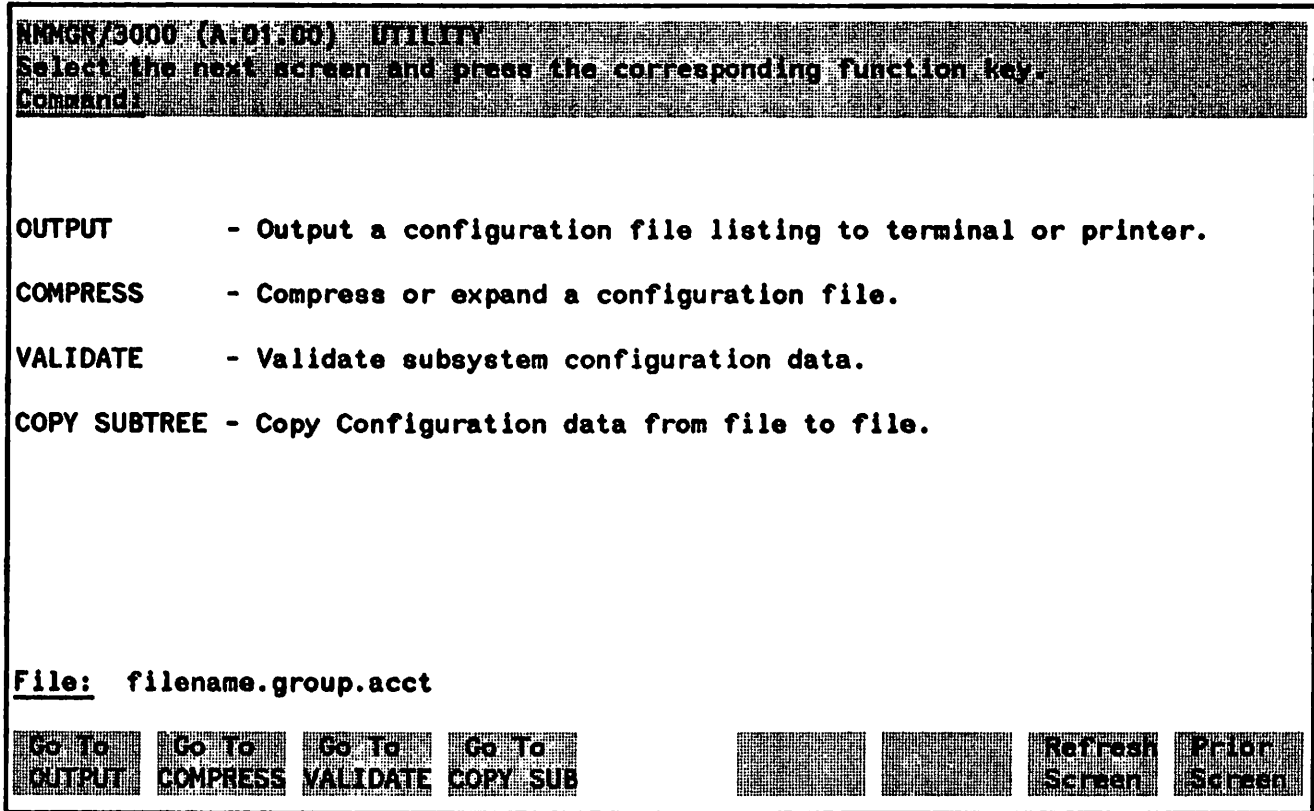


Figure 5-9. Utility Screen

The Output screen allows you to display or print the configuration file tree structure or the data screens associated with a configuration file.

The Compress screen allows you to compress or expand the configuration file, which is helpful if you run out of record space.

The Validate screen allows you to see if the configuration of a specified subsystem is valid.

The Configuration Subtree Copy screen allows you to copy configuration data from one configuration file to another.

Determine the function you wish to perform and press the corresponding function key.

Output Configuration File

The Output Configuration File screen (Figure 5-10) allows you to list or print the configuration file tree structure, to print the NMMGR data screens associated with a configuration file, and to print a critical summary of the configuration file data. Refer to Table 5-7 for a list of function keys for this screen. You may want to issue a file equation for the output file FORMLIST on the command line. For example, you could type:

:FILE FORMLIST;DEV=PP

If you then pressed **Print Data**, the output would be sent to the device PP.

For another example, you could type:

:FILE FORMLIST;DEV=DISC;SAVE

If you then pressed **Print Data**, the output would be stored on disc under the file name FORMLIST.

```

NMMGR/3000 (A.02.00) OUTPUT CONFIGURATION FILE
Select output option and press the corresponding function key.
Command:

DISPLAY TREE - Display configuration file tree structure to terminal.
PRINT TREE   - Print config file tree structure to line printer or FORMLIST.

PRINT DATA  - Print data screens to line printer or FORMLIST.
               Subsystem [0] [1] [2] [3]
                   0: All subsystems      3: NRJE           6: APPC
                   1: LINKCONF           4: SNANODE
                   2: LOGGING             5: NETXPORT

PRINT SUMMARY - Print critical summary of data for subsystem [5]
                  to line printer or FORMLIST.

PRINT SUBTREE - Print data screens for a subtree to line printer or FORMLIST.
                  Enter the path of the screen at the top of the subtree:
                  _____

File: file.group.acct

Display Tree  Print Tree  Print Data  Print Summary  Print Subtree  Refresh Screen  Prior Screen

```

Figure 5-10. Output Configuration File Screen

The tree structure printed by the **Print Tree** key shows the identifiers that are configured for each cell, but does not show any data that is configured. This key is useful for finding out which identifiers are already configured in a file, and for guidance in direct path branching, described earlier. To generate a printed listing of all the data screens in the file, use the **Print Data** key.

TABLE 5-7. OUTPUT FUNCTION KEYS

Key	Function
Display Tree	Displays the configuration file tree structure to your terminal. Refer to Figure 5-11 for an example.
Print Tree	Prints the configuration file tree structure to the line printer (default system device LP, or FORMLIST--Formal File Designator). Refer to Figure 5-11 for an example.
Print Data	Prints the NMMGR data screens associated with the configuration file to LP or FORMLIST. By default, output goes to the device LP. Refer to Figure 5-12 for an example.
Print Summary	Prints critical summary of data for Network Transport to line printer or FORMLIST. By default, output goes to the device LP.
Print Subtree	Prints the NMMGR data screens for a specified subtree to LP or FORMLIST. Default output device is LP.

NMMGR presents the hierarchical structure and data screens of a file by doing a depth-first traversal of the tree. The cells on each level are presented in the order they were configured.

If you press **Print Tree**, **Print Data**, **Print Summary** or **Print Subtree**, NMMGR prints the following message in the message field when it has finished listing the output:

Output listing completed.

Print Tree and Display Tree

Figure 5-11 is an example of a tree structure produced by pressing **Print Tree** or **Display Tree**. In this example, the user has configured a node on an IEEE 802.3 LAN. Thus, the structure corresponds to that seen in the template in figure 5-4. The level of each cell is printed on the left, in square brackets. The tree structure shows the identifiers of all the configured cells and items and those of the fixed cells reachable from the configured cells and items. The entries are indented according to their level in the tree structure.

```
[1] LINKCONF
[2]  LANLINK
[3]   TRACEDAT
[1] LOGGING
[2]  SUB0003
[3]   CLAS0001
[3]   CLAS0002
[3]   CLAS0003
[3]   CLAS0004
[3]   CLAS0005
[3]   CLAS0006
[1] NRJE
[1] SNANODE
[1] NETXPORT
[2]  NODE
[3]   NAME
[2]  GLOBAL
[2]  GPROT
[3]   IPU
[3]   PXP
[3]   TCP
[2]  NI
[3]   LAN1
[4]    PROTOCOL
[5]     IP
[5]     PROBE
[4]    LINK
[5]     LANLINK
[4]    INTERNET
[5]     LANINET
[4]    MAPPING
[5]     LANMAP
```

Figure 5-11. Example of Configuration File Tree Structure

Print Data

The **Print Data** key allows you to print the data screens of a configuration file. If data is present in the configuration file, the actual data is printed on the appropriate data screen, and the Data Flag is **Y**. However, where no data is present, the recommended values (screen default values) are printed on the appropriate data screens, and the Data Flag is **N**.

Figure 5-12 is an example of a data screen printed by **Print Data**:

```
NMMGR/3000 (A.01.00) GLOBAL TRANSPORT CONFIGURATION                               Data: Y
Fill in fields and press Update to configure the data for this item.
Command:

Path: NETXPORT.GLOBAL

[LAN1   ] Home Network Name

[2][3][1] Name Search Methods And Order

          1 - Network Directory      3 - Probe Proxy
          2 - Probe                  0 - Choice Omitted

[100 ] Maximum Directly Connected Nodes
[100 ] Maximum Outbound Destinations
[100 ] Maximum Inbound Destinations

File: filename.NET.SYS

Update  Refresh  Prior
Data    Screen   Screen
```

Figure 5-12. Print Data Screen Example

Print Summary

The **Print Summary** key allows you to print what is known as a critical summary--a listing of screens and configured field values for your configuration file. The example that follows is a sample critical summary for a full-gateway node that has been configured with a router NI and a LAN NI. The IP addresses shown have been reserved for use in examples only.

CRITICAL SUMMARY - NETXPORT CONFIGURATION

CONFIGURATION FILE NAME: NSCONF.NET.SYS

NODE NAME: FLAGSTAFF.ROUTE66.USA

TRANSPORT GLOBAL CONFIGURATION:

Name Search Method: 1. Probe
 2. Probe Proxy
 3. Network Directory
 Maximum Directly Connected Nodes: 100
 Maximum Outbound Destinations: 100
 Maximum Inbound Destinations: 100

IP UPDATE (IPU) CONFIGURATION:

Maximum Number of Networks in Internet: 64
 Maximum Gateway Nodes Per Network: 16

PACKET EXCHANGE PROTOCOL (PXP) CONFIGURATION:

Retransmission Interval (Secs): 10
 Maximum Retransmissions Per Request: 4

TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION:

Maximum Number of Connections: 128
 Retransmission Interval Upper Bound (Secs): 120
 Retransmission Interval Lower Bound (Secs): 4
 Initial Retransmission Interval: 4
 Maximum Number of Retransmissions: 4
 Connection Assurance Interval: 600
 Maximum Connection Assurance Retransmissions: 3

CONFIGURED NETWORK INTERFACES:

Network Interface Type: LAN
 Network Interface Name: LANA
 Network Interface IP Address: C 192.006.001 000
 Network Segment Size: 1497
 Number of Inbound Buffers: 256
 Number of Outbound Buffers: 256
 Number of Store and Forward Buffers: 20
 Maximum Number of Nodes in Network: 100

PROBE PROTOCOL CONFIGURATION:

Proxy Enabled: Yes

NETWORK INTERFACE LINKS:

Link Name	LDEV	Link Type	Buffer Size	Line Speed	Dial Enabled
LANLINK	150	LAN LAN802.3			

IEEE 802.3 MAPPING:

IP Internet Address	IP SAP	IEEE802.3 Address
---------------------	--------	-------------------

(None configured)

The NMS Configurator (NMMGR)

CONFIGURATION:

Neighbor Gateway Name: NODE2 Gateway IP Address: C 192.006.001 001
Reachable Networks:
 IP Network Number Hops IP Network Number Hops
 ----- ---- ----- ----
 C 192.006.250 000 1 C 192.006.251 000 2

Network Interface Type: Router
Network Interface Name: ROUTE66
Network Interface IP Address: C 192.006.252 006
Number of Inbound Buffers: 256
Number of Outbound Buffers: 256
Number of Store and Forward Buffers: 20
Number of Route Table Entries: 100
Network Hop Count: 10

DIAL PROTOCOL INFORMATION:

Maximum Retransmissions Per Packet: 2
Retransmission Timeout (Secs): 5
Security On: Yes
Security Strings: HP

NETWORK INTERFACE LINKS:

Link Name	LDEV	Link Type	Buffer Size	Line Speed	Dial Enabled
NEWMEX	151	SD LAPB	1024	56000	Yes
ARIZONA	152	DD ATP/ASNP	242	1200	Yes

ROUTER REACHABLE NODES:

Node Name	IP Address	Link Name	Adjacent?	Phone Number	Security String
CHICAGO	C 192.006.252 001	NEWMEX	Nonadjacent		HP
STLOUIS	C 192.006.252 002	NEWMEX	Nonadjacent		HP
OKCITY	C 192.006.252 003	NEWMEX	Nonadjacent		HP
AMARILLO	C 192.006.252 004	NEWMEX	Nonadjacent		HP
GALLUPNM	C 192.006.252 005	NEWMEX	Adjacent	71-555-555-5555	HP
WINOMA	C 192.006.252 007	ARIZONA	Adjacent	71-888-888-8888	HP
KINGMAN	C 192.006.252 008	ARIZONA	Nonadjacent		HP
BARSTOW	C 192.006.252 009	ARIZONA	Nonadjacent		HP
SANBERNA	C 192.006.252 010	ARIZONA	Nonadjacent		HP
LA	C 192.006.252 011	ARIZONA	Nonadjacent		HP

INTERNET CONFIGURATION:

Neighbor Gateway Name: CHICAGO Gateway IP Address: C 192.006.252 001
Reachable Networks:
 IP Network Number Hops IP Network Number Hops
 ----- ---- ----- ----
 C 192.006.253 000 1 C 192.006.254 000 2

The NMS Configurator (NMMGR)

Default: 0
Range: -32767 to 32767.

The Compress screen can compress, or expand configuration files. NMMGR compresses files before adding or deleting records, as explained below.

Configuration files initially contain 2048 32-byte records. As you configure items in a file, records are used sequentially from the beginning of the file. As the file size increases, the number of free records at the end of the file decreases.

If you delete items from a configuration file, the records are not immediately recovered, and the middle of your file may contain some unused records. Unused records are not reflected in the Number of Free Records count. If you then compress the file (by specifying 0 for Number of Additional Records and pressing **Compress File**), all data are stored in a contiguous block of records, and all unused records are now located at the end of the file. Thus, compressing a file enables you to determine the actual number of free records in a file before adding or deleting records.

When you press **Compress File**, NMMGR begins compressing the file immediately. The terminal is locked to indicate that NMMGR is not available until finished. When NMMGR has finished compressing a file, it prints the following message in the message field:

Configuration file compressed.

NOTE

Compress time is based on the number of entries in the file. For a file that contains a small amount of data, compression usually takes fewer than 30 seconds. However, compressing a file with a lot of data can take several minutes.

Validate Configuration File

The Validate Configuration File screen (Figure 5-14) allows you to test the validity of a specified subsystem configuration.

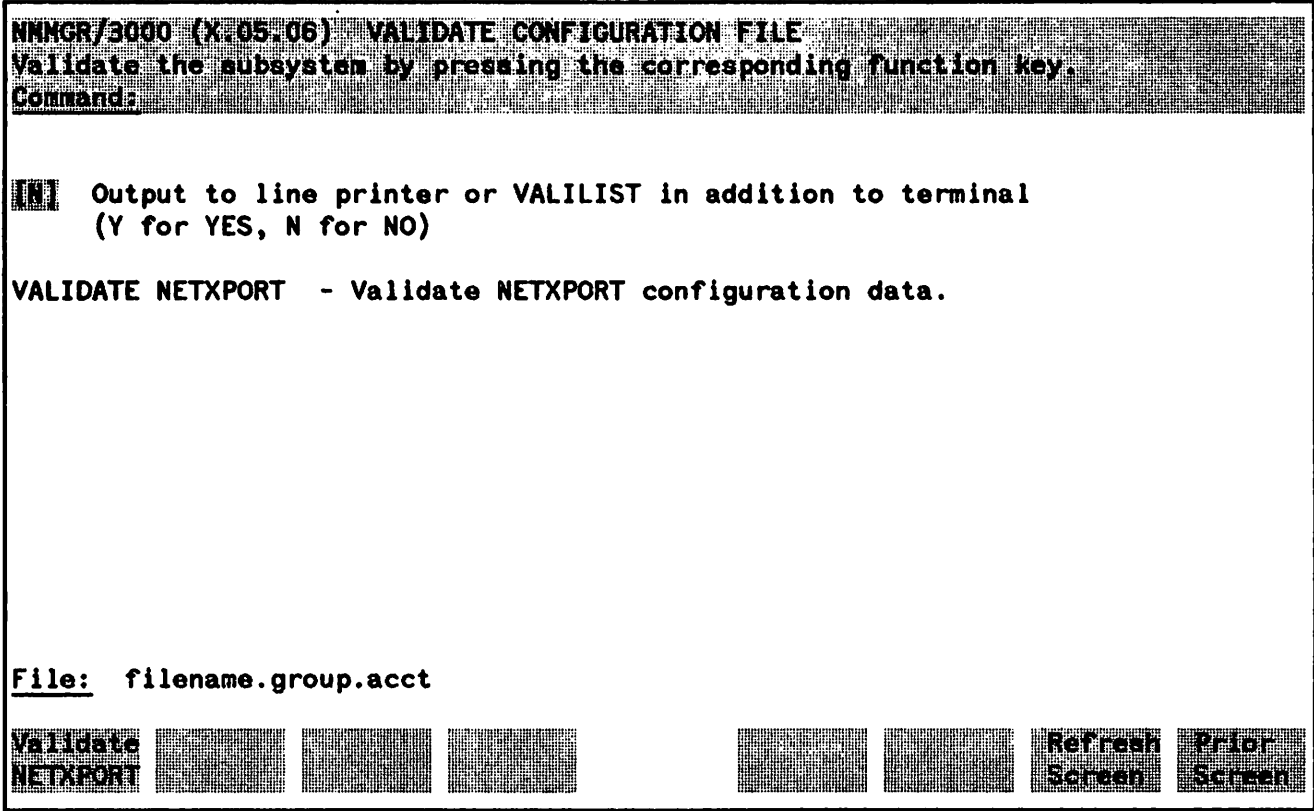


Figure 5-14. Validate Configuration File Screen

At present, you can specify only the Network Transport subsystem for validation. The purpose of the validation process is to ensure that your configuration data is syntactically and logically correct before you activate the node. The Link configuration must be complete before you attempt to validate the Network Transport configuration. This is because the Network Transport validation process uses Link configuration data.

The validation process creates a listing of error messages to pinpoint invalid items. One possible message, for instance, states that a phone number has not been configured for a Dial-type link. When you press the **Validate NETXPORT** key you enter character mode, in which validation errors are listed at your terminal. If you want the listing to be sent to a device in addition to your terminal, change the value to in the box next to Output to VALILIST in addition to terminal on the Validate Configuration File screen. You can have the listing sent to disc or a printer by setting a file equation, or you can have it routed to the default device, which is LP.

The NMS Configurator (NMMGR)

After viewing the messages, if any, press **RETURN** to go back to block mode. The message near the top of the Validate Configuration File screen now tells you if the validation process has completed and, if so, if the configuration is valid. It is possible you will see a message indicating that the validation routine never took place, possibly due to a load error or internal errors. You must see the following message to be sure that your configuration file is valid:

Validation completed; configuration of the selected subsystem is valid.

If you do not see the above message, you see one of these messages:

Validation completed; configuration of the selected subsystem is not valid.

Internal errors occurred during validation.

Cannot invoke subsystem validation routine.

Remember to refer, whenever necessary, to the *NS3000/V Error Message and Recovery Manual*. If you encounter errors that you cannot resolve, notify your HP representative.

The following items are checked during the validation procedure.

- These paths must exist:

LINKCONF

NETXPORT

NETXPORT.GLOBAL

NETXPORT.NODE

NETXPORT.NODE.NAME

NETXPORT.GPROT.TCP

NETXPORT.GRPOT.PXP

NETXPORT.GPROT.IPU

NETXPORT.NI

- Paths expected to have a defined data length are checked. These include:

A path which contains data that should not contain data.

A path which does not contain data that should contain data.

A path which has an incorrect data length.

- At least one NI must be configured for each node. (NETXPORT.NI.niName)

- The TCP retransmission lower bound must be less than the TCP retransmission upper bound. (NETXPORT.GPROT.TCP)
- The TCP initial retransmission timer must be in the range of the lower and upper bound retransmissions timers. (NETXPORT.GPROT.TCP)
- An unknown path will cause a validation error.
- If the number of internet reachable networks configured for an NI (NETXPORT.NI.*niName*.INTERNET.*gatewayn*) is greater than the configured maximum number of networks in the catenet (NETXPORT.GPROT.IPU), routing information will exceed the allocated space in the routing tables.
- If the number of internet gateways for an NI (NETXPORT.NI.*niName*.INTERNET) is greater than the configured maximum number of gateways in the network (NETXPORT.GPORT.IPU), routing information will exceed the allocated space in the routing tables.
- If the number of mapping entries for a router NI (NETXPORT.NI.*niName*.INTERNET) is greater than the number of routing table entries for that NI (NETXPORT.NI.*niName* for Router), there will be insufficient space in the routing tables.

- For Router mapping entries:

The link name must be configured for that NI (NETXPORT.NI.*niName*.LINK for Router, and LINKCONF).

The IP network address must match that NI's network number (NETXPORT.NI.*niName*.PROTOCOL.IP).

If Local and DIAL is enabled for the link, there must be a phone number (in the screen NETXPORT.NI.*niName*.MAPPING.*mapentry*).

If Local and DIAL is enabled for the link, and Security is enabled in dial protocol, there must be a security string (NETXPORT.NI.*niName*.MAPPING.*mapentry*).

The wildcard address, "@", is allowed only when a single link is configured for the network interface (NETXPORT.NI.*niName*.LINK).

When the wildcard address is configured, exactly two router mappings must be configured for the network interface (NETXPORT.NI.*niName*.MAPPING).

There can be at most one mapping entry with the wildcard address configured for each router NI.

- The network address of an internet gateway must be the same as that NI's IP network address.

- For each `NETXPORT.NI.niName.LINK` entry:

The corresponding `LINKCONF` link must be configured (`LINKCONF.Linkname`).

If the network interface type is LAN802.3, the link type must be LAN and the link name must correspond to a LAN802.3 link from `LINKCONF`.

If the link entry corresponds to a Bisync link from `LINKCONF`, the link-entry type must be Direct Dial or Shared Dial.

If the type is Direct Dial or Shared Dial (`NETXPORT.NI.niName.LINK`), the corresponding `LINKCONF` entry must have phone data configured (`LINKCONF.Linkname.PHONEDAT`).

If the type is Direct Connect, the corresponding `LINKCONF` entry must *not* have phone data configured.

If the type is Direct Dial or Shared Dial, and DIAL is enabled for the link, then the Dial Protocol must be configured.

If the type is Direct Dial or Shared Dial and the `LINKCONF` type is ATP/ASNP, the `LINKCONF` subtype must be either modem or European modem.

- If Dial Protocol is configured and security is enabled, there must be a security string configured (`NETXPORT.niName.PROTOCOL.DIAL.SECURITY`).
- A home network must be configured if there is a Gatehalf type NI, and the home network must *not* correspond to the Gatehalf NI or a Loopback NI.
- If Proxy is enabled, and the inbound Proxy multicast address is not present in the configuration file, then a validation warning message will be printed. See the *NS3000/V Error Message and Recovery Manual* for further details.
- If a LAN NI is configured and the Probe multicast address is not present in the configuration file, then a validation warning message will be printed. See the *NS3000/V Error Message and Recovery Manual* for further details.
- If a node has two or more NIs or a router NI with two or more links, and if no IP store-and-forward buffers are configured, then a validation warning message will be printed. See the *NS3000/V Error Message and Recovery manual* for further details.
- If there is a Router-type NI, then there must be one or more configured mapping entries.
- For `LINKCONF LAP-B` entries:
 - The T1 timer parameter should be greater than or equal to the recommended formula value: $400[(\text{Buffer Size} * 8) / \text{Baud Rate}]$ --in hundredths of a second.
 - The maximum number of reads and writes must always be 3 in the data record.
 - The line speed must not be zero.

- The IP Network number for the NETXPORT.NI.*niName*.MAPPING entry must be the same as the IP Network number for that NI.
- If Proxy is not enabled on the Probe Protocol Screen and the inbound Proxy multicast address is present in the configuration file, then a validation warning message will be printed. See the *NS3000/V Error Message and Recovery Manual* for further details.
- Subsystem 3 logging must be configured, and at least one logging class must be configured under subsystem 3.

Configuration Subtree Copy

The Configuration Subtree Copy Screen (Figure 5-15) allows you to copy specified parts of a configuration subtree into either the same configuration file or a different configuration file. The target file can be on a remote node in the network.

```
NMMGR/3000 (X.05.06) CONFIGURATION SUBTREE COPY
Enter source, destination files, and paths to roots of trees to copy.
Command:

Source file: [ ]

Source path:
[ ] . [ ] . [ ] . [ ] . [ ] . [ ] . [ ] . [ ]

Destination file [ ]

Destination path:
[ ] . [ ] . [ ] . [ ] . [ ] . [ ] . [ ] . [ ]

Overwrite existing subtree [N]

File: filename.group.acct

Copy Subtree [ ] [ ] [ ] [ ] [ ] [ ] Refresh Screen Prior Screen
```

Figure 5-15. Configuration Subtree Copy Screen

Description

This screen is used to copy the subtree which begins at the end of the source path, to a subtree which begins at the end of the destination path. The user starts the copy by pressing .

Fields

Source file

This field contains the name of the file where configuration data will be copied from. If this field is left blank, the current configuration file that is open in NMMGR is assumed.

If the file is on a remote node, you must use a file equation, and prefix the file name with an *. You may use an MPE command from the command line to set a file equation without having to leave NMMGR.

Source Path

The source path, a required field, is composed of eight NMMGR path identifier slots. Enter one path identifier in each slot, leaving blanks at the end of each identifier. Leave any unused identifier slots empty.

Destination file

This field contains the name of the file the configuration data will be copied to. If this field is left blank, the current configuration file that is open in NMMGR is assumed.

If the file is on a remote node, the user must use a file equation, and prefix the file name with an @.

Destination Path

The destination path is also composed of 8 path identifiers. You need to enter only those identifiers that are different from the source path. To copy data from the source file to the identical location in the destination file, leave this field blank. If you wish to change the fifth path identifier, then the fifth slot in the destination path should contain data. Only user-selected names can differ among corresponding identifiers in the source and destination paths. User-selected types must match. For example, if the source path includes a direct connect link, the corresponding identifier in the destination path must also be a direct connect link.

Overwrite existing subtree

This required field indicates whether or not existing data in the destination configuration file is to be overwritten when the copy is performed. A Y will overwrite the data, an N will not allow the copy to continue if data exists where the destination subtree starts. The default is N.

NOTE

To perform a copy within the configuration file (which was opened by NMMGR), leave both the source and destination fields blank.

Example

In this example, a subtree copy is being performed from node A to node B. Since the copy is being made to a remote node, the user must make a :DSLIN connection to node B, and set up a file equation to represent node B's configuration file. These steps are shown below. They are shaded because you would see them in inverse video on the screen.

```
Command: :REMOTE HELLO MGR .NET .SYS :DSLIN=B
Command: @FILE CONFIG-NSCONF .NET .SYS :B,OLD
```

The source file and path on node A are entered into the Source file and Source path fields. They appear below.

Source file: INSCONF .NET .SYS

Source path: NETXPORT .NI .LAN1 .INTERNET

The NMS Configurator (NMMGR)

The diagram in Figure 5-16 shows the subtree specified by the path above.

SOURCE: before and after copy (node A)

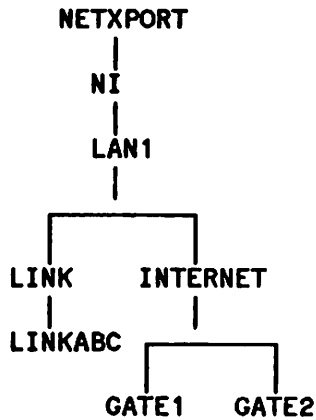


Figure 5-16. Source Subtree

For this copy, the destination file and path were specified as below:

Destination file `[*CONFIG`

Destination path:

`. . . LAN2`

The diagram in Figure 5-17 illustrates the results of the copy.

DESTINATION: before copy (node B)

DESTINATION: after copy (node B)

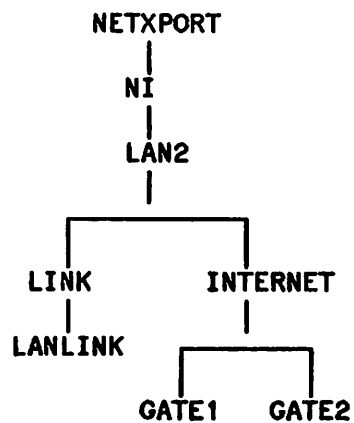
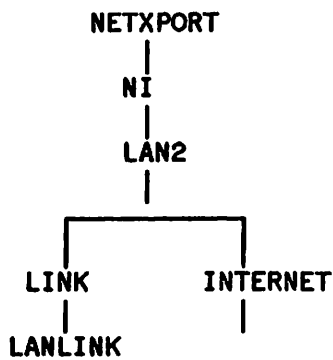


Figure 5-17. Destination Subtrees Before and After Copy

When subtrees contain several records, copies that occur over :DSLIME connections will take considerably longer than copies between two local configuration files. It is several times faster to DSCOPY the configuration file to the destination node, and then perform the subtree copy between two local configuration files.

NOTE

If you are performing a subtree copy with a remote file which is locked by the network transport on the remote system, you will not be able to access this file remotely. However, you can log on to the remote system to copy subtree data. It is not possible to directly copy between two configuration files on different systems which are both locked open. In this case, the steps you would take to copy remote configuration data to a local configuration file are: 1) Log on to the remote system. 2) Run NMMGR and create a new configuration file, which we will call CONFIG1 for purposes of this discussion. 3) While running NMMGR on the remote system, copy the desired subtree into CONFIG1. (If you are unable to copy data, the file may have been opened for exclusive access only, or the network transport may be performing a validation on the file. 4) Exit NMMGR. 5) Return to the local system. (At this point, you may wish to DSCOPY the new file back to the local system so that you can perform a fast subtree copy into the destination file.) 6) Run NMMGR on the local system, and open the file into which you want to copy data. 7) Still in NMMGR, copy subtree data from CONFIG1 into your destination file.

The Error Information Screen

The Error Information Screen displays the last error that NMMGR encountered and associated error messages, if any. It does not display the prompts that are a result of entering invalid data types in fields. This screen is displayed when you type ERRORS in the command window of any screen and press **ENTER**. Figure 5-18 shows an example of an Error Information Screen; Table 5-8 provides a description of the Error Information Screen function keys.

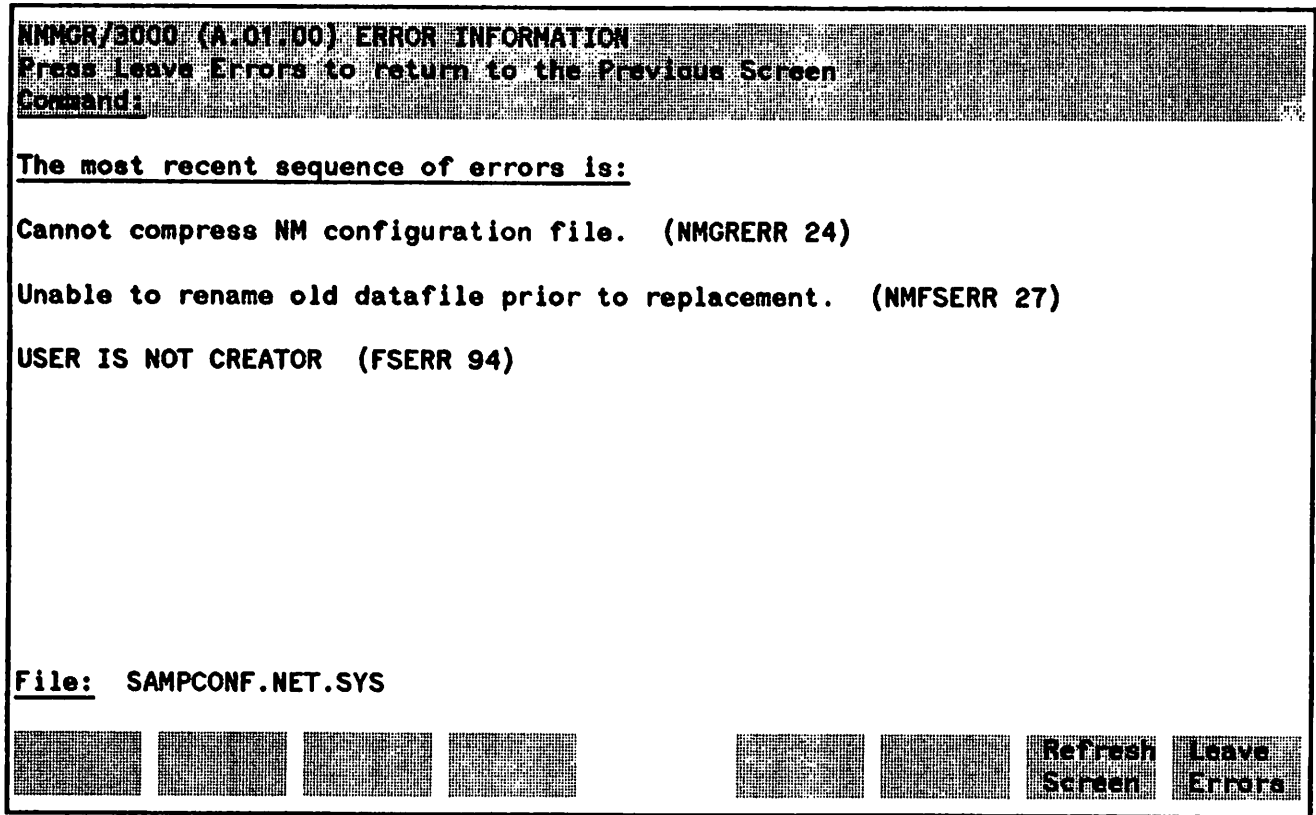




Figure 5-18. Error Information Screen

Figure 5-18 shows the error messages displayed on the Error Information screen if a user who was not the creator of SAMPCONF.NET.SYS tries to compress the file.

TABLE 5-8. ERROR INFORMATION FUNCTION KEYS

Key	Function
	Redisplays screen with current configuration file data.
	Leaves the Error Information Screen and returns to the screen from which you called the Error Information Screen.

In most cases, you do not need to use the Error Information Screen because NMMGR error messages displayed on other screens usually contain enough information for you to correct the error and continue operation. However, if you do not know the cause of the error, or if a more serious error is encountered, use the Error Information Screen to see if any other error messages are associated with the NMMGR error. As many as five levels of error messages can be displayed in the Error Information Screen, depending on where the error occurred in the software. The hierarchy of errors returned by NMS is shown in Figure 5-18. The top level is the NMMGR error message, and the other levels come from software accessed by NMMGR.

COPYING CONFIGURATION DATA

NMMGR features a configuration file copy utility named COPYCONF. COPYCONF allows you to perform the same kinds of copies you would execute from the Configuration Subtree Copy screen. Since it can be invoked from a stream file, you can use it to transfer configuration data to multiple nodes automatically. Note that this utility is accessed through maintenance mode. Maintenance mode is discussed in Section 14.

The syntax is shown below.

Syntax:

```
COPYCONF spath:sfilename, dpath:dfilename [;KEEP]
```

Parameters

spath:sfilename

The path to the beginning of the subtree to be copied from, and the name of the file in which it resides. The path is composed of up to eight NMMGR path identifiers. Enter the NMMGR path identifiers that will lead to the beginning of the subtree to be copied. The file name must be separated from the path by a colon and must be specified in filename.group.account form, or, in place of the file name, an asterisk can precede a formal designator to specify a file equation.

dpath:dfilename

The path to the beginning of the subtree to be copied to, and the name of the file in which it resides. The destination path is also composed of up to eight NMMGR path identifiers. Enter the NMMGR path identifiers that lead to the beginning of the destination path. The file name must be separated from the path by a colon and must be specified in filename.group.account form, or, in place of the file name, an asterisk can precede a formal designator to specify a file equation.

NOTE

All type select parameters in the path that specifies the root of the subtree to be copied must be of the same type for the source and destination configuration files. If they are not, an error will be flagged, and no copy will take place.

KEEP

(Optional.) A parameter that prevents the copy if it would overwrite existing data.

NOTE

If you do not specify this parameter, and data exists in the subtree specified, it will be overwritten.

When subtrees contain several records, copies that occur over DSLINE connections will take considerably longer than copies between two local configuration files. It is several times faster to DSCOPY the configuration file to the destination node, and then perform the subtree copy between two local configuration files.

Example

The example in "Configuration Subtree Copy" is used again to illustrate how the same subtree copy would be performed using the COPYCONF command. Again, the :DSLIME connection and file equation would be prepared as seen below.

```
:REMOTE HELLO MGR.NET.SYS:DSLIME=B
:FILE CONFIG-NSCONF.NET.SYS-B.OLD
```

The COPYCONF command would be entered as follows, at the prompt **NMMGR:**

```
:COPYCONF NETXPORT NI.LAN1 INTERNET-NSCONF NETXPORT NI.LAN2 INTERNET-NSCONF
```

To see an illustration of the source subtree, see Figure 5-16. To see the destination subtree before and after the copy has taken place, see Figure 5-17.

MAKING CONFIGURATION CHANGES

As mentioned earlier in this section, the network transport permits on-line reconfiguration of mapping and internet information but does not permit configuration changes to non-reconfigurable items while the transport is active. Special guided configuration options have been provided in order to permit on-line changes on allowable items.

This subsection describes a method for handling both on-line and off-line configuration changes so that network operation is minimally interrupted.

The basic approach is to create a configuration file that is used for making all configuration changes. We will refer to such a file as NSCONF.MET.SYS. When the transport requires reconfiguration, changes can be made to NSCONF, then copied into the NSCONF.MET.SYS file. If you are making changes to mapping and internet information only, you can perform the file copy while the transport is active; if you are making more extensive changes, you first must deactivate the transport.

To create an NSCONF file, simply run NMMGR and use the **Create Config** key. Then, assuming you already have an NSCONF file, you can use the subtree copy facility from the Utility screen to copy network transport data (NETXPORT, LINKCONF and LOGGING branches) from NSCONF.MET.SYS to NSCONF.MET.SYS.

Once NSCONF contains the complete transport configuration, use the Netxport Update branch of Guided Configuration to modify mapping or internet data; use the Netxport Configuration branch of Guided Configuration to make more extensive changes. Be certain to validate your configuration.

If you make mapping and internet configuration changes only, run NMMGR with a command file to copy these subtrees into your active configuration file. For example, a UDC could be written as such:

```
ONLINECHANGES (udc name)
FILE NMMGRCMD=<command filename>
RUN NMMGR.PUB.SYS
RESET NMMGRCMD
NETCONTROL UPDATE=INTERNET;NET=niName
NETCONTROL UPDATE=MAPPING;NET=niName
```

The command file should contain statements for each network interface. An example of a command file is shown below. Also, *niName* above should be replaced with the name of the desired network. For simplicity, one command file could be written to copy the mapping and internet data for all networks, even if changes occur to only one network. While the transport is active, LAN and Gatehalf network interface types permit internet reconfiguration; router network interface types permit internet and mapping reconfiguration.

The following sample command file contains typical COPYCONF commands showing how internet and mapping information could be copied from NSCONF.MET.SYS to NSCONF.MET.SYS. For readability, each command is broken into two lines, but NMMGR requires that the entire command be shown on a single line in your command file.

```
COPYCONF NETXPORT.NI.niName.INTERNET:NSCONF.MET.SYS,
          NETXPORT.NI.niName.INTERNET:NSCONF.MET.SYS
COPYCONF NETXPORT.NI.niName.MAPPING:NSCONF.MET.SYS,
```

NETXPORT.NI.niname.MAPPING:NSCONF.NET.SYS

EXIT

If more extensive changes must be made, it is easiest to replace the entire configuration file. For example, if you have finished making changes to the NSCONF file with NMMGR, the changes will take effect when the following commands are executed:

```
OFFLINECHANGES (udc name)
NETCONTROL STOP
PURGE OLDCONF.NET.SYS
FCOPY FROM=NSCONF.NET.SYS;TO=OLDCONF.NET.SYS;NEW (backup copy)
PURGE NSCONF.NET.SYS
FCOPY FROM=NSCONF.NET.SYS;TO=NSCONF.NET.SYS;NEW (move into place)
NETCONTROL START;NET=niName1
NETCONTROL START;NET=niName2 (etc.)
```

The reason for making a backup copy of the existing NSCONF file is that the backup copy can be used if you ever need to go back to your original configuration. Be aware that you cannot FCOPY a configuration file if you are still making changes with NMMGR. To quickly exit NMMGR, type "q" in the command window and press **ENTER**.

NOTE

Each time subtrees overwrite existing subtrees, the amount of available space within the configuration file becomes smaller. If you are frequently reconfiguring your mapping or internet data, you may want to expand the NSCONF and NSCONF.M files to avoid running out of available file space. The Compress function within the Utility screen of NMMGR can be used to change the size of a file; in addition, it removes inactive subtrees left by prior subtree copy operation. A file cannot be expanded while it is open.

If your operators are accustomed to making on-line changes on their own, they should follow set procedures like those listed above. This way, you can avoid situations where on-line changes might be made directly to NSCONF, then subsequently overwritten with a potentially out-of-date NSCONF.M file.



NOTE

HP strongly recommends that you use Guided Configuration to initially configure each node, and for most network maintenance and updating. Use manual configuration *only* if Guided Configuration does not provide access to the configuration data you need to change.

Guided configuration comprises two branches: NETXPORT CONFIGURATION and NETXPORT UPDATE. The first of these two branches, NETXPORT CONFIGURATION, allows you to create or modify the configuration file for all network interface types:

- Loopback (labeled LOOP)
- IEEE 802.3 (labeled LAN802.3)
- Router--two kinds of guided configuration exist for router networks. One kind (labeled PC ROUTER) is for a router network consisting of an HP 3000 with Asynchronous SERIAL Network Links to personal computers. The other kind (labeled ROUTER) is for a router network with only HP 3000s.
- Gateway half (labeled GATEHALF)

The sequence of screens that you will encounter as you proceed through guided configuration for each of these network interfaces includes the screens necessary for link and network transport configuration, and validation of the completed configuration file.

The second branch of guided configuration, NETXPORT UPDATE, provides a guided configuration interface for the following two types of online configuration changes (changes that you can make to an active file):

- Updating internet data for network interfaces (labeled UPDATE INTERNET)
- Updating mapping data for router network interfaces (labeled UPDATE ROUTER MAPPING)

The top three levels of the Guided Configuration tree are shown in Figure 6-2.

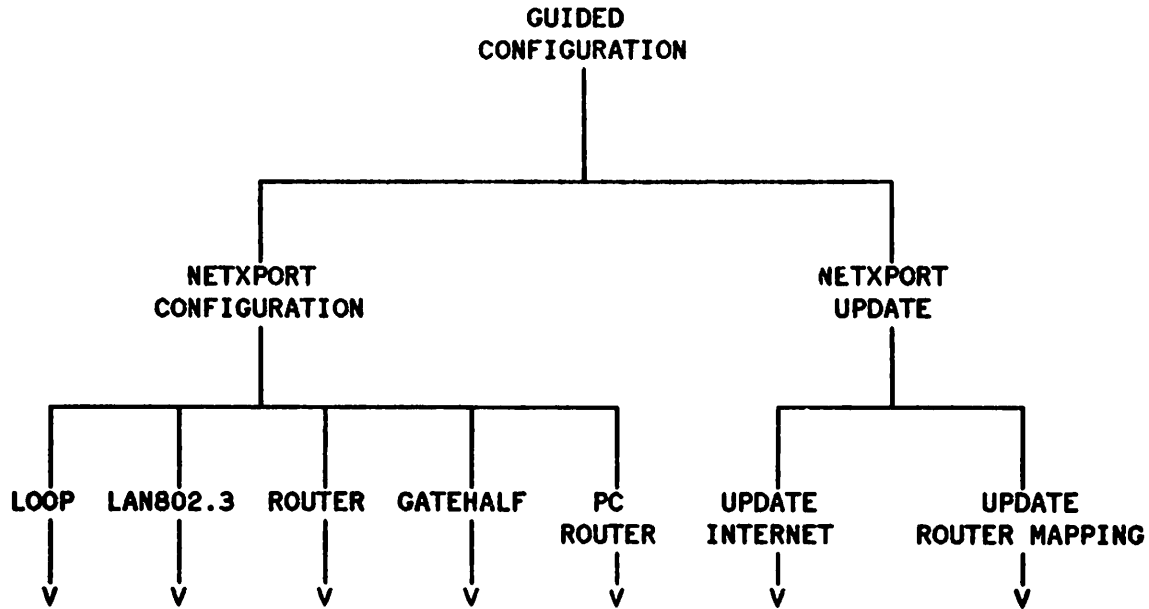


Figure 6-2. Guided Configuration Tree

NOTE

The ROUTER branch and the PC ROUTER branch of Guided Configuration are similar; however, the PC ROUTER branch is designed for configuration of a router network specifically composed of personal computers connected to the HP 3000 via Asynchronous SERIAL Network Links. The defaults imposed by using the PC ROUTER branch are those that HP recommends for such a network, and they differ from the defaults imposed by using the ROUTER branch. In addition, using the PC ROUTER branch allows you to bypass certain screens included in the ROUTER branch, such as those required to configure internet data, since no transparent internet communication can be initiated from or directed to personal computers.

CORRECTING CONFIGURATION ERRORS

Beyond the Configuration or Update level of the configuration tree, Guided Configuration is forced to proceed in a *forward* sequence. The **Prior Screen** key, which is common to most screens in the normal configuration process, is disabled. Furthermore, while in Guided Configuration, you will not be able to branch to other configuration screens by specifying their path in the command line. These restrictions are necessary to enable the configuration to be completed in an orderly and directed fashion.

If it is necessary to leave NMMGR altogether before the configuration is completed, issue the EXIT command in the command line and press **(ENTER)**. You will be warned that you are in the middle of Guided Configuration, and asked to repeat the command if you still want to exit. Exiting in the middle of Guided Configuration will result in an incomplete and unvalidated configuration file.

If you have started a configuration and find that you have made a mistake, type STOP on the command line and press **(ENTER)**. Guided Configuration will stop. Then, by typing @NIGUIDE and pressing **(ENTER)**, you can restart the Guided Configuration, fixing any errors on screens you revisit.

If errors occur during validation, a path name will be displayed as part of the error message, identifying the data screen where the error has apparently occurred. Note (or print out) the screen path name(s). Press the **Prior Screen** key to return to the Guided Configuration screen where you started. Re-enter your network interface name and press the corresponding function key. This will allow you to go back and fix any errors in the configuration you just created. You also have the option of using direct branching to visit the screens on which the validation routine reported errors.

If internal errors or errors that prevent Guided Configuration from continuing occur, you will be returned to your initial Guided Configuration screen and an error message will be printed. Type ERRORS in the command window and press **(ENTER)** to see other possible errors. The problem in most cases is either that the configuration file is locked or that a file is not properly installed. One situation that would cause a file-locking error is if you tried to update information other than internet data or router mapping data while the transport still was active. In this case, you should follow the procedures in Section 5 for making configuration changes. As for installation errors, you can check these by running NMMINT.PUB.SYS;PARM=24. For NMMINT information, refer to Volume II, Section 2.

NETXPORT CONFIGURATION

The Netxport Configuration branch directs the guided configuration of loopback, LAN, router, gateway half, and PC router networks. This branch can also be used to modify any of these networks in an existing configuration file. Netxport Configuration is reached by selecting **Go To NET CON** from the Guided Subsystem Configuration screen shown in Figure 6-1. The network interface selection is made from the Guided Network Interface Configuration screen shown in Figure 6-3

```

NNMGR/3000 (X-01-22) GUIDED NETWORK INTERFACE CONFIGURATION
Enter Net Interface name to configure, then press a Topology function key.
Command:

Network Interface Name [ ]

LOOP      - Guided Configuration Of LOOPBACK.
LAN802.3  - Guided Configuration Of Local Area Network.
ROUTER    - Guided Configuration Of Router.
GATEHALF  - Guided Configuration Of Gateway Half.
PC ROUTER - Guided Configuration Of ASNP Router For PCs.

NOTE: Be certain to use "NETXPORT UPDATE" to reconfigure an active network.

File:  FILENAME.NET.SYS

Go To  Go To  Go To  Go To  Go To  Refresh  Prior
LOOP  LAN802.3  ROUTER  GATEHALF  PC  Screen  Screen

```

Figure 6-3. Guided Network Interface Configuration

You must supply a name for the network interface, and then select the type of network interface by pressing the corresponding function key **[F1]** to **[F5]**. If you want to modify an existing network interface, you can review the configured network interface names by typing **@NETXPORT.NI** in the command line and pressing **(ENTER)**. When you are finished, press the **Prior Screen** key to return to the Guided Configuration screen. If you are configuring a new network interface, Guided Configuration immediately begins supplying appropriate default values to the configuration subsystems. Guided Configuration then proceeds to the screen sequence relevant to the type selected.

Tables 6-1 through 6-5 show the sequence of steps for each of the five Guided Network Interface Configuration routines. For each step, the tables show the screen or screens accessed and the fields for which you must supply a value. The table also provides a reference figure for each step. You must refer to that figure to see the actual screen display and read the detailed descriptions of the required fields in that screen.

TABLE 6-1 NETXPORT CONFIGURATION - LOOPBACK NI

Step	Screen Name	Required Values	Reference
1	GUIDED NETWORK INTERFACE CONFIGURATION	NI Name (Choose LOOP)	Figure 6-3 (p. 6-5)
2	NODE NAME CONFIGURATION	Local Node Name	Figure 8-3 (p. 8-5)
3	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

TABLE 6-2 NETXPORT CONFIGURATION - LAN802.3 NI

Step	Screen Name	Required Value	Reference
1	GUIDED NETWORK INTERFACE CONFIGURATION	NI Name (Choose LAN802.3)	Figure 6-3 (p. 6-5)
2	NODE NAME CONFIGURATION (Visited only if not previously configured)	Local Node Name	Figure 8-3 (p. 8-5)
3	LINK CONFIGURATION	Link Name	Figure 7-1 (p. 7-4)
4	LINK DATA	LDEV #	Figure 7-2 (p. 7-6)
5	PROBE PROTOCOL CONFIGURATION	Proxy Enabled	Figure 9-4 (p. 9-10)
6	IP PROTOCOL CONFIGURATION	IP Internet Address	Figure 9-3 (p. 9-7)
7	NEIGHBOR GATEWAYS (Repeat for each gateway; NEXT SCREEN to continue to Step 9)	Gateway Name	Figure 9-7 (p. 9-18)
8	NEIGHBOR GATEWAY REACHABLE NETWORKS (Repeat for each network; NEXT SCREEN to return to step 7)	Neighbor Gateway IP Internet Address IP Network Address Number of Hops	Figure 9-8 (p. 9-19)
9	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

TABLE 6-3 NETXPORT CONFIGURATION - ROUTER NI

Step	Screen Name	Required Values	Reference
1	GUIDED NETWORK INTERFACE CONFIGURATION	NI Name (Choose ROUTER)	Figure 6-3 (p. 6-5)
2	NODE NAME CONFIGURATION (Visited only if not previously configured)	Node Name	Figure 8-3 (p. 8-5)
3	LINK CONFIGURATION (Repeat Steps 3-6 for each link; NEXT SCREEN to continue to step 7)	Link Name Protocol Type	Figure 7-1 (p. 7-4)
4	LINK CONFIGURATION: LINK DATA	LDEV #	Figure 7-6 (Bisync) (p. 7-11) Figure 7-9 (LAP-B) (p. 7-19) Figure 7-12 (ASNP) (p. 7-27)
5	ROUTER NETWORK INTERFACE LINKS	Link Name Connection Type	Figure 10-6 (p. 10-17)
6	DIRECT CONNECT LINK CONFIGURATION or ROUTER DIAL LINK CONFIGURATION	None	Figure 10-7 (Direct) (p. 10-19) Figure 10-8 (Dial) (p. 10-21)
7	ROUTER NETWORK INTERFACE CONFIGURATION	Network Hop Count Idle Device Timeout	Figure 10-1 (p. 10-3)
8	IP PROTOCOL CONFIGURATION	IP Internet Address	Figure 10-3 (p. 10-8)
9	ROUTER MAPPING CONFIGURATION (Repeat as applicable; NEXT SCREEN to continue to step 11)	Router Node Name	Figure 10-12 (p. 10-30)

TABLE 6-3 NETXPORT CONFIGURATION - ROUTER NI (cont.)

Step	Screen Name	Required Values	Reference
10	ROUTER REACHABLE NODES	IP Internet Address Link Name Adjacent/Non-adjacent Phone # (if applicable)	Figure 10-13 (p. 10-32)
11	NEIGHBOR GATEWAYS (Repeat for each gateway; NEXT SCREEN to continue to step 13)	Gateway Name	Figure 10-9 (p. 10-24)
12	NEIGHBOR GATEWAY REACHABLE NETWORKS (Repeat for each network; NEXT SCREEN to return to step 11)	Neighbor Gateway Internet Address IP Network Address Number of Hops	Figure 10-10 (p. 10-25)
13	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

TABLE 6-4 NETXPORT CONFIGURATION - GATEHALF NI

Step	Screen Name	Required Values	Reference
1	GUIDED NETWORK INTERFACE CONFIGURATION	NI Name (Choose GATEHALF)	Figure 6-3 (p. 6-5)
2	GLOBAL TRANSPORT CONFIGURATION	Home Network Name	Figure 8-4 (p. 8-7)
3	NODE NAME CONFIGURATION (Visited only if not previously configured)	Local Node Name	Figure 8-3 (p. 8-5)
4	LINK CONFIGURATION (Repeat steps 4-7 for each link; NEXT SCREEN to continue with step 8)	Link Name Protocol Type	Figure 7-1 (p. 7-4)
5	LINK CONFIGURATION: LINK DATA	LDEV #	Figure 7-6 (Bisync) (p. 7-11) Figure 7-9 (LAP-B) (p. 7-19) Figure 7-12 (ASNP) (p. 7-27)
6	GATEWAY HALF NETWORK INTERFACE LINKS	Line Name Connection Type	Figure 11-6 (p. 11-16)
7	DIRECT CONNECT LINK CONFIGURATION or GATEWAY HALF DIAL LINK CONFIGURATION	None Phone Number	Figure 11-7 (Direct) (p. 11-17) Figure 11-8 (Dial) (p. 11-19)
8	GATEWAY HALF NETWORK INTERFACE CONFIGURATION	Idle Device Timeout Value	Figure 11-1 (p. 11-3)
9	IP PROTOCOL CONFIGURATION	IP Internet Address	Figure 11-3 (p. 11-7)

TABLE 6-4 NETXPORT CONFIGURATION - GATEHALF NI (cont.)

Step	Screen Name	Required Values	Reference
10	NEIGHBOR GATEWAYS (Repeat for each gateway; NEXT SCREEN to continue to step 12)	Gateway Name	Figure 11-9 (p. 11-23)
11	NEIGHBOR GATEWAY REACHABLE NETWORKS (Repeat for each network; NEXT SCREEN to return to Step 10)	Neighbor Gateway IP Internet Address IP Network Address Number of Hops	Figure 11-10 (p. 11-24)
12	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

TABLE 6-5 NETXPORT CONFIGURATION - PC ROUTER

Step	Screen Name	Required Values	Reference
1	GUIDED NETWORK INTERFACE CONFIGURATION	NI Name (Choose PC ROUTER)	Figure 6-3 (p. 6-5)
2	NODE NAME CONFIGURATION (Visited only if not previously configured)	Node Name	Figure 8-3 (p. 8-5)
3	LINK CONFIGURATION (Repeat Steps 3-6 as applicable; NEXT SCREEN to continue to step 7)	Link Name	Figure 7-1 (P. 7-4)
4	LINK CONFIGURATION: LINK DATA	LDEV #	Figure 7-12 (p. 7-27)
5	ROUTER NETWORK INTERFACE LINKS	Link Type	Figure 10-6 (p. 10-17)
6	DIRECT CONNECT LINK CONFIGURATION or ROUTER DIAL LINK CONFIGURATION	None	Figure 10-7 (Direct) (p. 10-19) Figure 10-8 (Dial) (p. 10-21)
7	IP PROTOCOL CONFIGURATION	IP Internet Address	Figure 10-3 (p. 10-8)
8	ROUTER MAPPING CONFIGURATION (Repeat as applicable; NEXT SCREEN to continue with step 10)	Router node name	Figure 10-12 (p. 10-30)
9	ROUTER REACHABLE NODES (Repeat as applicable; NEXT SCREEN to return to Step 8)	IP Internet Address Link Name	Figure 10-13 (p. 10-32)
10	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

NETXPORT UPDATE

The Netxport Update branch directs the Guided Configuration process for two online configuration updates.

UPDATE INTERNET leads to the screen sequence for updating gateway internet data on configured LAN or router networks or on gateway halves.

UPDATE ROUTER MAPPING leads to the screen sequence for updating mapping data on configured router networks.

It is important to note the different purposes of the two Guided Configuration branches. The Netxport Configuration branch adds or updates entire network interface configurations, and may not be used to update an active configuration file. The Netxport Update branch, on the other hand, performs guided updates of a selected part of existing, validated networks, and is intended for use in updating the active configuration.

Select **Go To UPDATE** in the Guided Subsystem Configuration screen to reach the Guided Configuration Update screen. Select the desired update path by pressing the corresponding function key, **F1** or **F2**, as shown in Figure 6-4.

Tables 6-6 and 6-7 show the sequence of steps followed by each of the two Guided Configuration Updates. For each step, the tables show the screen or screens accessed and the fields for which you must supply a value. The table also provides a reference figure for each step. You must refer to that figure to see the actual screen display and read the detailed descriptions of the required fields in that screen.

NMMGR/3000 (X.01.22) GUIDED NETXPORT UPDATE
Enter Net Interface name to update, then press a function key.
Command:

Network Interface Name []

UPDATE INTERNET - Update Internet Data For Specified Network Interface.
UPDATE ROUTER MAPPING - Update Mapping Data For Specified Router Network Interface.

File: FILENAME.NET.SYS

Go To	Go To					Refresh	Prior
INTERNET	RTR MAP					Screen	Screen

Figure 6-4. Guided Configuration Update

TABLE 6-6 NETXPORT UPDATE - UPDATE INTERNET

Step	Screen Name	Required Values	Reference
1	GUIDED NETXPORT UPDATE	NI Name (Choose INTERNET)	Figure 6-4 (p. 6-14)
2	NEIGHBOR GATEWAYS (Repeat as desired; NEXT SCREEN to continue to step 4)	Gateway Name	Figure 11-9 (p. 11-23)
3	NEIGHBOR GATEWAY REACHABLE NETWORKS (Repeat as desired; NEXT SCREEN to return to Step 2)	Neighbor Gateway Internet Address IP Network Address Number of Hops	Figure 11-10 (p. 11-24)
4	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

TABLE 6-7 NETXPORT UPDATE - UPDATE MAPPING

Step	Screen Name	Required Values	Reference
1	GUIDED NETXPORT UPDATE	NI Name (Choose RTR MAP)	Figure 6-4 (p. 6-14)
2	ROUTER MAPPING CONFIGURATION (Repeat as applicable; NEXT SCREEN to continue to step 4)	Router node name	Figure 10-12 (p. 10-30)
3	ROUTER REACHABLE NODES	IP Internet Address Link Name Entry Priority Phone # (if applicable)	Figure 10-13 (p. 10-32)
4	VALIDATE CONFIGURATION FILE	None	Figure 5-14 (p. 5-35)

The screens described in this section are used for link configuration. NMMGR provides four kinds of screens for configuration of each link. Which screens you are led to depends on what you enter in the first screen, the LINK CONFIGURATION screen; however, you will always proceed to a screen in which you must configure link data. From there, you can proceed to a screen in which you configure data about tracing, and (except for IEEE 802.3 links) to a screen in which you configure information about the telephone connection, for dial links.

The four kinds of screens are described below, with the level of indentation indicating each screen's place in the configuration tree:

LINK CONFIGURATION - allows you to specify the links configured for this node, including the link's identifying name and whether it uses IEEE 802.3, BSC, LAP-B, or ASNIP as a link-level protocol.

LINK DATA (One of four screens corresponding to the link level protocol chosen in the LINK CONFIGURATION screen.) Each LINK DATA screen allows you to configure data necessary for link level software, such as the logical device (Ldev) number of the hardware card, the number of buffers (which determines the amount of data accepted at the link level before packets are discarded), and parameters specific to the link-level protocol being used.

LINK TRACE DATA - From each LINK DATA screen, you can proceed to the LINK TRACE DATA screen for the link being configured. This screen allows you to enable link level tracing for this link, specify which link level activities will be recorded, and specify the name of the trace file.

LINK PHONE DATA - From each LINK DATA screen except that for IEEE 802.3 links, you can proceed to the LINK PHONE DATA screen for the link being configured. This screen allows you to specify whether the dial connection to a remote node is initiated by manual dial (in which a system operator must dial the telephone number) or auto dial (in which the number is automatically dialed by a device with auto dial capability).

NOTE

Configurable fields described in this manual are required unless otherwise stated.

All fields in the Link Configuration screens are noted as "HP modifiable." and should be changed only upon the recommendation of your HP representative.

On the screens shown in this section, fields that must be configured when performing guided configuration are underlined.

NOTE

Information that you specify in the NMMGR program always overrides any similar information entered within the SYSDUMP facility.

LINK CONFIGURATION

The select screen in Figure 7-1 is displayed when you press the function key for **Go To LINKCONF** at the Configuration Menu Screen. It is also displayed when you type the path name:

@LINKCONF

in the command window of any screen and press **(ENTER)**

Use the fields and the function keys of the select screen to perform the desired action.

- To define a new link configuration, specify the link name and the type; then press **Add**. The path for the selected link name is added to the configuration file and the data screen for the type specified is displayed.
- To modify an existing link configuration, specify the link name; then press **Update**. The data screen on the path for the specified link name is displayed.
- To change the name of an existing link configuration, specify the link name and a new name; then press **Rename**. The previously configured link name is replaced and the screen displays the new name in the display fields labeled Configured Links.
- To delete an existing link configuration, specify the link name, then press **Delete**. The previously configured link name is deleted and is no longer displayed in the display fields labeled Configured Links.

```

NNMGR/3000 (A.01.00) LINK CONFIGURATION
Type in name of Item to Update, Delete, or Rename; or Add a new item.
Command:

Path: LINKCONF

[ ] Link name [ ] Types: SNA/SDLC, LAN802.3
[ ] New name [ ] Types: BSC, LAPB, ATP/ASNP
                        (if new)

Configured Links

Name      Type      Name      Type      Name      Type
[ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ]

File: filename.NET.SYS

Next      Prev      Delete  Rename      Add      Update  Refresh  Prior
Page      Page
  
```

Figure 7-1. Link Configuration Screen

Fields

Link name

(HP modifiable) Select the link name for one of the following: 1) LAN802.3 link, 2) BSC link, 3) LAP-B link, or 4) ATP/ASNP link.

The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic. The link name must match the link name configured in the corresponding network transport configuration screen.

Types

(HP modifiable.) Required only when adding a link. Enter the type shown on the screen that corresponds to your link. Choose LAN802.3 if you are using StarLAN/3000, ThinLAN/3000, or the ThickLAN option.

Choose LAP-B if you are using an NS Point-to-Point 3000/V Link with the LAP-B protocol.

Choose BSC if you are using an NS Point-to-Point 3000/V Link with the BSC protocol.

Choose ATP/ASNP if you are using an Asynchronous Serial Network Link.

For the SNA/SDLC choice, follow the instructions for choosing your link type according to the *SNA Link Services* manual (part number 30246-90003).

New name

(HP modifiable.) Required only when renaming a link. Enter a new link name. The new name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

LINK CONFIGURATION: LAN802.3 LINK DATA

The screen in Figure 7-2 is displayed when you select a link name and the link type LAN802.3 at the Link Configuration Screen (Figure 7-1) and press **Add** or **Update**. It is also displayed when you type the path name:

@LINKCONF.*linkname*

in the command window of any screen and press **(ENTER)**, where *linkname* is the configured LAN802.3 link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data:** flag is set to **Y**.

```

NMGR/3000 (A.01.00) LINK CONFIGURATION: LAN802.3 LINK DATA      Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname

[  ] Logical Device      (1-999)
[0000] Driver Options in Hex (0 - normal mode operation)
[ 16] Maximum Outstanding Reads (7-64)
[  7] Maximum Outstanding Writes (7-64)
[ 42] Number of Buffers (16-138)
[ Y ] Use Factory-Configured Local Station Address? (Y/N)
[FF-FF-FF-FF-FF-FF] Local Station Address in Hex
                    (replace default if above = N)

File: filename.NET.SYS

Go To  Update  Refresh  Prior
TRACEDAT Data  Screen  Screen
    
```

Figure 7-2. LAN802.3 Link Data Screen.

Fields

Logical Device (HP modifiable.) Enter the logical device number of the LANIC as configured in SYSDUMP.

Range: 1-999

Driver Options in Hex	(HP modifiable.) Enter 0 for normal mode of operation. All other options are reserved. Default Value: 0 Range: 0-9, A-F hexadecimal
Maximum Outstanding Reads	(HP modifiable.) Specifies the maximum number of reads that can be outstanding at any given time. Default Value: 16 Range: 7-64
Maximum Outstanding Writes	(HP modifiable.) Specifies the maximum number of writes that can be outstanding at any given time. Default Value: 7 Range: 7-64
Number of Buffers	(HP modifiable.) The maximum amount of incoming data that the link level can accept before discarding packets. The number of buffers to configure can be calculated with the following formula: $numBuffers := 2 \times maximum\ outstanding\ reads + 10$ where: <i>numBuffers</i> is the number of buffers to be configured, Default Value: 42 Range: 16-138
Factory-Configured Local Node Address?	(HP modifiable.) The LANIC board is supplied with a 48-bit station address. These are guaranteed to be unique. Do not change the factory configured local node address except on the specific instructions of your HP representative. Default Value: Y
Local Node Address	(HP modifiable.) This field is to be used only with specific instructions from your HP representative. It allows you to enter a station address to replace the factory configured address. The format <i>must</i> be compatible with HP software requirements. Your HP representative will supply instructions in the unlikely event that you need to enter an address to replace the default.

After configuring link data, you can configure tracing for the link. The Link Trace Data Screen allows you to specify the events to trace and the name of the file for storing the tracing information. *For best performance, do not enable tracing.* You can override NMMGR activated link tracing by using the LINKCONTROL TRACE=OFF command. Using the LINKCONTROL command to enable and disable link tracing is described in the "Commands" section (Section 1) of Volume II of this manual set. For information on formatting the link trace file, refer to the *LAN/3000 Diagnostic and Troubleshooting Guide*.

Fields

- Link trace enabled?** (HP modifiable.) Enter Y (YES) to enable link tracing, N (NO) otherwise. Can be overridden with the LINKCONTROL command. If you do enable link tracing, you are required to enter a trace file name. For best performance, do not enable tracing.
- Default Value:** N
- Trace ALL or ERRORS only** (HP modifiable.) Enter 1 (ALL) to trace all events, 0 (ERRORS) to trace errors only.
- Default Value:** 0
- WRAP or DISCARD overflow?** (HP modifiable.) Enter 1 (WRAP) to overlay previous internal record entries with overflow trace entries, 0 (DISCARD) if you want it to discard the overflow.
- Default Value:** 0
- PRCT?** (HP modifiable.) Enter Y (YES) to record Receive Controls (PRCTs) received on the line, N (NO) otherwise.
- Default Value:** Y
- PRTX?** (HP modifiable.) Enter Y (YES) to record Receive Text (PRTXs) received on the line, N (NO) otherwise.
- Default Value:** Y
- PSCT?** (HP modifiable.) Enter Y (YES) to record Send Controls (PSCTs) sent on the line, N (NO) otherwise.
- Default Value:** Y
- PSTX?** (HP modifiable.) Enter Y (YES) to record Send Text (PSTXs) sent on the line, N (NO) otherwise.
- Default Value:** Y
- ICD?** (HP modifiable.) Enter Y (YES) to record Interconnect Driver Entries (ICDs), N (NO) otherwise.
- Default Value:** N

Link Configuration

Trace File

(HP modifiable.) Required if link trace is enabled. Name of the disc file in which you want to record tracing. Must be a valid MPE file name. Enter the filename in the format *filename.groupname.acctname*. The fully qualified file name can be as many as 26 characters. Lockwords are not allowed for trace files.

Do not specify the same file name with the NMMGR configuration as specified with the LINKCONTROL command.

Only one active trace is allowed per link. Refer to *LAN/3000 Diagnostic and Troubleshooting Guide* for information on how to format the trace file.

LINK CONFIGURATION: BSC LINK DATA

The screen in Figure 7-6 is displayed when you select a link name and the link type BSC at the Link Configuration Screen (Figure 7-1) and press **Add** or **Update**. It is also displayed when you type the path name:

@LINKCONF.*linkname*

in the command window of any screen and press **ENTER**, where *linkname* is the configured BSC link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NMGR/3000 (X.05.06) LINK CONFIGURATION:   BSC LINK DATA           Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:
Path: LINKCONF.linkname

   [  ] Logical device      (1-999)
  [900] Connect timeout    (60-900 seconds or 0)
  [15 ] Number of error recovery retries (1-255)
   [ 0 ] Clear to send delay (0-20 tenths of a second)
   [N ] Data set ready delay (Y/N)
  [1500] Buffer size (32-1500 bytes)
  [12 ] Number of buffers (10-50)
  [9600] Line speed in bits/second (1200,2400,4800,9600,19200,38400,56000)
   [ 0 ] Leading SYN characters (0=4 SYN, 1=8 SYN, 2=12 SYN, 3=16 SYN)

File: filename.NET.SYS

Go To  Go To  Update  Refresh  Prior
TRACEDAT PHONEDAT Data  Screen  Screen

```

Figure 7-6. BSC Link Data Screen

Fields

Logical device (HP modifiable.) Enter the logical device number of the INP card as configured in SYSDUMP.

Range: 1-999

Link Configuration

Connect timeout

(HP modifiable.) During link initialization, this value specifies the amount of time the INP will wait for a response from the remote station. If this time lapse is exceeded, it is assumed that the remote station is not responding.

Default Value: 900

Range: 60-900 seconds or 0

Number of error recovery retries

(HP modifiable.) The total number of times a block will be retransmitted due to the lack of an acknowledgement. If this number is exceeded, it is assumed that the remote station is not responding.

Default Value: 15

Range: 1-255

Clear to send delay

(HP modifiable.) User selectable. When initializing the link, this value specifies the amount of time the INP will wait for the DCE to raise Clear To Send (CTS) after raising Request To Send (RTS).

Default Value: 0 (Delay determined by modems)

Range: 0-20 tenths of a second

Data set ready delay

User selectable.

(HP modifiable.) This value specifies the time lapse allowed for DCE to raise Data Set Ready after the INP raises Data Terminal Ready (DTR).

Default Value: N

Buffer size

(HP modifiable.) Size, in bytes, of the buffers used to hold user data, plus layer 3 and layer 4 protocol headers. The size of the packets transmitted over the link is the buffer size plus the layer 2 header.

Default Value: 1500

Range: 32-1500

Number of Buffers

(HP modifiable.) This field specifies the number of buffers used to transfer blocks of data to and from the INP. The field specifies the number of buffers to be allocated on the HP 3000 not the INP.

Default Value: 12

Range: 10-50

Line speed

(HP modifiable.) This is the line-transmission speed in bits per second. It may be overridden by whichever device is providing clocking. The INP simply transmits using the provided clock source.

Default Value: 9600

Leading SYN characters (HP modifiable.) This field specifies the number of leading synchronization characters (SYN) that will precede each block transmission. These SYN characters are used by the receiving station to establish character-phase synchronization. If the receiving station is having difficulty establishing character phase synchronization, increasing the value of this field may help.

Default Value: 0

tracing is described in the "Commands" section (Section 1) of Volume II of this manual set. For information on formatting the link trace file, refer to the *Fundamental Data Communications Handbook*.

Fields

- Link trace enabled?** (HP modifiable.) Enter Y (YES) to enable link tracing, N (NO) otherwise. Can be overridden with the LINKCONTROL command. If you do enable link tracing, you are required to enter a trace file name. For best performance, do not enable tracing.
- Default Value:** N
- Trace ALL or ERRORS only** (HP modifiable.) Enter 1 (ALL) to trace all events, 0 (ERRORS) to trace errors only.
- Default Value:** 0
- Entries per record** (HP modifiable.) Enter the number of entries you want formatted per record.
- Default Value:** 24
- WRAP or DISCARD overflow?** (HP modifiable.) Enter 1 (WRAP) to overlay previous internal record entries with overflow trace entries, 0 (DISCARD) if you want it to discard the overflow.
- Default Value:** 0
- STN?** (HP modifiable.) Enter Y (YES) to record State Transitions (STNs), N (NO) otherwise. Hewlett-Packard use only.
- Default Value:** N
- OPR and EDT?** (HP modifiable.) Enter Y (YES) to record operand and editor entries, N (NO) otherwise.
- Default Value:** N
- RCT?** (HP modifiable.) Enter Y (YES) to record Receive Controls (RCTs) received on the line, N (NO) otherwise.
- Default Value:** Y
- RTX?** (HP modifiable.) Enter Y (YES) to record Receive Text (RTXs) received on the line, N (NO) otherwise.
- Default Value:** Y
- SCT?** (HP modifiable.) Enter Y (YES) to record Send Controls (SCTs) sent on the line, N (NO) otherwise.
- Default Value:** Y

Link Configuration

STX? (HP modifiable.) Enter Y (YES) to record Send Text (STXs) sent on the line, N (NO) otherwise.

Default Value: Y

ICD? (HP modifiable.) Enter Y (YES) to record Interconnect Driver Entries (ICDs), N (NO) otherwise. The ICD entry is for Hewlett-Packard use only.

Default Value: N

Trace File (HP modifiable.) Required if link trace is enabled. Name of the disc file in which you want to record tracing. Must be a valid MPE file name. Enter the filename in the format *filename.groupname.acctname*. The fully qualified file name can be as many as 26 characters. Lockwords are not allowed for trace files.

Do not specify the same file name with the NMMGR configuration as specified with the LINKCONTROL command.

Only one active trace is allowed per link. Refer to the *Fundamental Data Communications Handbook* for information on how to format the trace file.

LINK CONFIGURATION: BSC LINK PHONE DATA

The screen in Figure 7-8 is displayed when you press the function key for **Go To PHONEDAT** at the BSC Link Data Screen (Figure 7-6). It is also displayed when you type the path name:

```
@LINKCONF.linkname.PHONEDAT
```

in the command window of any screen and press **ENTER**, where *linkname* is the configured BSC link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NNNGR/3000 (X.05.06) LINK CONFIGURATION:      BSC LINK PHONE DATA      Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname.PHONEDAT

  [1] manual or autodial? (0=Manual, 1=Autodial)

File: filename.NET.SYS

Delete Data  Update Data  Refresh Screen  Prior Screen

```

Figure 7-8. BSC Link Phone Data Screen.

Fields

manual or autodial? (HP modifiable.) Enter 1 if you want the INP to automatically dial the phone number without intervention from the system operator. Enter 0 if you want the link manager to display the phone number on the console for the system operator to dial.

Default Value: 1

Link Configuration

Related Screens:

- **NETXPORT.NI.*niName*.MAPPING.*mapentry***
This Router Reachable Node screen is where you enter phone numbers of destination nodes.
- **NETXPORT.NI.*niName*.LINK.*nilink***
This Gateway Half Dial Link Configuration screen is where you enter phone numbers of destination nodes.

LINK CONFIGURATION: LAP-B LINK DATA

The screen in Figure 7-9 is displayed when you select a link name and the link type LAP-B at the Link Configuration Screen (Figure 7-1) and press **Add** or **Update**. It is also displayed when you type the path name:

@LINKCONF.*linkname*

in the command window of any screen and press **(ENTER)**, where *linkname* is the configured LAP-B link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data:** flag is set to **Y**.

```

NMNCR/3000 (X.05.06) LINK CONFIGURATION: LAP-B LINK DATA Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname

  Logical device      (1-999)
  900 Connect timeout  (60-900 seconds or 0)
  60  local timeout   (5-900 seconds or 0)
  300 LAP-B parameter T1 (5-3000 hundredths of a second)
  17  LAP-B parameter K - Maximum outstanding frames (1-7)
  20  LAP-B parameter N2 - retry count (1-255)
  0   Clear to send delay (0-20 tenths of a second)
  1024 Buffer size (32-1024 bytes)
  12  Number of buffers (10-50)
  11  Local mode (5=DTE, 6=DCE, 11=Point to Point)
  56000 Line speed in bits/second (1200,2400,4800,9600,19200,38400,56000)

File: filename.NET.SYS

Go To Go To Update Refresh Prior
TRACEDAT PHONEDAT Data Screen Screen

```

Figure 7-9. LAP-B Link Data Screen

Fields

Logical device (HP modifiable.) Enter the logical device number of the INP card as configured in SYSDUMP.

Default Value: N

Range: 1-999

Link Configuration

Connect timeout

(HP modifiable.) During link initialization, this value specifies the amount of time the INP will wait for a response from the remote station. If this time lapse is exceeded, it is assumed that the remote station is not responding.

Default Value: 900

Range: 60-900 seconds or 0

Local timeout

(HP modifiable.) Timer on the INP-to-HP 3000 communications path.

If the INP and the HP 3000 do not communicate during this time, LED 1 on the INP will flash, and the INP will no longer attempt to communicate.

Default Value: 60

Range: 5-900 seconds or 0

LAP-B parameter T1

(HP modifiable.) Response timeout in hundredths of a second. This is the maximum amount of time that the transmitter should wait for an acknowledgement before initiating a recovery procedure. This delay must account for 3 frame transmissions and 2 frame-processing delays. An approximation of this value is 3 seconds for line speeds greater than or equal to 9600 bits per second and 4 seconds for line speeds less than 9600 bits per second. The formula for the approximation in hundredths of a second is: $400 \times [(buffer\ size \times 8)/line\ speed]$. The configuration validation program will issue a warning if the set value does not comply to this specification.

Default Value: 300

Range: 5-3000

LAP-B parameter K

(HP modifiable.) This parameter specifies the maximum number of sequentially numbered frames that the configured node may have unacknowledged at any given time. This parameter is also called the Level 2 window size.

Default Value: 7

Range: 1-7

LAP-B parameter N2

(HP modifiable.) This field specifies the maximum number of times to retransmit a frame if the T1 timer expires. The recovery procedure mentioned in "LAP-B parameter T1" usually refers to the retransmission of the oldest unacknowledged frame. The value of N2 specifies the total number of times that the T1 timer expires and a frame is retransmitted in determining that the other side is not responding.

Default Value: 20

Range: 1-255

Clear to send delay

(HP modifiable.) User selectable. When initializing the link, this value

specifies the amount of time the INP will wait for the DCE to raise Clear To Send (CTS) after raising Request To Send (RTS).

Default Value: 0 (Delay determined by modems)

Range: 0-20 tenths of a second

Buffer size

(HP modifiable.) Size, in bytes, of the buffers used to hold user data, plus layer 3 and layer 4 protocol headers. The size of the packets transmitted over the link is the buffer size plus the layer 2 header.

Default Value: 1024

Range: 32-1024

Number of Buffers

(HP modifiable.) This field specifies the number of buffers used to transfer blocks of data to and from the INP. The field specifies the number of buffers to be allocated on the HP 3000 not the INP.

Default Value: 12

Range: 10-50

Local mode

(HP modifiable.) For HP Point-to-Point (all NS links) enter 11. If you are HP point-to-point, the other side must also be HP point-to-point. Enter 5 if the local station is acting as DTE, and enter 6 if the local station is acting as DCE. If you are DCE, the other side must be DTE. If you are DTE, the other side must be DCE. HP recommends using HP point-to-point because the system handles the designation for which side is DTE and DCE.

Default Value: 11

Range: Point-to-Point, DTE, or DCE

Line speed

(HP modifiable.) This is the line-transmission speed in bits per second. It may be overridden by whichever device is providing clocking. The INP simply transmits using the provided clock source.

Default Value: 5600

Range: 1200-5600

tracing is described in the "Commands" section (Section 1) of Volume II of this manual set. For information on formatting the link trace file, refer to the *Fundamental Data Communications Handbook*.

Fields

- Link trace enabled?** (HP modifiable.) Enter Y (YES) to enable link tracing, N (NO) otherwise. Can be overridden with the LINKCONTROL command. If you do enable link tracing, you are required to enter a trace file name. For best performance, do not enable tracing.
- Default Value:** N
- Trace ALL or ERRORS only** (HP modifiable.) Enter 1 (ALL) to trace all events, 0 (ERRORS) to trace errors only.
- Default Value:** 0
- Entries per record** (HP modifiable.) Enter the number of entries you want formatted per record.
- Default Value:** 24
- WRAP or DISCARD overflow?** (HP modifiable.) Enter 1 (WRAP) to overlay previous internal record entries with overflow trace entries, 0 (DISCARD) if you want it to discard the overflow.
- Default Value:** 0
- STN?** (HP modifiable.) Enter Y (YES) to record State Transitions (STNs), N (NO) otherwise. The STN entry is for Hewlett-Packard use only.
- Default Value:** N
- RCT?** (HP modifiable.) Enter Y (YES) to record Receive Controls (RCTs) received on the line, N (NO) otherwise.
- Default Value:** Y
- RTX?** (HP modifiable.) Enter Y (YES) to record Receive Text (RTXs) received on the line, N (NO) otherwise.
- Default Value:** Y
- SCT?** (HP modifiable.) Enter Y (YES) to record Send Controls (SCTs) sent on the line, N (NO) otherwise.
- Default Value:** Y
- STX?** (HP modifiable.) Enter Y (YES) to record Send Text (STXs) sent on the line, N (NO) otherwise.
- Default Value:** Y

Link Configuration

ICD?

(HP modifiable.) Enter Y (YES) to record Interconnect Driver Entries (ICDs), N (NO) otherwise. The ICD entry is for Hewlett-Packard use only.

Default Value: N

Trace File

(HP modifiable.) Required if link trace is enabled. Name of the disc file in which you want to record tracing. Must be a valid MPE file name. Enter the filename in the format *filename.groupname.acctname*. The fully qualified file name can be as many as 26 characters. Lockwords are not allowed for trace files.

Do not specify the same file name with the NMMGR configuration as specified with the LINKCONTROL command.

Only one active trace is allowed per link. Refer to the *Fundamental Data Communications Handbook* for information on how to format the trace file.

LINK CONFIGURATION: LAP-B LINK PHONE DATA

The screen in Figure 7-11 is displayed when you press the function key for **Go To PHONEDAT** at the LAP-B Link Data Screen (Figure 7-9). It is also displayed when you type the path name:

```
@LINKCONF.linkname.PHONEDAT
```

in the command window of any screen and press **(ENTER)**, where *linkname* is the configured LAP-B link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data:** flag is set to **X**.

```

NNMGR/3000 (X.05.06) LINK CONFIGURATION: LAPB LINK PHONE DATA Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname.PHONEDAT

 manual or autodial? (0=Manual, 1=Autodial)

File: filename.NET.SYS

Delete Update Refresh Prior
Data Data Screen Screen

```

Figure 7-11. LAP-B Link Phone Data Screen.

Fields

manual or autodial? (HP modifiable.) Enter 1 if you want the INP to automatically dial the phone number without intervention from the system operator. Enter 0 if you want the link manager to display the phone number on the console for the system operator to dial.

Default Value: 1

Related Screens:

- **NETXPORT.NI.*niName*.MAPPING.*mapentry***
This Router Reachable Node screen is where you enter phone numbers of destination nodes.

- **NETXPORT.NI.*niName*.LINK.*nilink***
This Gateway Half Dial Link Configuration screen is where you enter phone numbers of destination nodes.

LINK CONFIGURATION: ASNP LINK DATA

The screen in Figure 7-12 is displayed when you select a link name and the link type ATP/ASNP at the Link Configuration Screen (Figure 7-1) and press **Add** or **Update**. It is also displayed when you type the path name:

@LINKCONF.*linkname*

in the command window of any screen and press **ENTER**, where *linkname* is the configured ATP/ASNP link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NNMGR/3000 (X.05.06) LINK CONFIGURATION: ASNP LINK DATA      Data:N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname

[ ] Logical Device (1-999)
[ ] Subtype (0=Hardwired, 1=Modem, 2=European Modem)
[1200] Linespeed in bits/second (1200, 2400, 9600)
[0] Connect timeout (0-900 seconds)
[5] Maximum Outstanding Reads (1-32)
[5] Maximum Outstanding Writes (1-32)
[242] Buffer size in bytes (1-1024)
[20] Number of Buffers (2-128)

File: filename.NET.SYS

Go To   Go To   Update   Refresh   Prior
TRACEDAT PHONEDAT Data   Screen   Screen
  
```

Figure 7-12. ASNP Link Data Screen

Fields

Logical Device (HP modifiable.) Enter the logical device number of the link as configured in SYSDUMP.

Default Value: N

Range: 1-999

Link Configuration

- Subtype** (HP modifiable.) Enter the number shown on the screen that corresponds to your subtype.
- Default Value:** 1
- Linespeed** Must be a value supported by the modem.
- Default Value:** 1200
- Range:** 1200, 2400, 9600
- Connect timeout** (HP modifiable.) The number of seconds the operator has to dial the phone number of the remote node after the DTR signal goes on.
- Default Value:** 0
- Range:** 0-900
- Maximum Outstanding Reads** (HP modifiable.) Specifies the maximum number of reads that can be outstanding at any given time.
- Default Value:** 5
- Range:** 1-32
- Maximum Outstanding Writes** (HP modifiable.) Specifies the maximum number of writes that can be outstanding at any given time.
- Default Value:** 5
- Range:** 1-32
- Buffer size** (HP modifiable.) Size, in bytes, of the buffers used to hold user data, and layer 3 and layer 4 protocol headers. The size of the packets transmitted over the link is the buffer size plus the layer 2 header.
- For PC connections, use the default value of 242 bytes. For connections to other HP 3000s, the suggested value is 512 bytes. This configured buffer size should be the same as the buffer size configured for the remote HP 3000. You may choose to increase the buffer size for HP 3000 to HP 3000 connections if you are using high-quality lines.
- Default Value:** 242
- Range:** 1-1024
- Number of Buffers** (HP modifiable.) The maximum amount of incoming data that the link level can accept. Determines the total amount of space in virtual memory used for incoming data. The count is also dependent on the maximum outstanding reads. It should be equal to or greater than 2 times the amount of outstanding reads.
- Default Value:** 20
- Range:** 2-128

LINK CONFIGURATION: ASNP LINK TRACE DATA

The screen in Figure 7-13 is displayed when you press the function key for **Go To TRACEDAT** at the ASNP Link Data Screen (Figure 7-12). It is also displayed when you type the path name:

@LINKCONF.*linkname*.TRACEDAT

in the command window of any screen and press **ENTER**, where *linkname* is the configured ATP/ASNP link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NMMGR/3000 (X.05.06) LINK CONFIGURATION: ASNP LINK TRACE DATA      Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname.TRACEDAT

[N] Link trace enabled?          (Y/N)
[0] Trace ALL or ERRORS only? (ERRORS=0; ALL=1)
[0] WRAP or DISCARD overflow? (DISCARD=0; WRAP=1)
[Y] PRCT? (Y/N)  Receive Control Entries
[Y] PRTX? (Y/N)  Receive Text Entries
[Y] PSCT? (Y/N)  Send Control Entries
[Y] PSTX? (Y/N)  Send Text Entries
[N] ICD? (Y/N)   Internal Driver Entries

[ ] Trace File

File: filename.NET.SYS

Delete Data  Update Data  Refresh Screen  Prior Screen

```

Figure 7-13. ASNP Link Trace Data Screen.

After configuring link data, you can configure tracing for the link. The Link Trace Data Screen allows you to specify the events to trace and the name of the file for storing the tracing information. *For best performance, do not enable tracing.* You can override NMMGR activated link tracing by using the LINKCONTROL TRACE=OFF command. Using the LINKCONTROL command to enable and disable link tracing is described in the "Commands" section (Section 1) of Volume II of this manual set. For information on formatting the link trace file, refer to the *Fundamental Data Communications Handbook*.

Link Configuration

Fields

Link trace enabled? (HP modifiable.) Enter Y (YES) to enable link tracing, N (NO) otherwise. Can be overridden with the LINKCONTROL command. If you do enable link tracing, you are required to enter a trace file name. For best performance, do not enable tracing.

Default Value: N

Trace ALL or ERRORS only (HP modifiable.) Enter 1 (ALL) to trace all events, 0 (ERRORS) to trace errors only.

Default Value: 0

WRAP or DISCARD overflow? (HP modifiable.) Enter 1 (WRAP) to overlay previous internal record entries with overflow trace entries, 0 (DISCARD) if you want it to discard the overflow.

Default Value: 0

PRCT? (HP modifiable.) Enter Y (YES) to record Receive Controls (PRCTs) received on the line, N (NO) otherwise.

Default Value: Y

PRTX? (HP modifiable.) Enter Y (YES) to record Receive Text (PRTXs) received on the line, N (NO) otherwise.

Default Value: Y

PSCT? (HP modifiable.) Enter Y (YES) to record Send Controls (PSCTs) sent on the line, N (NO) otherwise.

Default Value: Y

PSTX? (HP modifiable.) Enter Y (YES) to record Send Text (PSTXs) sent on the line, N (NO) otherwise.

Default Value: Y

ICD? (HP modifiable.) Enter Y (YES) to record Interconnect Driver Entries (ICDs), N (NO) otherwise.

Default Value: N

Trace File (HP modifiable.) Required if link trace is enabled. Name of the disc file in which you want to record tracing. Must be a valid MPE file name. Enter the filename in the format *filename.groupname.acctname*. The fully qualified file name can be as many as 26 characters. Lockwords are not allowed for trace files.

Do not specify the same file name with the NMMGR configuration as specified with the LINKCONTROL command.

Only one active trace is allowed per link. Refer to the *Fundamental Data Communications Handbook* for information on how to format the trace file.

LINK CONFIGURATION: ASNP LINK PHONE DATA

The screen in Figure 7-14 is displayed when you press the function key for **Go To PHONEDAT** at the ASNP Link Data Screen (Figure 7-12). It is also displayed when you type the path name:

`@LINKCONF.Linkname.PHONEDAT`

in the command window of any screen and press **ENTER**, where *linkname* is the configured ATP/ASNP link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. This is necessary if you are planning to use either the direct dial or shared dial link. Verify that the data record has been created by checking that the **Data:** flag is set to **Y**.

```
NMMGR/3000 (X.05.06) LINK CONFIGURATION: ASNP LINK PHONE DATA Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: LINKCONF.linkname.PHONEDAT

[1] manual or autodial? (0=Manual, 1=Autodial)

File: filename.NET.SYS

Delete Update Refresh Prior
Data Data Screen Screen
```

Figure 7-14. ASNP Link Phone Data Screen.

Fields

manual or autodial? (HP modifiable.) Display only. This field is currently always set to 1; hence no messages for the system operator will appear on the console for manual dial. For RASP, dial manually *after* the network comes up.

Default Value: 1

This section contains information about the NMMGR configuration screens that are common to all network interface types. The network transport configuration branch of NMMGR begins with a screen called the NETWORK TRANSPORT CONFIGURATION SELECTION screens. This screen, and those to which it leads, are listed and described below. The level of indentation shown in the following list indicates the place held by each screen in the configuration tree.

NETWORK TRANSPORT CONFIGURATION SELECTION - This screen presents a selection of four configuration branches: for configuration of nodal identity information, global transport information, general protocols (TCP, PXP, and IP Update protocols), and configuration of network interfaces.

NODE CONFIGURATION - This screen, which you will reach by pressing **Go To Node** on the NETWORK TRANSPORT CONFIGURATION SELECTION screen, requires you to press a function key to proceed to the next screen

NODE NAME CONFIGURATION - This screen allows you to enter the node name of the node being configured.

GLOBAL TRANSPORT CONFIGURATION - This screen, which you reach by pressing **Go To GLOBAL** on the NETWORK TRANSPORT CONFIGURATION SELECTION screen, allows you to enter information used for transferring data between nodes. For example, it enables you to specify and prioritize the methods used to resolve names and IP addresses, the name of a home network (needed only if this node is used as a gateway half), and the maximum number of nodes expected to be communicating concurrently with the node you are configuring.

GENERAL PROTOCOL CONFIGURATION - This screen allows you to specify which of three protocols to configure next: IPU (IP Update), PXP, or TCP.

IP UPDATE CONFIGURATION - Information entered on this screen specifies the upper limit of memory that will be reserved for the IPU module, which creates and maintains internet routing tables for this node.

PACKET EXCHANGE (PXP) CONFIGURATION - This screen allows you to configure information needed by the PXP protocol running on this node.

TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION - This screen allows you to configure information used by the TCP protocol running on this node.

NETWORK INTERFACE CONFIGURATION - This screen, which you will reach by pressing **Go To NI** on the NETWORK TRANSPORT CONFIGURATION SELECTION screen, allows you to specify a network interface name and its type for each of the node's network interfaces. Each time you specify an interface, NMMGR allows you to proceed through the series of configuration screens necessary for configuring the specified interface type. The configuration screens for each type are described in Sections 9, 10, 11, and 12 of this manual.

The network transport must be configured in the configuration file that is also used for the link configuration. This configuration file must be located in the NET group of the SYS account. The recommended file name for the actual configuration file that contains the link and network transport configurations is NSCONF.NET.SYS. If you use a different filename, you need to specify the filename with the CONF keyword when you use the NETCONTROL START command to initiate a network

Network Transport Configuration

connection. A description of the NETCONTROL command is contained in Section 1, Volume II of this manual.

To reach the network transport configuration screens, follow these steps:

- Issue the run command for NMMGR; the Open Configuration/Directory File Screen is displayed.
- Enter the name of the configuration file to be created or updated in the Configuration File Name field.
- Press the appropriate function key (Open Config or Create Config); the Main Menu Screen is displayed.
- Press the function key for Go To CONFIG; the Configuration Menu Screen is displayed.
- Press the function key for Go To NETXPORT; the Network Transport Configuration Selection Screen is displayed.

For more general information on NMMGR, refer to "Getting Started with NMMGR" in Section 5.

NOTE

Configurable fields described in this manual are required unless otherwise stated.

Fields described as "HP modifiable" should be changed only upon the recommendation of your HP representative.

On the screens shown in this section, fields that must be configured when performing guided configuration are underlined.

NETWORK TRANSPORT CONFIGURATION SELECTION

The menu screen shown in Figure 8-1 is displayed when you press the function key for **Go To NETXPORT** at the Configuration Menu Screen. It is also displayed when you type the path name:

@NETXPORT

in the command window of any screen and press **ENTER**.

From this screen you proceed to the screens used to configure the network transport.

```

NNMGR/3000 (X.05.06) NETWORK TRANSPORT CONFIGURATION SELECTION
Select the next screen and press the corresponding function key.
Command:

Path:  NETXPORT

NODE   -  Configure Nodal Identity Information
GLOBAL -  Configure Global Transport Information
GPROT  -  Configure General Protocols (TCP,PXP,IPU)
NI     -  Configure Network Interfaces

NOTE:  Be certain to use "NETXPORT UPDATE" to reconfigure an active network.
       Type "NIUPDATE" in the command window and press enter to use this
       Guided Configuration feature.

File:  filename.NET.SYS

Go To  Go To  Go To  Go To
NODE   GLOBAL GPROT  NI
Refresh Prior
Screen Screen
    
```

Figure 8-1. Network Transport Configuration Selection Screen

Choose the item you wish to configure and press the corresponding function key.

NODE CONFIGURATION

The menu screen shown in Figure 8-2 is displayed when you press the function key for **Go To NODE** at the Network Transport Configuration Selection Screen (Figure 8-1). It is also displayed when you type the path name:

@NETXPORT.NODE

in the command window of any screen and press **ENTER**.

From this screen press **Go to Name** to proceed to the screen used to configure a unique name for this node.

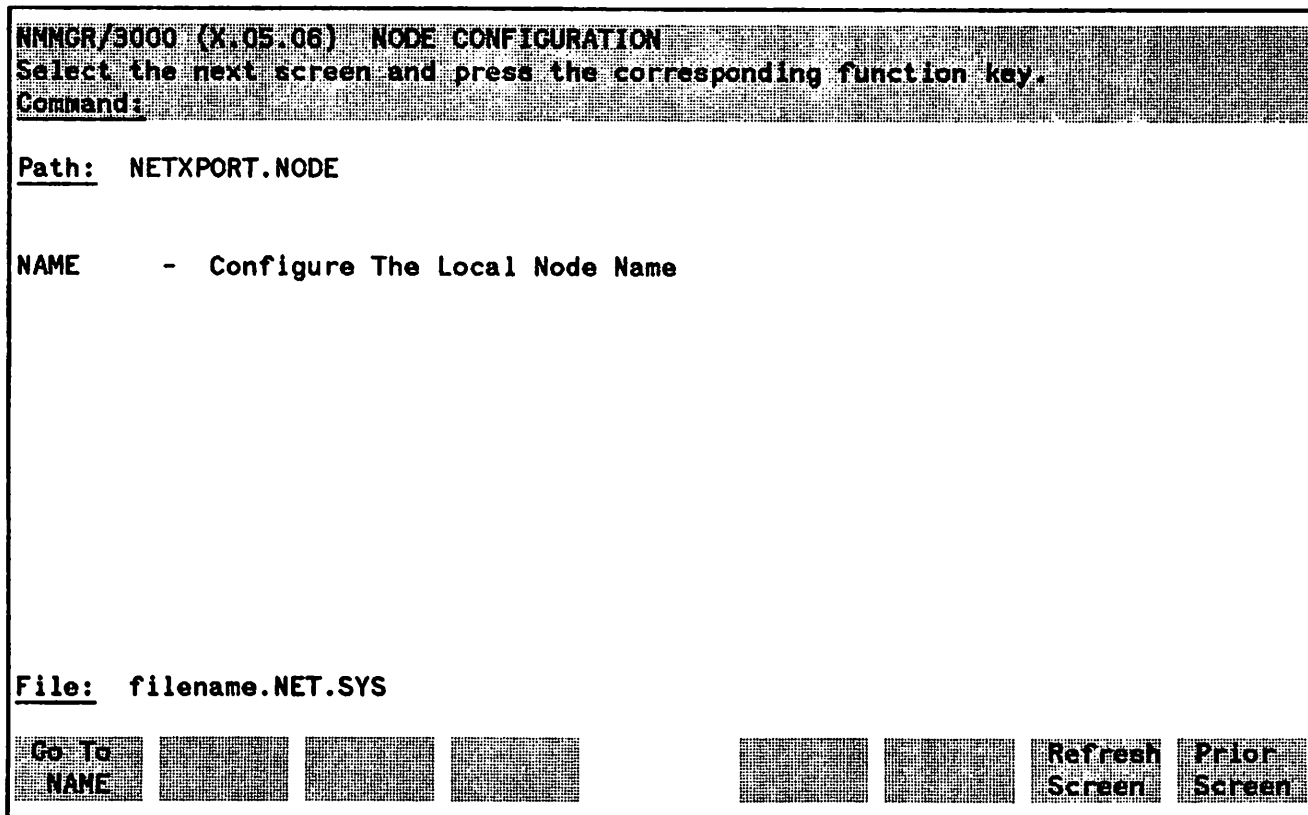


Figure 8-2. Node Configuration Screen

NODE NAME CONFIGURATION

The screen in Figure 8-3 is displayed when you press the function key for **Go To NAME** at the Node Configuration Screen (Figure 8-2). It is also displayed when you type the path name:

```
@NETXPORT.NODE.NAME
```

in the command window of any screen and press **ENTER**.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

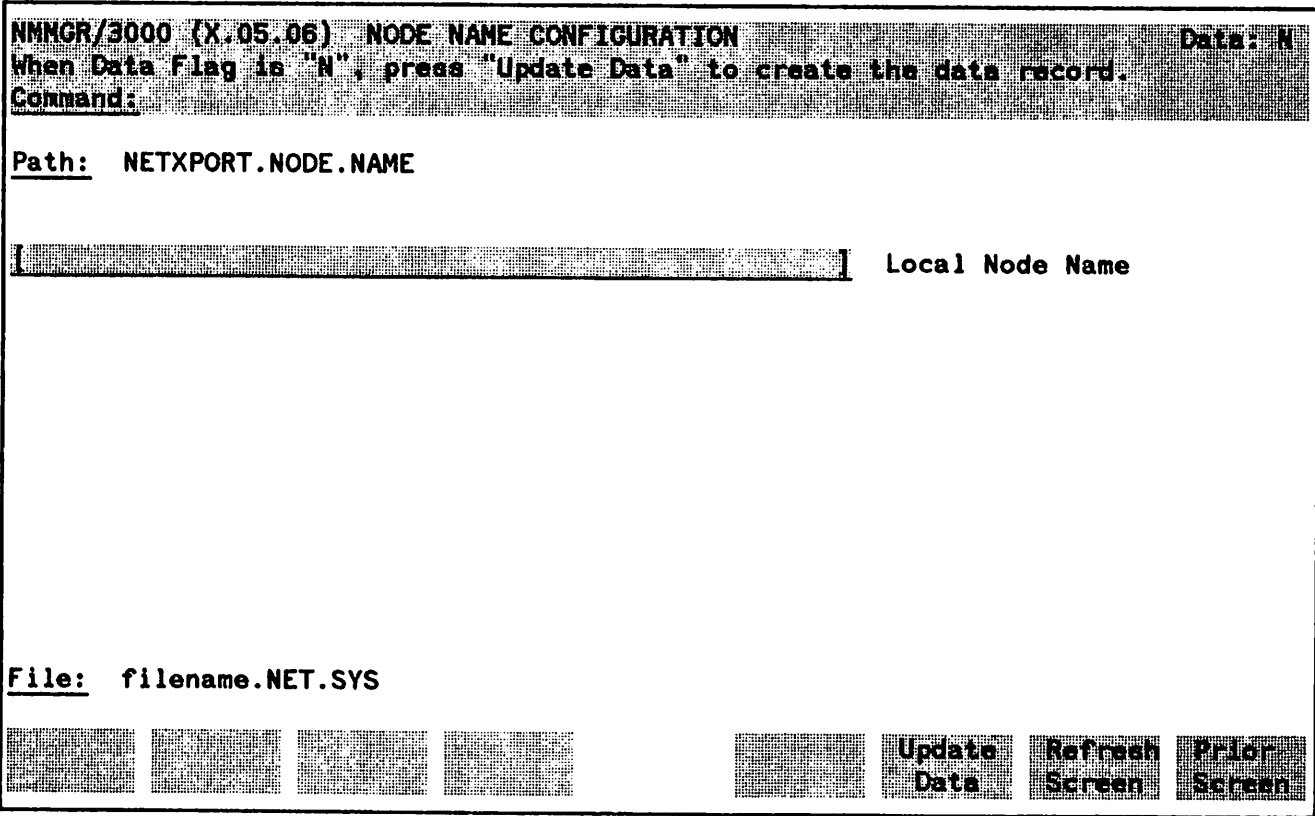


Figure 8-3. Node Name Configuration Screen.

Fields

Local Node Name

The format of a node name is *name.domain.organization* where the total number of characters is 50 or fewer, and each field can contain as many as 16 characters (alphanumeric, underscore or hyphens). The first character of each field must be alphabetic.

The *name* portion of each node name must be unique within the node's network, and the *name.domain* portion of each node name must be unique within the catenet.

HP recommends that all nodes on the same network be assigned the same *domain* and *organization*. You should assign meaningful names. For example, MKTG.LAN1.HP and LAB.LAN1.HP would be reasonable names for two nodes on the same Local Area Network at Hewlett Packard. One node in this example would be used by a marketing department, and one node would be used by a lab. The *organization* fields in this example are the same because the nodes belong to the same catenet. Refer to Section 3, Volume 1 for more information about node names.

GLOBAL TRANSPORT CONFIGURATION

The screen in Figure 8-4 is displayed when you press the function key for **Go To GLOBAL** at the Network Transport Configuration Selection Screen (Figure 8-1). It is also displayed when you type the path name:

@NETXPORT.GLOBAL

in the command window of any screen and press **ENTER**.

The purpose of this data-entry screen is to enter information that is used for transferring information between nodes.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NNMGR/3000 (X.05.06) GLOBAL TRANSPORT CONFIGURATION          Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: NETXPORT.GLOBAL

[ ] Home Network Name

[2][3][1] Name Search Methods And Order

      1 - Network Directory      3 - Probe Proxy
      2 - Probe                  0 - Choice Omitted

[100] Maximum Directly Connected Nodes
[100] Maximum Outbound Destinations
[100] Maximum Inbound Destinations

File: filename.NET.SYS

[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
Update Data Refresh Screen Prior Screen
  
```

Figure 8-4. Global Transport Configuration Screen

Fields

Home Network Name Leave this field blank if there are no gateway-half NIs configured for this node. Otherwise, enter the name of a configured LAN802.3 NI or router NI.

The Home Network Name is required when configuring a gateway half to determine the source IP address for packets originating from the node over the gateway half Link. The source IP address that will be used will be the one configured for the Home Network IP protocol.

The name you enter in this field should give the greatest number of destination networks a short return path to this node.

Related Screens:

- NETXPORT.NI
- NI names configured here

Name Search Methods and Order

The Name Search Methods and Order field is used to select the method and relative order by which node names (specified in the DSLINE command and the NetIPC IPCCConnect intrinsic) will be resolved into transport addressing information. This addressing information is contained in a structure called a path report.

The path report for a particular node name may be retrieved by one of three methods: the Network Directory, the Probe Protocol or the Probe Protocol Proxy. Refer to section 3 for information about these methods.

Configurable values are:

- 1 = Network Directory
- 2 = Probe
- 3 = Probe Proxy
- 0 = Choice Omitted

Default Value: 2,3,1 Probe, Probe Proxy, Network Directory)

Range: 0-3

Maximum Directly Connected Nodes

This field controls the allocation of data structures needed to communicate with nodes directly connected to this node. A node is directly connected when it is a member of the same network(s) as the local node. This field need only reflect the maximum number of directly connected nodes that will be communicated with simultaneously. If this node can communicate to all other nodes in the network simultaneously, the maximum number can be computed as follows:

Type Of NI	# Directly Connected Nodes
-----	-----
Loopback	1
Gateway Half	1
LAN	Maximum Number Of Nodes In Network (Taken From LAN802.3 NETWORK INTERFACE CONFIGURATION SCREEN)
ROUTER	Maximum Number Of Links Configured under the NI

To the above computation an additional amount should be added. This amount is computed as follows:

$$10 + (10 * \text{each configured NI})$$

This field should be configured relatively large and reviewed whenever the network(s) of which this node is a member expands.

Related Screens:

- NETXPORT.NI.lan
Maximum nodes in network
- NETXPORT.NI.router.LINK
Number of links configured

Default Value: 100

Range: 1-1024

**Maximum Outbound
Destinations**

This is the maximum number of nodes that this node expects to be communicating with concurrently, with this node initiating communication. It includes both directly and non-directly connected nodes.

This field should be configured relatively large to allow for future communication expansion. Note that changes to this field will not take effect until the operating system is restarted.

Default Value: 100

Range: 2-400

**Maximum Inbound
Destinations**

This is the maximum number of nodes that this node expects to be communicating with concurrently, with the other nodes initiating communication. It includes both directly and non-directly connected nodes.

This field should be configured relatively large to allow for future communication expansion. Note that changes to this field will not take effect until the operating system is restarted.

Default Value: 100

Range: 2-600

GENERAL PROTOCOL CONFIGURATION

The menu screen in Figure 8-5 is displayed when you press the function key for **Go To GPROT** at the Network Transport Configuration Selection Screen (Figure 8-1). It is also displayed when you type the path name:

@NETXPORT.GPROT

in the command window of any screen and press **ENTER**.

From this screen you proceed to the screens used to configure the general protocols of the network transport. All three general protocols must be configured for each node.

```
MMGR/3000 (X.05.06) GENERAL PROTOCOL CONFIGURATION
Select the next screen and press the corresponding function key.
Command:

Path: NETXPORT.GPROT

IPU      -  Configure IP Update Protocol
PXP      -  Configure Packet Exchange Protocol
TCP      -  Configure Transmission Control Protocol

File: filename.NET.SYS

Go To    Go To    Go To
IPU      PXP      TCP
Refresh  Prior
Screen   Screen
```

Figure 8-5. General Protocol Configuration Screen

Choose the protocol you wish to configure and press the corresponding function key.

INTERNET PROTOCOL (IP) UPDATE CONFIGURATION

The screen in Figure 8-6 is displayed when you press the function key for **Go To IPU** at the General Protocol Configuration Screen (Figure 8-5). It is also displayed when you type the path name:

@NETXPORT.GPROT.IPU

in the command window of any screen and press **ENTER**.

This screen is used to supply information to the IPU module. The IPU module is responsible for the creation and maintenance of the IP internet routing tables which are used to establish connectivity to remote networks through local network gateways. The information supplied by this screen is required to put a limit on the memory to be reserved for these tables.

Reserved routing table space is based on the product of the two values configured on this screen.

NOTE

Note that if both maximum values are configured, the space required would exceed internal memory limitations. The product of the two values should not exceed 2000.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

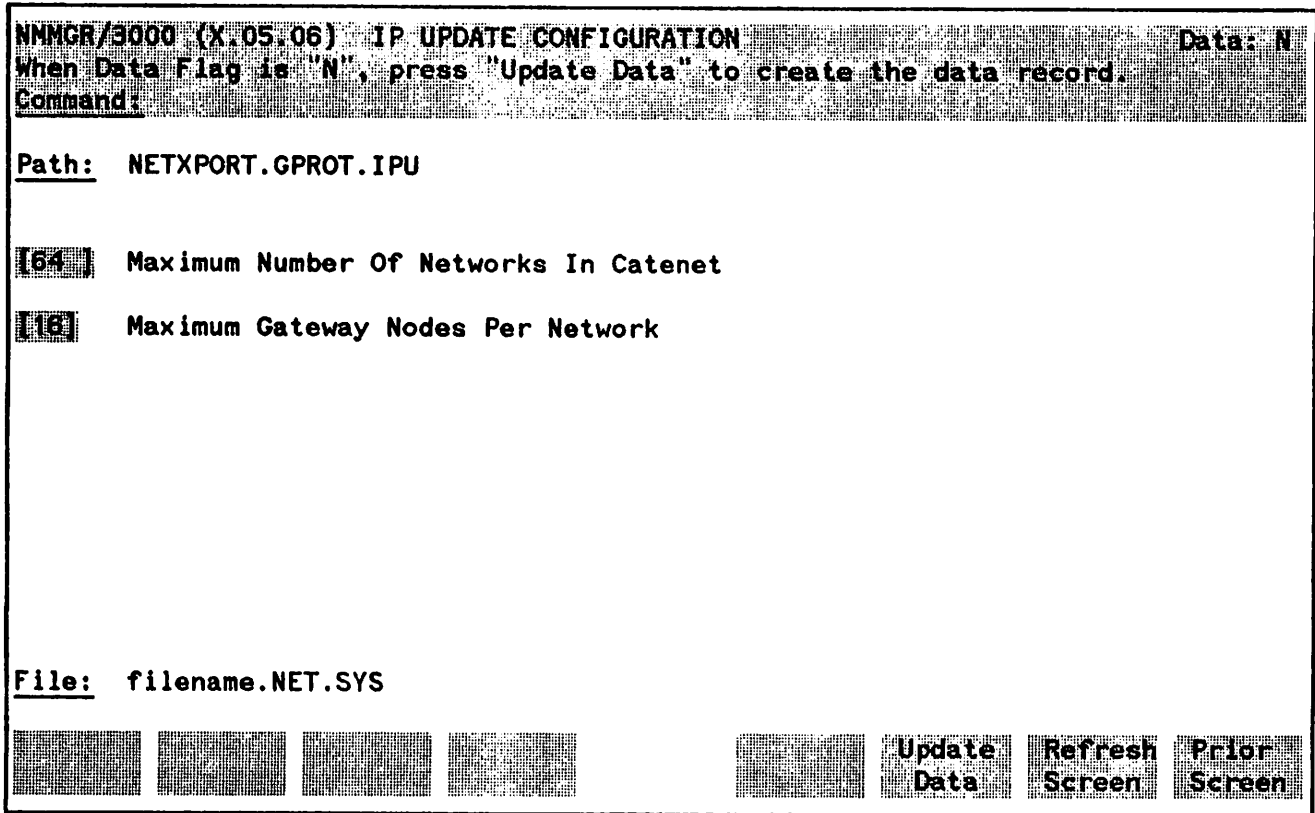


Figure 8-6. IP Update Configuration Screen

Fields

Maximum Number Of Networks in Catenet

This is the maximum number of networks that the catenet might be expected to contain. The number is used to allocate routing table space. Note that networks can be added dynamically (by using the NETCONTROL UPDATE command) but allocated table space cannot be altered without stopping the entire transport. It is wise, then, to anticipate growth when configuring this value to minimize the need to take down the transport to reconfigure the size of the internet tables.

If more networks are added (via NETCONTROL UPDATE) than there is space allocated for, a log message will indicate that adding the network would have exceeded the allocated space and that the IPU module ignored the update. Consult the *NS3000/V Error Message and Recovery Manual* for the specific IP log message in question.

Default Value: 64

Range: 1-256

Related Screens:

- NETXPORT.NI.*niName*.INTERNET.*gatewayn*

This field specifies networks reachable through a particular gateway. If more reachable networks are configured than Maximum Networks, configuration validation will fail.

**Maximum Gateway
Nodes Per Network**

This is the maximum number of gateways that there might be on any network that the node is directly connected to. The number is used, together with Maximum Networks above, to allocate routing table space. Note that gateways can be added dynamically (by using the NETCONTROL UPDATE command) but allocated table space cannot be altered without stopping the entire transport. As with Maximum Networks above, it is wise to anticipate growth when configuring this value to minimize the need to take down the transport to reconfigure the size of the internet tables.

Default Value: 16

Range: 0-64

If more gateways are added (by using the NETCONTROL UPDATE command) than there is space allocated for, a log message will indicate that adding the gateway would have exceeded the allocated space and that the IPU module ignored the UPDATE. Consult the *NS3000/V Error Message and Recovery Manual* for the specific IP log message in question.

PACKET EXCHANGE PROTOCOL (PXP) CONFIGURATION

The screen in Figure 8-7 is displayed when you press the function key for **Go To PXP** at the General Protocol Configuration Screen (Figure 8-5). It is also displayed when you type the path name:

@NETXPORT.GPROT.PXP

in the command window of any screen and press **ENTER**.

This screen contains the information necessary to configure Packet Exchange Protocol (PXP) for the node.

This screen provides the necessary information for the operation of the PXP protocol. The information configured falls into two categories:

- Reliability (checksum field)
- Performance parameters (retransmission fields)

NOTE

This protocol must be configured in order for the network transport to function.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NNMGR/3000 (X.05.06) PACKET EXCHANGE PROTOCOL (PXP) CONFIGURATION      Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: NETXPORT.GPROT.PXP

[N]      Checksum Enabled      (Y for YES, N for NO)

[10]    Retransmission Interval (Secs)

[4]     Maximum Retransmissions Per Request

File: filename.NET.SYS

[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
Update Data Refresh Screen Prior Screen
    
```

Figure 8-7. Packet Exchange Protocol Configuration Screen

Fields

Checksum Enabled

(HP modifiable). Checksumming is a method of error checking. PXP checksumming causes significant overhead, and is not normally needed for this protocol. Also, error checking is provided for at the link level. For these reasons, HP recommends the default value (N) for this field so that checksumming will be disabled for this protocol.

Default Value: N

Retransmission Interval (Secs)

The time in seconds to wait for a reply from a remote node before retransmitting a request. In general, the value to configure should reflect the load on the local system, the remote system, and the networks through which the request and the reply must travel.

If the value is set too low, needless retransmissions may occur, or IPCLOOKUP calls may fail. If the value is set too high, an unnecessarily long delay will occur when a packet is lost and a retransmission is necessary.

Frequent log messages indicating that retransmissions are taking place or that requests are failing indicates that the value needs to be increased.

Default Value: 10

Range: 1-600

**Maximum
Retransmissions
Per Request**

This is the number of times that PXP will retransmit a request when a reply has not been received within the retransmission interval (explained above).

As in the discussion of Retransmission Interval above, this field is a tuning parameter. The two values work together to determine the maximum time that a PXP user will wait for a reply.

This maximum reply time is calculated as follows:

$$\text{RTXinterval} + (\text{RTXinterval} * \text{MAXRTX})$$

where:

RTXinterval is the configured retransmission interval and MAXRTX is the configured maximum retransmissions per packet.

Default Value: 4

Range: 1-100

TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION

The screen in Figure 8-8 is displayed when you press the function key for **Go To TCP** at the **General Protocol Configuration Screen** (Figure 8-5). It is also displayed when you type the path name:

@NETXPORT.GPROT.TCP

in the command window of any screen and press **ENTER**.

This screen contains the information necessary to configure Transmission Control Protocol (TCP) for the node.

NOTE

This protocol is required in order for the network transport to function.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

This screen provides the necessary information for the operation of the TCP protocol. The information configured falls into three categories:

- Reliability (Checksum field)
- Sizing parameters (Maximum connections fields)
- Performance parameters (Retransmission fields)

The TCP retransmission algorithm is as follows. Per connection, TCP calculates the average packet acknowledgement delay. It then doubles this time for use as the retransmission timer. For each time that a particular packet must be retransmitted, the timer set is increased again by the amount of the delay. For example, should the remote side of an active connection with a calculated delay of 1 second fail, the retransmission of an outstanding packet would be at intervals of 2, 4, 6, and 8 seconds. A final timer of 10 seconds will be set to wait for the fourth retransmission, bringing the total interval to 30 seconds.

The various configuration retransmission fields work together to establish the initial, minimum and maximum values for the retransmission timers, and the number of retransmissions that are to be performed before a connection is broken. If the values are set too low, needless retransmissions may occur, or connections may be prematurely aborted. If the values are set too high, an unnecessarily long delay will occur when a packet is lost, and a retransmission will be necessary. All of these retransmission fields are configurable to optimize connection performance. Values to be entered for the retransmission fields should, in general, reflect the average load on system resources at the local node, the remote node, and the intervening network(s), if any. The optimal values for these fields can be determined only by experience for each node.

```

NNMGR/3000 (X.05.06) TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: NETXPORT.GPROT.TCP

[N] Checksum Enabled (Y For YES, N For NO)
[128] Maximum Number Of Connections
[4] Retransmission Interval Lower Bound (Secs)
[120] Retransmission Interval Upper Bound (Secs)
[4] Initial Retransmission Interval (Secs)
[4] Maximum Retransmissions Per Packet

[600] Connection Assurance Interval (Secs)
[3] Maximum Connection Assurance Retransmissions

File: filename.NET.SYS

Update Refresh Prior
Data Screen Screen
    
```

Figure 8-8. Transmission Control Protocol Configuration Screen

Fields

Checksum Enabled

Checksumming is a method of error checking. TCP checksumming causes significant overhead, and is not normally needed for this protocol. Also, error checking is provided for at the link level. For these reasons, HP recommends the default value (N) for this field so that checksumming will be disabled for this protocol.

The checksum decision for a given connection is determined from several sources: 1) The destination path report, 2) the local configuration (as specified in this screen) and 3) the values specified in the NetIPC intrinsic, IPCCONNECT and IPCREVCN. Should any of these sources indicate checksumming enabled, the connection will be checksummed.

Note then, that the effect of disabling checksum in the configuration is not to prohibit checksumming, but to simply allow each connection to choose for itself. The NS Services specify checksumming disabled in their NetIPC calls thereby allowing control to be taken through the configuration and network directory. Therefore, TCP checksumming for NS Services must be specified in the TCP Configuration screen (via the checksum enabled field), or within the network directory.

Default Value: N

Range: Y or N

Maximum Number of Connections

All TCP communication occurs over connections. Each connection functions as a separate entity in regard to destination, flow control and retransmissions. There is a one-to-one correspondence between TCP connections and NetIPC calls to IPCCONNECT, and therefore between each NS Service invoked by each user. There is no multiplexing of user or NS Services data over shared connections.

The number of connections configured should reflect an estimation of the number of NS Services and NetIPC users that will be active simultaneously. This includes both outbound and inbound connections. The field should be configured relatively large to accommodate expansion.

Note that the allocation of buffers is related to the number of TCP connections. Should this field be modified, the NI screens controlling buffer allocation (NETXPORT.NI.*niName*.) must be updated.

Default Value: 128

Range: 1-1024

Retransmission Interval Lower Bound (Secs) The retransmission interval is the time in seconds that a TCP connection will wait for a reply from a remote node before retransmitting a packet. The retransmission interval is dynamically adjusted by TCP for each connection, depending on a number of factors. This field sets the lower bound for the readjustment.

A general discussion of retransmissions is provided in the overall description of this screen above.

Default Value: 4

Range: 2-600

Retransmission Interval Upper Bound (Secs) The retransmission interval is dynamically adjusted by TCP for each connection, depending on a number of factors. This field sets the upper bound for the readjustment.

A general discussion of retransmissions is provided in the overall description of this screen above.

Default Value: 120

Range: 2-600

Initial Retransmission Interval (Secs) This field sets the initial amount of time that TCP will wait for a reply from a remote node before attempting to retransmit a packet. This value is used for connection setup when the retransmission interval has not yet been calculated. It must be in the range of the lower and upper bound. The default of 4 with the default Maximum Retransmissions Per Packet of 4 will cause TCP to wait a total of 60 seconds when attempting a connection to a non-responding system.

A general discussion of retransmissions is provided in the overall description of this screen above.

Default Value: 4

Range: 2-600

**Maximum
Retransmissions
Per Packet**

This is the maximum number of times that TCP will retransmit a packet before aborting the connection. Together with the Lower and Upper Bound configuration, and the dynamically calculated delay, it controls the total time interval TCP will wait before aborting a non-responding connection.

Default Value: 4

Range: 1-100

**Connection Assurance
Interval (Secs)**

(HP modifiable.) The TCP protocol guarantees the integrity of connections so long as they are actively in use through the use of TCP's retransmission timer. However, guaranteeing the integrity of idle connections requires that TCP exchange protocol packets at some timed interval. This field allows the configuration of the interval at which these connection assurance packets will be exchanged.

Default Value: 600

Range: 1-600

**Maximum Connection
Assurance
Retransmissions**

(HP modifiable.) This is the maximum number of times that TCP will transmit a connection assurance packet to a non-responding remote system. Together with the Connection Assurance Interval, this field defines the time it will take for an idle connection to abort if the remote TCP fails to respond. Unlike the retransmission timer, a backoff algorithm is not used. Therefore, the timeout period is calculated as follows:

CAinterval + (CAinterval * MAXCARTX)

Default Value: 3

Range: 1-100

NETWORK INTERFACE CONFIGURATION

The select screen in Figure 8-9 is displayed when you press the function key for **Go To NI** at the Network Transport Configuration Selection Screen (Figure 8-1). It is also displayed when you type the path name:

@NETXPORT.NI

in the command window of any screen and press **ENTER**.

Use the fields and the function keys of the select screen to perform the desired action.

- To define a new NI configuration, specify the NI name and the NI type; then press **Add**. The path for the selected NI name is added to the configuration file, and the data screen on that path is displayed.
- To modify an existing NI configuration, specify the NI name; then press **Update**. The data screen on the path for the specified NI name is displayed.
- To change the name of an existing NI configuration, specify the NI name and a new name; then press **Rename**. The previously configured NI name is replaced and the screen displays the new name in a display field under the label Configured Network Interfaces.
- To delete an existing NI configuration, specify the NI name; then press **Delete**. Press **Delete** again to confirm the deletion. If you do not press **Delete** a second time, the deletion will not occur. The previously configured NI name is deleted and is no longer displayed in a display field under the label Configured Network Interfaces.

The network interface is responsible for providing the interface between network transport protocols and link protocols. It also provides the software loopback capability.


```

NNMGR/3000 (X.05.06) NETWORK INTERFACE CONFIGURATION
Type in name of item to Update, Delete, or Rename; or Add a new item
Command:

Path: NETXPORT.NI

Network Interface Name [ ] Type : LOOP,LAN802.3,
New Name [ ] ROUTER,GATEHALF
(if new)

Configured Network Interfaces

Name Type Name Type Name Type
[ ] [ ] [ ] [ ] [ ] [ ]

File: filename.NET.SYS

Next Prev Delete Rename Add Update Refresh Prior
Page Page Screen Screen Screen Screen
    
```

Figure 8-9. Network Interface Configuration Screen

Fields

Network Interface Name

Select the network interface name for one of the following: 1) software loopback capability, 2) LAN802.3 network connection, 3) router network or 4) gateway half.

The Network Interface Name can contain as many as eight alphanumeric characters; first character must be alphabetic.

Type (LOOP, LAN802.3, ROUTER, or GATEHALF)

(Required only when adding.) Enter the appropriate type:

LOOP to identify the software loopback capability.

LAN802.3 to identify the LAN802.3 network connection.

ROUTER to identify a router network.

GATEHALF to identify a gateway half.

New Name

(Required only when renaming.) Enter a new NI name. The new name can contain as many as eight alphanumeric characters, and the first character must be alphabetic. You need to specify a new name only when renaming an existing NI.

LAN802.3 NETWORK INTERFACE CONFIGURATION

SECTION

9

The screens described in this section are used for configuring a node with a LAN802.3 network interface. All IEEE 802.3 networks must have a LAN802.3 network interface configured for each node. This includes nodes using ThinLAN/3000 Links (including ThickLAN) and StarLAN/3000 Links. Configuration of the LAN802.3 network interface branch of NMMGR begins with the LAN802.3 NETWORK INTERFACE CONFIGURATION screen. From this screen, you can proceed to a number of other screens needed to complete network interface configuration. The screens are listed and briefly described below, with the level of indentation shown indicating each screen's place in the configuration hierarchy.

LAN802.3 NETWORK INTERFACE CONFIGURATION - This screen allows you to configure items needed for any IEEE 802.3 network interface: numbers of buffers, the maximum number of nodes in the network, an address used by the Probe protocol, and whether to load IP to IEEE 802.3 address information from the node's network directory. From this screen, you can choose to go to one of four screens that begin lower branches of configuration.

PROTOCOL CONFIGURATION - This screen, which you reach by pressing **Go To PROTOCOL** on the previous screen, allows you to proceed to configure the IP or Probe protocols.

IP PROTOCOL CONFIGURATION - This screen enables you to enter information needed for the operation of the IP protocol on this node.

PROBE PROTOCOL CONFIGURATION - This screen enables you to enter information needed for the operation of the Probe protocol on this node.

NETWORK INTERFACE LINKS - This screen, which is displayed after you press **Go To LINK** on the LAN802.3 NETWORK INTERFACE CONFIGURATION screen, allows you to specify a link name (as configured in the link configuration branch of NMMGR), and to specify that it is of type LAN (used for all IEEE 802.3 links).

LAN LINK CONFIGURATION - This screen contains default values for the LAN link defined in the previous screen that cannot be changed.

NEIGHBOR GATEWAYS - This screen appears after you press **Go To INTERNET** on the LAN802.3 NETWORK INTERFACE CONFIGURATION screen. It begins the branch of LAN802.3 network interface configuration that allows you to configure internet information. In this screen, you can identify the nodes in the network that will be functioning as gateways to other networks. **Note:** Internet configuration is not needed if this network is not connected to any other networks, or if its nodes are connected to other personal computers only, and not to other HP 3000s or other computers that perform internet routing.

NEIGHBOR GATEWAY REACHABLE NETWORKS - You must configure an instance of this screen for each of the gateways identified in the previous screen. In this screen, you will specify information about each of the networks that can be reached by a particular gateway.

LAN802.3 MAPPING CONFIGURATION - This screen, which you will reach by pressing **Go To MAPPING** on the LAN802.3 NETWORK INTERFACE CONFIGURATION screen, begins a branch of configuration that enables you to provide information about a non-HP computer's addresses. For HP computers, this information is provided by the Probe protocol, and

LAN802.3 Network Interface Configuration

configuration of this and the subsequent screen in this branch is unnecessary. In this screen, you will identify the non-HP node.

STATIC NEIGHBOR NODE CONFIGURATION (LAN802.3) - An instance of this screen must be configured for every non-HP node identified on the previous screen. You will configure a node's IP and IEEE 802.3 addresses here.

NOTE

Configurable fields described in this manual are required unless otherwise stated.

Fields described as "HP modifiable" should be changed only upon the recommendation of your HP representative.

On the screens shown in this section, fields that must be configured when performing guided configuration are underlined

LAN802.3 NETWORK INTERFACE CONFIGURATION

The screen in Figure 9-1 is displayed when you select an NI name and the NI type LAN802.3 at the Network Interface Configuration Screen (Figure 8-9) and press **Add** or **Update**. It is also displayed when you type the path name:

@NETXPORT.NI.*niName*

in the command window of any screen and press **ENTER**, where the *niName* is the configured LAN802.3 NI name.

Use the screen in Figure 9-1 to configure a LAN network interface. The LAN802.3 Network Interface (NI) module serves to interface the upper layers of the transport product to the IEEE802.3 link layer. This screen supplies the information required for that interface. All of the fields, with the exception of the HP UPC Number, are used for internal resource allocation.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. After pressing **Update Data**, verify that the data record has been created by checking that the **Data:** flag is set to **Y**.

From this screen you proceed to the screens used to configure the LAN link, internet routing, and the IEEE802.3 address mappings.

NMGR/3000 (X.05.06) LAN802.3 NETWORK INTERFACE CONFIGURATION				Data: N	
When Data Flag is 'N', press 'Update Data' to create the data record.					
Command:					
Path: NETXPORT.NI. <i>niName</i>					
1497	Network Segment Size (Bytes)				
256	Number Of Inbound Buffers				
256	Number Of Outbound Buffers				
100	Maximum Number Of Nodes In Network				
08-00-09	HP UPC Number (Hex XX-XX-XX)				
File: filename.NET.SYS					
Go To	Go To	Go To	Go To		Update
PROTOCOL	LINK	INTERNET	MAPPING		Data
					Refresh
					Screen
					Prior
					Screen

Figure 9-1. LAN802.3 Network Interface Configuration Screen

LAN802.3 Network Interface Configuration

Choose the item you wish to configure, and press the corresponding key.

The only time you need to press **Go To Mapping** is when your LAN includes non-HP nodes. You do not need to configure mapping if any proxy node in the network already includes the mapping information in its network directory. Non-HP nodes do not support the Probe protocol. Therefore, you must configure mapping information about non-HP nodes so that other nodes on your LAN can communicate with them.

Fields

Network Segment Size

(HP modifiable). This field specifies the largest packet (data + protocol headers and not including the IEEE802.3 header) that will be sent by the LAN device (LANIC board).

The only reason for entering a value smaller than 1497 is to make better use of memory for those systems where it is known that upper layer services will always send shorter messages. Note that whenever packets larger than the network segment size are sent, they will be fragmented to the network segment size, thus incurring fragmentation overhead at the source and assembly overhead at the destination node.

Default Value: 1497 bytes

Range: 300-1497

Number Of Inbound Buffers

This field specifies the number of buffers to be allocated for inbound data. Buffer configuration is based on the number of TCP connections that will use a given network interface. An allocation of two buffers per connection will suffice for typical usage.

The default value is based on the assumption that the network manager desires to allow no more than the default number of TCP connections (see **Related Screens** below) to use the LAN NI. Hence the default is 128 (default TCP connections) * 2 = 256 buffers. When there is more than one NI, this value should probably be adjusted downward, since the connections might reasonably be expected to be using more than one NI at any one time. If the number of TCP connections is changed from the default value, the number of inbound buffers for all NIs should be reconsidered.

Whenever there are not enough buffers to support inbound traffic, an IP log message will indicate that the node is congested and the packet had to be discarded. See the *NS3000/V Error Message and Recovery Manual* for the exact IP log location and message. Repeated occurrence of this log message indicates that more inbound buffers need to be configured.

Related Screens:

- NETXPORT.GPROT.TCP

Maximum Number Of Connections is configured here. Default value is 128.

Default Value: 256

**Number Of
Outbound Buffers****Range: 32-2048**

This field specifies the number of buffers to be allocated for outbound data. Outbound buffers are used for outbound data packets and are held by the transport until they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Calculation of default values is as described above for inbound buffers.

Related Screens:

-NETXPORT.GPROT.TCP

The Maximum Number Of Connections is configured here. If it is increased, consider increasing the number of outbound buffers also.

Default Value: 256**Range: 32-2048****Maximum Number Of
Nodes In Network**

This number should equal the anticipated maximum number of nodes on the LAN. The number is used to allocate space for IP to IEEE802.3 address mappings that are obtained by the Probe protocol. If the maximum number of nodes is set too low and there is not enough room in the mapping table when a mapping entry needs to be made, a Probe error message is logged. See the *NS3000/V Error Message and Recovery Manual* for the exact log location and message.

It is wise to anticipate growth when configuring this value to minimize the need to shut down the transport subsystem to reconfigure this field.

Related Screens:

- NEXPORT.GLOBAL

Maximum Number Of Nodes In Network is a component of the computation of Maximum Directly Connected Nodes on the NETXPORT.GLOBAL screen.

Default Value: 100**Range: 1-1024****HP UPC Number**

(HP modifiable.) The HP universal product code, which is used to establish an HP-unique address used by the Probe protocol.

Default Value: 08-00-09

Only change the default in rare circumstances. If all nodes on the IEEE802.3 LAN are not configured with identical HP UPC numbers, Probe multicasts will not be universally recognized on the LAN.

PROTOCOL CONFIGURATION

The menu screen in Figure 9-2 is displayed when you press the function key for **Go To PROTOCOL** at the LAN802.3 Network Interface Configuration Screen (Figure 9-1). It is also displayed when you type the path name:

`@NETXPORT.NI.niName.PROTOCOL`

in the command window of any screen and press **ENTER**, where *niName* is the configured LAN802.3 NI name.

For the LAN802.3 NI, you must configure both the IP and Probe protocols. Therefore, both the **Go To PROBE** and the **Go To IP** function key labels are displayed.

MMGR/3000 (X.05.06) PROTOCOL CONFIGURATION
Select the next screen and press the corresponding function key.
Command:

Path: NETXPORT.NI.niName.PROTOCOL

IP - Configure Internet Protocol
PROBE - Configure PROBE Protocol (LAN Only)
DIAL - Configure DIAL Protocol (Router/Gateway Half Only)
Necessary Only If There Are Any Switched Links

File: filename.NET.SYS

Go To IP Go To PROBE Refresh Screen Prior Screen

Figure 9-2. Protocol Configuration Screen

Choose the protocol to configure, and press the corresponding function key.

INTERNET PROTOCOL CONFIGURATION

The screen in Figure 9-3 is displayed when you press the function key for **Go To IP** at the Protocol Configuration Screen (Figure 9-2). It is also displayed when you type the path name:

```
@NETXPORT.NI.niName.PROTOCOL.IP
```

in the command window of any screen and press **ENTER**, where *niName* is the configured LAN802.3 NI name.

This data-entry screen is used to supply information to the IP protocol instance for the network being configured. Each NI has an IP protocol. The IP address field is a key element in IP routing and datagram delivery algorithms. The other fields are useful for internal resource allocation and performance tuning.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NNXCR/3000 (X.05.06) IP PROTOCOL CONFIGURATION          Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:
Path: NETXPORT.NI.niName.PROTOCOL.IP

[20]          Store & Forward Buffers
              (Enter 0 To Disable Store & Forward)

[          ] IP Internet Address

[1]          Internal Message Queue Length

[20]          Fragment Assembly Queue Elements

File: filename.NET.SYS

[          ] [          ] [          ] [          ] [          ]
[          ] [Update] [Refresh] [Prior]
[          ] [Data]  [Screen]  [Screen]

```

Figure 9-3. IP Protocol Configuration Screen

Fields

Store & Forward Buffers

(HP modifiable.) This field allocates buffers to support store-and-forward over the network interface being configured. You do not need to allocate store-and-forward buffers if the node you are configuring is a non-gateway node on this IEEE 802.3 network. You will need to allocate store and forward buffers if the node being configured is an internet gateway and packets from another network will be forwarded over this network interface.

This number of store-and-forward buffers is configurable to allow performance tuning for different network types. However, HP recommends that you use the default number of store-and-forward buffers (20), and that you consult your HP representative before modifying this value.

Default Value: 20

NOTE

If this node is a non-gateway node on an IEEE 802.3 network and you are concerned about conserving MPE resources, you may wish to set this field to 0. No store-and-forward buffers will then be allocated.

Range: 0-50

IP Internet Address

Enter the internet protocol (IP) address for the network interface being configured.

Addresses are made up of a network portion and a node portion. The supported classes of network addresses have the following forms (Note: Δ=a space):

Class C	CΔnnn.nnn.nnnΔxxx
Class B	BΔnnn.nnnΔxxx.xxx
Class A	AΔnnnΔxxx.xxx.xxx

where nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address. The leftmost group of nnn has the following ranges for each address class:

Class C:	192-223
Class B:	128-191
Class A:	0-127

where xxx is a value ranging from 0 to 255, representing the node portion of the address.

Default Value: N

**Internal Message
Queue Length**

(HP modifiable.) This field puts a limit on the number of internal resources that the IP protocol may hold while awaiting some other protocol module action. It is a tuning parameter that should be modified only upon the recommendation of your HP representative.

The default is set to handle most cases; if it is too low for your network, packets will be discarded and you will receive a logging error message. Consult the *NS3000/V Error Message and Recovery Manual* for the specific log message.

Default value: 4

Range: 0-20

**Fragment Assembly
Queue Elements**

(HP modifiable.) This field specifies the maximum number of incomplete message fragments that this IP instance may hold.

HP recommends that you use the default of 20 for this field. For purposes of tuning your network's performance, and upon the recommendation of your HP representative, you may wish to alter the number of Fragment Assembly Queue Elements.

You may wish to configure a higher value if traffic conditions on your network are less than optimal; e.g., if internet routes are heavily loaded and intermediate nodes are congested. If conditions on your network are less busy, you may wish to configure a lower value. Only configure 0 if no fragmented messages will ever be received by the node you are configuring.

If message fragments are discarded, (indicating that the value configured in this field is too low) a log message will be recorded. Refer to the *NS3000/V Error Message and Recovery Manual* for a description of the message you receive.

Default value: 20

Range: 0-100

PROBE PROTOCOL CONFIGURATION

The screen in Figure 9-4 is displayed when you press the function key for **Go To PROBE** at the Protocol Configuration Screen (Figure 9-2). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.PROTOCOL.PROBE

in the command window of any screen and press **ENTER**, where *niName* is the configured LAN802.3 NI name.

This data-entry screen allows you to configure the information required for the Probe protocol. The Probe protocol exists on a LAN802.3 network to provide a means of exchanging addressing and naming information between nodes.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **N**.

```

MMGR/3000 (X.05.06) PROBE PROTOCOL CONFIGURATION Data: N
When Data Flag is "N", Press "Update Data" to create the data record.
Command:

Path: NETXPORT.NI.niName.PROTOCOL.PROBE

[N] Proxy Enabled (Y For YES, N For NO)

Probe Requests      Proxy Requests
[2]                 [2]      Retransmission Maximum
[10]                [40]     Retransmission Timeout (X100ms)

File: filename.NET.SYS

[Function Keys] [Update Data] [Refresh Screen] [Prior Screen]
    
```

Figure 9-4. Probe Protocol Configuration Screen

Fields

Proxy Enabled

Proxy nodes exist on LANs to provide node name and address mapping facilities for nodes that do not have local network directories. Proxy requests are multicast on the LAN to request information about a third party node from a proxy node.

YES enables this node to be a proxy server and to answer all proxy requests on this LAN. NO means that this node will ignore all proxy requests on this LAN network.

Other proxy related fields on this screen are:

- Proxy Requests Retransmission Maximum
- Proxy Requests Retransmission Timeout

Proxy related fields on other screens are:

- HP UPC Number on LAN802.3 Network Interface screen

Default Value: N

Range: Y or N

Probe Requests Retransmission Maximum

This is the maximum number of retransmissions of Probe requests (Name Requests and Address Requests) before a Probe failure is reported.

Because it is unlikely that Probe-request data is being lost, HP recommends that you keep the maximum number of retransmissions low.

Default Value: 2

Range: 1-10

Probe Requests Retransmission Timeout (x 100ms)

This field is for specifying the time limit between retransmissions of Probe requests. This is the time interval (in tenths of a second) that the Probe protocol will wait for a reply before attempting to retransmit a request. The value should be set sufficiently large to avoid retransmissions in a temporarily overloaded environment, yet small enough to get a timely failure report when failure is inevitable.

Default Value: 10

Range: 1-100

LAN802.3 Network Interface Configuration

Proxy Requests Retransmission Maximum

The maximum number of retransmissions of proxy requests before a Probe failure is reported.

Because it is unlikely that Probe-request data is being lost, HP recommends that you keep the maximum number of retransmissions low.

Default Value: 2

Range: 1-10

Proxy Requests Retransmission Timeout (x 100ms)

The time interval (in tenths of a second) that the Probe protocol will wait for a reply before attempting to retransmit a proxy request. The value should be set sufficiently large to avoid retransmissions in a temporarily overloaded environment, yet small enough to get a timely failure report when failure is inevitable.

The default value is set somewhat higher than for Probe requests timeout because proxy requests involve a network directory lookup and consequently more time than regular Probe requests.

Default Value: 40

Range: 1-100

LAN802.3 NETWORK INTERFACE LINK

The select screen in Figure 9-5 is displayed when you press the function key for **Go To LINK** at the LAN802.3 Network Interface Configuration Screen (Figure 9-1). It is also displayed when you type the path name:

`@NETXPORT.NI.niName.LINK`

in the command window of any screen and press **ENTER**, where *niName* is the configured LAN802.3 NI name.

Use the fields and the function keys of this select screen to perform the desired action.

- To define a new link configuration, specify the link name; then press **Add**. The path for the selected link name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing link configuration, specify the link name; then press **Update**. The data screen on the path for the specified link is displayed.
- To change the link name of an existing link configuration, specify the link name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Network Links.
- To delete an existing link configuration, specify the link name; then press **Delete**. Press **Delete** again to confirm the deletion. If you do not press **Delete** a second time, the deletion will not occur. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Network Links.

```

HMNCR/3000 (X.05.06) LAN802.3 NETWORK INTERFACE LINK
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path: NETXPORT.NI.niName.LINK

[ ] Link Name      [ ] Type : LAN - LAN
[ ] New Name      (if new)

          Configured Network Links

Name      Type      Name      Type      Name      Type
[ ]       [ ]       [ ]       [ ]       [ ]       [ ]

File: filename.NET.SYS

Next Page  Prev Page  Delete  Rename  Add  Update  Refresh Screen  Prior Screen
    
```

Figure 9-5. LAN802.3 Network Interface Link Screen

Fields

Link Name

Enter the link name from the LAN802.3 Link configuration to allow the Network Transport to associate the correct link with the LAN802.3 NI. The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

The link name is used by the Network Transport when establishing connections.

Related Screens:

The Link name on this screen *must* match the link name in the Link name field of the LINK CONFIGURATION screen whose pathname is LINKCONF.

Type

(Required when adding.) Enter LAN as the link type.

New Name

(Required when renaming.) Enter a link name. This new link name is used in place of the current link name for an existing link configuration. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

LAN LINK CONFIGURATION

The screen in Figure 9-6 is displayed when you select an NI link name at the LAN802.3 Network Interface Link Screen (Figure 9-5) and press **Add** or **Update**. It is also displayed when you type the path name:

```
@NETXPORT.NI.niName.LINK.nilink
```

in the command window of any screen and press **ENTER**, where *niName* is the configured LAN802.3 NI name and *nilink* is the configured LAN802.3 NI link name.

This screen supplies the information required to interface the LAN NI to a LAN802.3 link.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

NMMGR/3000 (X.05.06) LAN LINK CONFIGURATION		Data: N
When Data Flag is "N", press "Update Data" to create the data record.		
Command:		
Path:	NETXPORT.NI.niName.LINK.nilink	
[Y]	Start Device On Network Initialization (Y/N)	
[N]	Enable Idle Device Timer (Y/N)	
File:	filename.NET.SYS	
	Update Data	Refresh Screen
		Prior Screen

Figure 9-6. LAN Link Configuration Screen

Fields

Start Device

(Display only.) A YES value means that the device is to be started when a NETCONTROL START command is issued for the network interface. For the LAN, this is always the case, and therefore this field cannot be changed.

Default Value: Y

Enable Idle Device Timer

(Display only.) Specifies whether the device is to be disconnected automatically if no packets are received or transmitted over the link during a specified time period. This does not apply to the LAN.

Default Value: N

NEIGHBOR GATEWAYS

The select screen in Figure 9-7 is displayed when you press the function key for **Go To INTERNET** at the LAN802.3 Network Interface Configuration Screen (Figure 9-1). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.INTERNET

in the command window of any screen and press **(ENTER)**, where the *niName* is the configured LAN802.3 NI name.

You only need to configure this screen, and the screens that follow it, if the node you are configuring is a gateway (full or half) node.

Use the fields and the function keys of this select screen to perform the desired action.

- To define a new gateway configuration, specify the gateway name; then press **Add**. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing gateway configuration, specify the gateway name; then press **Update**. The data screen on the path for the specified gateway is displayed.
- To change the gateway name of an existing gateway configuration, specify the gateway name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Gateways.
- To delete an existing gateway configuration, specify the gateway name; then press **Delete**. Press **Delete** again to confirm the deletion. If you do not press **Delete** a second time, the deletion will not occur. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Gateways.

From this screen you proceed to the screen used to configure names of all networks reachable from this gateway node.

NNMGR/3000 (X.05.06) NEIGHBOR GATEWAYS
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path: NETXPORT.NI.niName.INTERNET

	Gateway Name
	New Name

Configured Gateways

--	--	--	--	--	--

File: filename.NET.SYS

Next Page	Prev Page	Delete	Rename	Add	Update	Refresh Screen	Prior Screen
-----------	-----------	--------	--------	-----	--------	----------------	--------------

Figure 9-7. Neighbor Gateways Screen

Fields

Gateway Name

Enter a name to represent a gateway on this LAN802.3 network, through which one or more remote networks can be reached. A gateway name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

New Name

(Required only when renaming.) Enter a gateway name to represent a neighbor gateway. This new gateway name is used in place of the current gateway name for an existing gateway configuration. The name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

NEIGHBOR GATEWAY REACHABLE NETWORKS

The screen in Figure 9-8 is displayed when you select a gateway name at the Neighbor Gateways Screen (Figure 9-7) and press **Add** or **Update**. It is also displayed when you type the path name:

`@NETXPORT.NI.niName.INTERNET.gatewayn`

in the command window of any screen and press **ENTER**, where *niName* is the configured LAN802.3 NI name, and *gatewayn* is the configured LAN802.3 NI gateway name.

After you have entered all the required data, you must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data:** flag is set to **Y**.

MMNGR/3000 (X.05.06) NEIGHBOR GATEWAY REACHABLE NETWORKS Data: N
 When Data Flag is "N", press "Update Data" to create the data record.
 Command:

Path: NETXPORT.NI.niName.INTERNET.gatewayn

Neighbor Gateway IP Internet Address

Configured Reachable Networks PAGE 1

IP Network Address	Hops	IP Network Address	Hops

File: filename.NET.SYS

Next Page
Prev Page
First Page
Last Page
Condense Page
Update Data
Refresh Screen
Prior Screen

Figure 9-8. Neighbor Gateway Reachable Networks Screen

NOTE

The information configured in this screen can extend to more than one page, if necessary, to allow configuration of more than 10 reachable networks. Press **Next Page** to proceed to a new page. Press **Prev Page** to display a prior page. Use **First Page** to display the first page (for example, if you are viewing the third page, pressing **First Page** will immediately display the first page). Press **Last Page** to display the last page of reachable networks that has been configured. To consolidate reachable networks entries (from several pages, for example) press **Condense Page**.

Fields

**Neighbor Gateway
IP Internet Address**

Enter the full network address of a gateway node (on this network) that is to be used to reach other networks (any network in the same catenet other than the network of which this node is a member). The network portion of the address must be the same as that entered on the IP Protocol Configuration screen for the network interface you are configuring (see Related Screens, below).

Addresses are made up of a network portion and a node portion. The possible classes of network addresses have the following forms (Δ =a space):

Class C	C Δ nnn.nnn.nnn Δ xxx
Class B	B Δ nnn.nnn Δ xxx.xxx
Class A	A Δ nnn Δ xxx.xxx.xxx

where nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address, and xxx is a value ranging from 0 to 255, representing the node portion of the address. The leftmost group of nnn has the following ranges for each address class:

Class C:	192-223
Class B:	128-191
Class A:	0- 127

Default Value: None

Related Screens:

- NETXPORT.NI.niName.PROTOCOL.IP

The network address (network portion of the IP address) configured in this screen must match the Neighbor Gateway IP Internet Address configured in the current screen.

**Configured Reachable
Networks IP Network
Address**

Enter the internet addresses of the remote networks that can be reached through the gateway whose network address is configured in the previous field. Only the internet portion of the network address is significant for this field (see above for valid formats of internet addresses). The node portion must be entered; however, it may be set to all zeros.

Related Screens:

- NETXPORT.NI.*niName*.INTERNET

This pathname corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

**Configured Reachable
Networks Hops**

Enter the internet hop count to the reachable network whose IP address is configured to the left of the Hops field. (The internet hop count is the number of full internet gateways that will be used to route a message to the destination network. If two partner gateway halves are used as part of the internet route, they are counted as one hop.)

Hop count is used internally to determine which neighbor gateway (if more than one exists) is on the shortest path to the remote network. If more than one gateway can reach a given remote network, and the number of hops to the remote network is equal for each gateway, you can specify which gateway the Network Transport will use by configuring an artificially high hop count. The Network Transport will always use the gateway with the lowest hop count.

If the same hop count value is configured for multiple gateways, then the Network Transport will choose internally from among the routes with equal hop counts.

Default Value: None

Range: 1-32767

NOTE

To delete a reachable network entry, fill the field to be deleted with blanks and press **Update Data**.

LAN802.3 MAPPING CONFIGURATION

The select screen in Figure 9-11 is displayed when you press the function key for **Go To MAPPING** at the LAN802.3 Network Interface Configuration Screen (Figure 9-1). It is also displayed when you type the path name:

`@NETXPORT.NI.niName.MAPPING`

in the command window of any screen and press **ENTER**, where the *niName* is the configured LAN802.3 NI name.

Mapping information is required only when you have non-HP nodes on a LAN. This is because non-HP nodes do not support the Probe Protocol, and they do not have LAN802.3 addresses configured in the network directory. Mapping information pertaining to a non-HP node is used by other nodes to communicate with the non-HP node.

Use the fields and the function keys of this select screen to perform the desired action.

- To define a new mapping configuration, specify the mapping name; then press **Add**. The path for the selected mapping name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing mapping configuration, specify the mapping name; then press **Update**. The data screen on the path for the specified mapping name is displayed.
- To change the mapping name of an existing mapping configuration, specify the mapping name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Mappings.
- To delete an existing mapping configuration, specify the mapping name; then press **Delete**. Press **Delete** again to confirm the deletion. If you do not press **Delete** a second time, the deletion will not occur. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Mappings.

NMMGR/9000 (X.05.06) LAN802.3 MAPPING CONFIGURATION
 Type in name of item to Update, Delete, or Rename; or Add a new item.
 Command:

Path: NETXPORT.NI.niName.MAPPING

Static Neighbor Node Name
 New Name

Configured Mappings

File: filename.NET.SYS

Next Page Prev Page Delete Rename Add Update Refresh Screen Prior Screen

Figure 9-11. Mapping Configuration Screen

Fields

Static Neighbor Node Name

Enter a mapping name to represent the non-HP node for which you are configuring mapping information. A mapping name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

New Name

(Required only when renaming.) Enter a mapping name. This new mapping name is used in place of the current mapping name for an existing mapping configuration. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

Fields

IP Internet Address

This is the full network address of a non-HP node. Note that the network portion of the address must be the same as that entered on the IP Protocol Configuration screen. (See related screens below.)

Addresses are made up of a network portion and a node portion. The supported classes of network addresses have the following forms:

Class C	CΔnnn.nnn.nnnΔxxx
Class B	BΔnnn.nnnΔxxx.xxx
Class A	AΔnnnΔxxx.xxx.xxx
Loopback	EΔ255.255.255.255

where Δ denotes a blank space, and nnn is a value ranging from 255, representing eight bits of the network portion of an address. The leftmost group of nnn has the following ranges for each address class:

Class C:	192-223
Class B:	128-191
Class A:	0-127

and xxx is a value ranging from 0 to 255, representing the node portion of the address. Note also that a space is used to delimit the boundary between the network portion and the node portion of the address.

Default Value: N

Related Screens:

- NETXPORT.NI.*niName*.PROTOCOL.IP. The network address (network portion of the IP address) in this screen must match the IP internet address configured in the current screen.

IEEE802.3 IP SAP

(HP modifiable). The protocol ID assigned to the Internet Protocol (IP) by ARPA.

Default Value: 06

IEEE802.3 Address

The IEEE802.3 station address of the destination node.



ROUTER NETWORK INTERFACE CONFIGURATION

SECTION

10

The screens described in this section are used for configuring a node with a router network interface.

There are four main branches of router network interface configuration. These are reached by choosing different function keys displayed on the first screen, called the ROUTER NETWORK INTERFACE screen. All of the router network interface configuration screens are listed below, with their places in the configuration tree indicated by indentation.

ROUTER NETWORK INTERFACE CONFIGURATION - This screen enables you to configure information about a router network interface, such as the number of inbound and outbound buffers, the size of an internal table that holds information about routes, and the network hop count. From this screen, you can proceed to one of four branches of router NI configuration: protocol configuration, link configuration, internet configuration, and mapping configuration.

PROTOCOL CONFIGURATION - You will reach this screen if you press **Go To PROTOCOL** on the ROUTER NETWORK INTERFACE CONFIGURATION screen. This screen allows you to choose to proceed to either IP or DIAL protocol configuration.

IP PROTOCOL CONFIGURATION - This screen, which you will reach by pressing **Go To IP** on the previous screen, enables you to configure the number of store and forward buffers on this node, the node's IP address, and tuning parameters for the IP protocol.

DIAL ID PROTOCOL CONFIGURATION - This screen enables you to configure information about a dial link that is used by the Dial ID protocol--retransmission information, and whether security is in effect.

SECURITY STRING(S) CONFIGURATION - This screen allows you to specify the security strings used by the Dial ID protocol.

ROUTER NETWORK INTERFACE LINKS - This screen, which you will reach by pressing **Go To Link** on the ROUTER NETWORK INTERFACE CONFIGURATION screen, allows you to specify the name of the link (as previously configured in the LINK CONFIGURATION screen), and whether the link is a direct dial, shared dial, or direct connect link.

DIRECT CONNECT LINK CONFIGURATION - This screen, which NMMGR displays when you specify a direct connect link in the previous screen, allows you to enter information pertaining to the direct connect link.

ROUTER DIAL LINK CONFIGURATION - This screen, which NMMGR displays when you specify a direct dial or shared dial link in the previous screen, allows you to enable or disable the Dial ID protocol.

NEIGHBOR GATEWAYS - This screen, which you will reach by pressing **Go To INTERNET** on the ROUTER NETWORK INTERFACE CONFIGURATION screen, permits you to specify the nodes that will be functioning as gateways to other networks.

NEIGHBOR GATEWAY REACHABLE NETWORKS - One instance of this screen will be configured for each gateway entered in the previous screen. This screen provides data

Router Network Interface Configuration

about the networks that can be reached from the gateway, and the gateway's IP address

ROUTER MAPPING CONFIGURATION - This screen, which you will reach by pressing **Go To MAPPING**, begins the NMMGR branch that allows you to specify information about routes between the node you are configuring and other nodes on the same router network. This screen in particular allows you to specify a name that identifies each route.

ROUTER REACHABLE NODES - This screen, which is revisited for each route specified in the previous screen, allows you to enter data about each route.

NOTE

Configurable fields described in this manual are **required** unless otherwise stated.

Fields described as "**HP modifiable**" should be changed only upon the recommendation of your **HP** representative.

On the screens shown in this section, fields that must be configured when performing guided configuration are underlined.

ROUTER NETWORK INTERFACE CONFIGURATION

The router network interface (NI) serves to interface the upper layers of the transport protocol to the data link layer. The router NI screen (shown below) supplies the information required for that interface. The screen is displayed when you select an NI name and the NI type **ROUTER** at the Network Interface Configuration Screen (Figure 8-9) and press **Add** or **Update**. It is also displayed when you type the path name:

@NETXPORT.NI.*niName*

in the command window of any screen and press **(ENTER)**, where the *niName* is the configured router NI name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

From this screen you proceed to the screens used to configure the router network interface.

NNMGR/3000 (X.05.06) ROUTER NETWORK INTERFACE CONFIGURATION				Data: N	
When Data Flag is "N", press "Update Data" to create the data record.					
Command:					
Path: NETXPORT.NI. <i>niName</i>					
[256]	Number Of Inbound Buffers				
[256]	Number Of Outbound Buffers				
[100]	Number Of Routing Table Entries				
[]	Network Hop Count				
[]	Idle Device Timeout Value (Minutes)				
	0 = Timer Disabled For All Devices				
File: filename.NET.SYS					
Go To PROTOCOL	Go To LINK	Go To INTERNET MAPPING	[]	Update Data	Refresh Screen
					Prior Screen

Figure 10-1. Router Network Interface Configuration Screen

Choose the item you wish to configure and press the corresponding function key.

Fields

Number of Inbound Buffers

This field specifies the number of buffers to be allocated for inbound data. Buffer configuration is based on the number of TCP connections that will use a given network interface. An allocation of two buffers per connection will suffice for typical usage.

The default value is based on the assumption that the Network Manager desires to allow no more than the default number of TCP connections (128) to use the router NI (see related screens, below). Hence the default is $128 * 2 = 256$ inbound buffers. When there is more than one NI, this value should probably be adjusted downward, since the connections might reasonably be expected to be spread over all the NIs rather than be concentrated over only one NI. If the number of TCP connections is changed from the default value, the number of inbound buffers for all NI's should be reconsidered.

Whenever there are not enough buffers to support inbound traffic, an IP log message will indicate that the node is congested and the packet had to be discarded. (See the *NS3000/V Error Message and Recovery Manual* for the exact IP log location and message.) Repeated occurrence of this log message indicates that more inbound buffers should be configured.

Related Screens:

- NETXPORT.GPROT.TCP

The maximum number of TCP Connections is configured here. The default value is 128.

Default Value: 256

Range: 32-2048

Number of Outbound Buffers

This field specifies the number of buffers to be allocated for outbound data. Outbound buffers are used for outbound data packets and are held by the transport until acknowledged by the destination. Not allocating enough outbound buffers may adversely affect TCP throughput. Calculation of the default value is the same as described above for inbound buffers.

Related Screens:

- NETXPORT.GPROT.TCP

The default value for maximum TCP connections is configured here. If it is increased, the number of outbound buffers must also be increased.

Default: 256

Range: 32-2048

**Number of Routing
Table Entries**

This is the number of routing table entries necessary to support the router network configuration. The router NI uses this value to allocate memory for the routing table.

This value should be at least as large as the total number of router reachable nodes that are configured. In addition, future growth should be anticipated. If insufficient space is allocated, the router NI logs a message indicating this. (See the *NS3000/V Error Message and Recovery Manual* for the specific NI log message details.)

Related Screens:

- NETXPORT.NI.*HiName*.MAPPING.*mapentry*
Reachable nodes are configured here.

- NETXPORT.GLOBAL
The number of path descriptors configured in this screen is related to the maximum number of nodes in the network.

Default Value: 100

Range: 1-1024

Network Hop Count

This is the maximum number of hops that a packet entering the network can make. It is the distance between the two most remotely separated nodes on the network. Distance is measured in terms of "hops," where each intermediate node between two end nodes is counted as a "hop."

The network hop count determines a packet's time to live, that is, the time (in numbers of hops) that a packet is allowed to remain in the network. A packet whose time to live has expired can be assumed to be undeliverable because of some undetected routing anomaly, and will be discarded.

If this value is set too low, the danger exists that packets will be discarded prematurely (that is, before they reach their destination). If the value is set too high, an undeliverable packet may remain in the network too long, and possibly contribute to network congestion.

Default Value: None

Range: 1-1024

Router Network Interface Configuration

Idle Device Timeout Value (Mins)

This field is relevant only if the link is a dial link. For those devices that have the Idle Device Timer enabled, if there is no activity during this time interval, the device is considered to be inactive and will be shut down. A timeout value of zero disables the Idle Device Timer for the link on this network interface, thus overriding any enabled device timer (see Related Screens, below). The purpose of the Idle Device Timer is to shut down dial links that have become idle.

Related Screens:

- NETXPORT.NI.*niName*.LINK.*nilink*
An entry in this screen enables/disables Idle Device Timer for the device.
- NETXPORT.GPROT.TCP
The Connection Assurance Interval set in this screen must be less than the Idle Device Timeout value configured in the current screen. Note that one value (Connection Assurance) is configured in seconds, the other (Idle Device Timeout) is configured in minutes. You must convert to the same units to compare the values.

Default Value: None

Range: 0-720

ROUTER NETWORK INTERFACE PROTOCOL CONFIGURATION

The menu screen in Figure 10-2 is displayed when you press the function key for **Go To PROTOCOL** at the Router Network Interface Configuration screen (Figure 10-1). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.PROTOCOL

in the command window of any screen and press **ENTER**, where *niName* is the configured router NI name.

For the router NI, you must configure the IP protocol. The Dial protocol must be configured only if you have any switched lines. The **Go To DIAL** and **Go To IP** function key labels are displayed.

```

MMGR/3000 (X.05.08) PROTOCOL CONFIGURATION
Select the next screen and press the corresponding function key.
Command:

Path:  NETXPORT.NI.niName.PROTOCOL

IP      -  Configure Internet Protocol
PROBE   -  Configure PROBE Protocol (LAN Only)
DIAL    -  Configure DIAL Protocol (Router/Gateway Half Only)
          Necessary Only If There Are Any Switched Links

File:  filename.NET.SYS

Go To  Go To  Refresh  Prior
IP     DIAL  Screen  Screen

```

Figure 10-2. Protocol Configuration Screen

Choose the protocol to configure and press the corresponding function key.

Fields

Store & Forward Buffers

(HP modifiable.) This field allocates buffers to support store-and-forward over the network interface being configured.

You must allocate store-and-forward buffers if (a) this is a node with two or more router links or (b) the node being configured is an internet gateway and packets from another network will be forwarded over this network interface.

This number of store-and-forward buffers is configurable to allow performance tuning for different network types. However, HP recommends that you use the default number of store-and-forward buffers (20), and that you consult your HP representative before modifying this value.

Default Value: 20

Range: 0-50

IP Internet Address

Enter the internet protocol (IP) address for the network interface being configured.

Addresses are made up of a network portion and a node portion. The supported classes of network addresses have the following forms:

Class C	CΔnnn.nnn.nnnΔxxx
Class B	BΔnnn.nnnΔxxx.xxx
Class A	AΔnnnΔxxx.xxx.xxx

where Δ denotes a blank, and nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address. The leftmost group of nnn has the following ranges for each address class:

Class C:	192-223
Class B:	128-191
Class A:	0-127

where xxx is a value ranging from 0 to 255, representing the node portion of the address.

Default Value: None

Internal Message Queue Length

(HP modifiable.) This field puts a limit on the number of internal resources that the IP protocol may hold while awaiting some other protocol module action. It is a tuning parameter that should be modified only upon the recommendation of your HP representative.

The default is set to handle most cases; if it is too low for your network, packets will be discarded and you will receive a logging error message.

Consult the *NS3000/V Error Message and Recovery Manual* for the specific log message.

Default value: 4

Range: 0-20

**Fragment Assembly
Queue Elements**

(HP modifiable.) This field specifies the maximum number of incomplete message fragments that this IP instance may hold.

HP recommends that you use the default of 20 for this field. For purposes of tuning your network's performance, and upon the recommendation of your HP representative, you may wish to alter the number of Fragment Assembly Queue Elements.

You may wish to configure a higher value if traffic conditions on your network are less than optimal; e.g., if internet routes are heavily loaded and intermediate nodes are congested. If conditions on your network are less busy, you may wish to configure a lower value. Only configure 0 if no fragmented messages will ever be received by the node you are configuring.

If message fragments are discarded, (indicating that the value configured in this field is too low) a log message will be recorded. Refer to the *NS3000/V Error Message and Recovery Manual* for a description of the message you receive.

Default value: 20

Range: 0-100

DIAL ID PROTOCOL CONFIGURATION

Along with other information, the Dial ID Protocol Configuration screen provides a means of verifying that the remote node is indeed the intended remote node and that both local and remote nodes have proper security access. This screen, shown below, is displayed when you press the function key for **Go To DIAL** at the Protocol Configuration Screen (Figure 10-2). It is also displayed when you type the path name:

```
@NETXPORT.NI.niName.PROTOCOL.DIAL
```

in the command window of any screen and press **ENTER**, where *niName* is the configured router NI name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

After the data has been updated, press **Go to SECURITY** to proceed to the next screen.

NNMGR/3000 (X.05.06) DIAL ID PROTOCOL CONFIGURATION		Data: N
When Data Flag is "N", press "Update Data" to create the data record.		
Command:		
Path: NETXPORT.NI.niName.PROTOCOL.DIAL		
[2]	Maximum Retransmissions Per Packet	
[5]	Retransmission Timeout (Secs)	
[Y]	Security On (Y/N)	
File: filename.NET.SYS		
Go To SECURITY		Update Data Refresh Screen Prior Screen

Figure 10-4. Dial ID Protocol Configuration Screen

Fields

Maximum Retransmissions Per Packet

(HP modifiable.) This is the maximum number of times that a Dial ID Protocol packet will be retransmitted. If the expected response to a packet is not received after this number of retransmissions, the link device it is using is closed. This value is related to the Retransmission Timeout value discussed below. Multiplying these values results in the total time that passes before a failure is reported (an error message will be recorded).

HP recommends that you alter this value only upon the recommendation of your HP representative. However, note that if the value is set too low, dial connections may fail unnecessarily when response times are temporarily slowed by transient conditions such as an abnormally high volume of traffic. The higher the value, the longer it will take to be notified of a link failure if one occurs.

Default Value: 2

Range: 1-10

Retransmission Timeout (Secs)

(HP modifiable.) The Retransmission Timeout is the time interval that passes between retransmissions of a Dial ID protocol packet.

Multiplying the values configured for Maximum Number of Retransmissions Per Packet (described above) and Retransmission Timeout results in the total time that passes before a failure is reported (an error message will be recorded).

HP recommends that you alter this value only upon the recommendation of your HP representative. However, note that if the value is set too low, dial connections may fail unnecessarily when response times are temporarily slowed by transient conditions such as an abnormally high volume of traffic. The higher the value, the longer it will take to be notified of a link failure if one occurs.

Default Value: 5

Range: 1- 10

Security On (Y/N)

A Y (Yes) value in this field indicates that security strings are to be exchanged and validated between the node being configured and a remote node.

When a dial connection is initiated by a remote node, the security string sent by the remote node is checked against the list of valid security strings configured for the Dial ID Protocol for this network interface. (See Related Screens, below).

When a dial connection is initiated by this node, the local Dial ID protocol sends the destination's security string (as configured on this node) to that node. (Related Screens, below, indicates the pathname of the screen in

which you can configure security strings.)

If security validation fails, an error message is logged, where PARM indicates whether the failure was local or remote. (See the *NS3000/V Error Message and Recovery Manual* for a description of any error message received.)

Related Screens:

- NETXPORT.NI.*niName*.PROTOCOL.DIAL.SECURITY
Security Strings valid for this network are configured in this screen.
- NETXPORT.NI.*niName*.MAPPING.*mapentry*
The remote node's security string is configured in this screen.

Default Value: Y

Range: Y or N

Fields

Configured Security Strings

Enter the security string that remote nodes must use to gain dial link access to the node you are configuring. The string can contain up to eight alphanumeric characters, left justified, with no embedded blanks.

Default Value: HP

Related Screen:

- NETXPORT.NI.*niName*.LINK.*niLink*

The Dial ID protocol is enabled/disabled on this screen.

NOTE

To delete a security string, blank out the field that contains the string you want deleted, and press **Update Data**.

ROUTER NETWORK INTERFACE LINKS

The select screen in Figure 10-6 is displayed when you press the function key for **Go To LINK** at the Router Network Interface Configuration Screen (Figure 10-1) It is also displayed when you type the path name:

@NETXPORT NI *niName*.LINK

in the command window of any screen and press **(ENTER)**, where *niName* is the configured router NI name.

Use the fields of this select screen in combination with the function keys to perform the desired action.

- To define a new link configuration, specify the link name; then press **Add**. The path for the selected link name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing link configuration, specify the link name; then press **Update**. The data screen on the path for the specified link is displayed.
- To change the link name of an existing link configuration, specify the link name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Network Links.
- To delete an existing link configuration, specify the link name; then press **Delete**. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Network Links. Press **Delete** again to confirm; otherwise, the deletion will not take effect.

```

NMNCR/3000 (X.05.06)  ROUTER NETWORK INTERFACE LINKS
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path:  NETXPORT.NI.niName.LINK

[ ] Link Name
[ ] New Name

Types:  DD - Direct Dial
        DC - Direct Connect
        SD - Shared Dial
        (if new)

Configured Network Links

Name      Type      Name      Type      Name      Type

[ ] [ ]  [ ] [ ]  [ ] [ ]

File:  filename.NET.SYS

Next Page  Prev Page  Delete  Rename  Add  Update  Refresh Screen  Prior Screen
    
```

Figure 10-6. Router Network Interface Links Screen

Fields

Link Name

Enter the link name that pertains to this NI as specified in the link configuration screen. This enables the Network Transport to associate the correct link with this router NI. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

The link name is used by the Network Transport when establishing connections and *must* match the link name configured for the router link configuration.

Related Screens:

- LINKCONF

A link name specified in this screen (and specified as a BSC, LAP-B, or ATP/ASNP type) must match the link name here.

- NETXPORT.NI.niName.MAPPING.mapentry

This screen specifies which link to use to reach a specific node on the router network. The link specified must be one entered on the current screen.

Types

Enter DD if only one remote node can be reached over a dial link.

Router Network Interface Configuration

Enter SD if more than one remote node can be reached over a dial link.

Enter DC if the link is direct-connect (hardwired) or a leased line.

Related Screens:

- NETXPORT.NI.*nzName*.MAPPING.*mapentry*

This screen maps router links to destination nodes. If multiple destinations are mapped to a single link, the link must be configured as a shared dial (SD) link in the current screen.

New Name

(Required only when renaming.) Enter a link name. This new link name is used in place of the current link name for an existing link configuration. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

DIRECT CONNECT LINK CONFIGURATION

The Direct Connect Link Configuration Screen supplies the information required to interface a router NI to a non-dial link (that is, a leased line or a hardwired connection). This screen, shown below, is displayed when you select an NI link name and the link type DC at the Network Interface Links Screen (Figure 10-6) and press **Add** or **Update**. It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.LINK.*nilink*

in the command window of any screen and press **ENTER**, where *niName* is the configured router NI name, and *nilink* is the configured router NI link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

NMMGR/3000 (X.05.06) DIRECT CONNECT LINK CONFIGURATION		Data: N	
When Data Flag is "N", press "Update Data" to create the data record.			
Command:			
Path: NETXPORT.NI. <i>niName</i> .LINK. <i>nilink</i>			
[Y]	Start Device On Network Initialization (Y/N)		
[N]	Enable Idle Device Timer		
File: filename.NET.SYS			
		Update Data	Refresh Screen
			Prior Screen

Figure 10-7. Direct Connect Link Configuration Screen

Fields

**Start Device
On Network
Initialization (Y/N)**

A Y (Yes) value means that the device is to be started when a NETCONTROL START command is issued for the network interface being configured. An N (No) means that a NETCONTROL ADDLINK command must be used to start the device.

Default Value: Y

Range: Y or N

**Enable Idle
Device Timer**

This field specifies whether the device is to be disconnected automatically if no packets have been received or transmitted over the link during a specified time period. This field is relevant only if a timeout value has been entered in the network interface screen listed below.

Related screens:

- NETXPORT.NI.*niName*

The Idle Device Timeout value is configured on this screen.

Default Value: N

Range: Y or N

ROUTER DIAL LINK CONFIGURATION

Dial Link Configuration provides the information necessary to interface the router NI to a dial link. This screen, shown below, is displayed when you select an NI link name and link type DD or link type SD at the Network Interface Links Screen (Figure 10-6) and press **Add** or **Update**. It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.LINK.*nilink*

in the command window of any screen and press **ENTER**, where *niName* is the configured router NI name, and *nilink* is the configured router NI link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NMNGR/3000 (X.05.06)  ROUTER DIAL LINK CONFIGURATION           Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path:  NETXPORT.NI.niName.LINK.nilink

[Y]      Enable DIAL ID Protocol (Y/N)
[Y]      Start Device On Network Initialization (Y/N)
[Y]      Enable Idle Device Timer

File:  filename.NET.SYS

[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
Update  Refresh  Prior
Data    Screen  Screen
  
```

Figure 10-8. Router Dial Link Configuration Screen

Fields

Enable Dial ID Protocol

(HP modifiable.) A Y (Yes) value activates the Dial ID Protocol for a dial link. The Dial ID protocol verifies the identity of a remote node and ensures that both local and remote nodes have the required security access.

The Dial ID Protocol should be disabled (by entering a NO value) only to

Router Network Interface Configuration

connect a dial link to a remote node that does not support the Dial ID Protocol (that is, a non-HP node).

Related Screens:

- NETXPORT.NI.*niName* LINK
Configures a link name and link type. The link name specified leads to this screen.
- NETXPORT.NI.*niName*.PROTOCOL.DIAL.SECURITY
Configures security strings for this node.
- NETXPORT.NI.*niName*.MAPPING
Configures information about reachable router nodes. Remote nodes' security strings are configured on this screen.

Default Value: Y

Range: Y or N

Start Device On Network Initialization (Y/N)

A Y (Yes) value means that the device is to be started when a NETCONTROL START command is issued for this network interface. An N (No) means that a NETCONTROL ADDLINK command must be used to start the device.

Default Value: Y

Range: Y or N

Enable Idle Device Timer

This field specifies whether the device is to be disconnected automatically if no packets have been received or transmitted over the link during a specified time period. It is relevant only if a timeout value has been entered in the router NI screen (see Related Screens below).

Related Screens:

- NETXPORT.NI.*niName*
Configures router network interface information. The value configured for Idle Device Timeout is configured on this screen.

Default Value: Y

Range: Y or N

NEIGHBOR GATEWAYS

The select screen in Figure 10-9 is displayed when you press the function key for **Go To INTERNET** at the Router Network Interface Configuration screen (Figure 10-1). It is also displayed when you type the path name:

`@NETXPORT.NI.niName.INTERNET`

in the command window of any screen and press **ENTER**, where the *niName* is the configured router NI name.

Use the fields and the function keys of this select screen to perform the desired action.

- To define a new gateway configuration, specify the gateway name; then press **Add**. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing gateway configuration, specify the gateway name; then press **Update**. The data screen on the path for the specified gateway is displayed.
- To change the gateway name of an existing gateway configuration, specify the gateway name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Gateways.
- To delete an existing gateway configuration, specify the gateway name; then press **Delete**. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Gateways. Press **Delete** again to confirm; otherwise, the deletion will not take effect.

MMGR/3000 (X.05.06) NEIGHBOR GATEWAYS
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path: NETXPORT.NI.niName.INTERNET

Gateway Name
New Name

Configured Gateways

--	--	--	--	--	--

File: filename.NET.SYS

Next Page	Prev Page	Delete	Rename	Add	Update	Refresh Screen	Prior Screen
-----------	-----------	--------	--------	-----	--------	----------------	--------------

Figure 10-9. Neighbor Gateways Screen

Fields

Gateway Name

Enter a name to represent a gateway node on this router network, through which one or more remote networks can be reached. A gateway name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

New Name

(Required only when renaming.) Enter a name to represent a gateway node on this router network. This new gateway name is used in place of the current gateway name for an existing gateway configuration. The name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

NOTE

The information configured in this screen can extend to more than one page, if necessary, to allow configuration of more than 10 reachable networks. Press **Next Page** to proceed to a new page. Press **Prev Page** to display a prior page. Use **First Page** to display the first page (for example, if you are viewing the third page, pressing **First Page** will immediately display the first page). Press **Last Page** to display the last page of reachable networks that has been configured. To consolidate reachable networks entries (from several pages, for example) press **Condense Page**.

Fields

**Neighbor Gateway
IP Internet Address**

Enter the full network address of a gateway node (on this network) that is to be used to reach other networks (any network in the same catenet other than the network of which this node is a member). The network portion of the address must be the same as that entered on the IP Protocol Configuration screen for the network interface you are configuring (see Related Screens, below).

Addresses are made up of a network portion and a node portion. The possible classes of network addresses have the following forms (Δ =a space):

Class C C Δ nnn.nnn.nnn Δ xxx
Class B B Δ nnn.nnn Δ xxx.xxx
Class A A Δ nnn Δ xxx.xxx.xxx

where nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address, and xxx is a value ranging from 0 to 255, representing the node portion of the address. The leftmost group of nnn has the following ranges for each address class:

Class C: 192-223
Class B: 128-191
Class A: 0- 127

Default Value: None

Related Screens:

- NETXPORT.NI.*niName*.PROTOCOL.IP

The network address (network portion of the IP address) configured in this screen must match the Neighbor Gateway IP Internet Address configured in the current screen.

**Configured Reachable
Networks IP Network
Address**

Enter the internet addresses of the remote networks that can be reached through the gateway whose network address is configured in the previous field. Only the internet portion of the network address is significant for this field (see above for valid formats of internet addresses). The node portion must be entered; however, it may be set to all zeros.

Related Screens:

- NETXPORT.NI.*niName*.INTERNET

This pathname corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

**Configured Reachable
Networks Hops**

Enter the internet hop count to the reachable network whose IP address is configured to the left of the Hops field. (The internet hop count is the number of full internet gateways that will be used to route a message to the destination network. If two partner gateway halves are used as part of the internet route, they are counted as one hop.)

Hop count is used internally to determine which neighbor gateway (if more than one exists) is on the shortest path to the remote network. If more than one gateway can reach a given remote network, and the number of hops to the remote network is equal for each gateway, you can specify which gateway the Network Transport will use by configuring an artificially high hop count. The Network Transport will always use the gateway with the lowest hop count.

If the same hop count value is configured for multiple gateways, then the Network Transport will choose internally from among the routes with equal hop counts.

Default Value: None

Range: 1-32767

NOTE

To delete a reachable network entry, fill the field to be deleted with blanks and press **Update Data**.

ROUTER MAPPING CONFIGURATION

The screen in Figure 10-12 is displayed when you press the function key for **Go To MAPPING** at the Router Network Interface Configuration Screen (Figure 10-1). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.MAPPING

in the command window of any screen and press ENTER, where the *niName* is the configured router NI name. The screen following this one allows you to configure a set of characteristics for a route from the local node to a remote node. Each set of route characteristics is referred to as a "mapping." The router node name entered on this screen is used to identify a mapping that is configured in the next screen. You must configure one mapping for each non-adjacent node that you want to reach through a link to a given adjacent node, as well as mappings for each adjacent node. There may be multiple routes to a destination node; if the routes are through different adjacent nodes, a mapping must be configured for each of them. For example, Figure 10-11 shows a router network that could have eight mappings configured at node A.

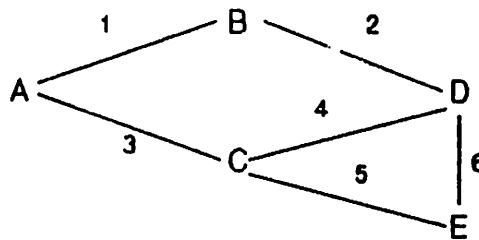


Figure 10-11. Configuring Mapping

If node A is the node being configured, mappings are needed for routes to both node B and node C, and for routes through nodes B and C to any other node. A mapping could be configured for each of the following routes (the rightmost node in these sets is the destination node):

Routes to adjacent nodes:

A-B (uses Link 1)
A-C (uses Link 3)

Routes to non-adjacent nodes through B:

A-B-D (uses Link 1)
A-B-D-E (uses Link 1)

Routes to non-adjacent nodes through C:

A-C-D (uses Link 3)
A-C-E (uses Link 3)

Alternate routes to adjacent nodes.

A-C-D-B (uses Link 3)
A-B-D-C (uses Link 1)

Note that it is not necessary to configure alternate routes to nodes B and C; however, you can configure the routes listed above (A-C-D-B and A-B-D-C) to allow for the possibility that the link used for the primary route becomes non-operational. Refer to the section "Non-Operational Links" in Section 3 of this manual for more information about alternate routes.

Router Network Interface Configuration

Use the fields and the function keys of this select screen to perform the desired action, as follows:

- To define a new mapping configuration, specify a name for the route (called a router node name on the screen); then press **Add**. The path for the selected route is added to the configuration file, and NMMGR displays a mapping data screen (called the Router Reachable Nodes screen). This screen must be configured to define the specified route.
- To modify an existing mapping configuration, specify the name of the route (router node name); then press **Update**. NMMGR displays the data screen corresponding to the specified name.
- To change the name of an existing mapping configuration, specify the existing router node name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Mappings.
- To delete an existing mapping configuration, specify the existing router node name; then press **Delete**. Press **Delete** again to confirm; otherwise, the deletion will not take effect. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Mappings.

NMMGR/3000 (X.05.06) ROUTER MAPPING CONFIGURATION
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path: NETXPORT.NI.niName.MAPPING

	Router Node Name
	New Name

Configured Mappings

--	--	--	--	--	--

File: filename.NET.SYS

Next Page	Prev Page	Delete	Rename	Add	Update	Refresh Screen	Prior Screen
-----------	-----------	--------	--------	-----	--------	----------------	--------------

Figure 10-12. Router Mapping Configuration Screen

Fields

Router Node Name

Enter a name to represent a route between the node you are configuring and another node on the router network. This name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

New Name

(Required only when renaming.) Enter a new router node name. This new name is used in place of the current name for an existing route. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

ROUTER REACHABLE NODES

The screen shown in Figure 10-13 is used to configure the route characteristics to a destination node on the router network. You must configure one mapping (i.e. one instance of this screen) for each node that you want to reach through a link to a given adjacent node, as well as mappings for each adjacent node. The name of the link connecting this node to the adjacent node is what you enter in the Link Name field of this screen.

Because at least one route should be defined to every other node on the network, this screen will be visited at least as many times as there are *other nodes* in the router network. There may be multiple routes to a non-adjacent destination node; if the routes are through different adjacent nodes, a mapping must be configured for each of them. The screen shown below is displayed when you select a router node name at the Router Mapping Configuration screen (Figure 10-12) and press **Add** or **Update**. It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.MAPPING.*mapentry*

in the command window of any screen and press **(ENTER)**, where *niName* is the configured router NI name, and *mapentry* is the router node name configured in the Router Mapping Configuration screen (Figure 10-12). You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data:** flag is set to **Y**.

MMGR/3000 (X.05.06) ROUTER REACHABLE NODES Data: N
 When Data Flag is "N", press "Update Data" to create the data record.
 Command:

Path: NETXPORT.NI.*niName*.MAPPING.*mapentry*

[] IP Internet Address

[] Link Name

[] Adjacent (0)/ Non-adjacent (1)

[50] Entry Priority

If Adjacent and DIAL Then:

[] Phone Number
 [HP] Security String

[N] Route Disabled (Y For Yes, N For No)

File: filename.NET.SYS

Figure 10-13. Router Reachable Nodes Screen

Fields

IP Internet Address

This is the internet address of the destination node to which a route is being defined.

Addresses are made up of a network portion and a node portion. The supported classes of network addresses have the following forms (Note: Δ = a space):

```
Class C   CΔ nnn.nnn.nnnΔxxx
Class B   BΔ nnn.nnnΔxxx.xxx
Class A   AΔ nnnΔxxx.xxx.xxx
```

where nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address, and xxx is a value ranging from 0 to 255, representing the node portion of the address. The leftmost group of nnn has the following ranges for each address class:

```
Class C:  192-223
Class B:  128-191
Class A:   0-127
```

If the link specified in the Link Name field is the only link configured for this network interface, you can enter a "wildcard" symbol by specifying an "at sign" (@) in place of the IP address. The @ in this field indicates that multiple non-adjacent router nodes on this network can be reached via this link (specified in the Link Name field). Using the @ wildcard enables you to configure this screen only once for all non-adjacent nodes reachable by the specified link. Use the @ only if the link specified is the only link for this network interface. The @ must be left-justified in the IP Internet Address field. Make sure you separately configure the mapping to the adjacent node from which the non-adjacent nodes can be reached.

For example, Figure 10-14 shows a router network. From node A, all other nodes on the network must be reached through node B. During configuration of node A, the @ could be entered to indicate that all communication to non-adjacent nodes originating from A must be routed through node B (over Link 1). In addition to this mapping, only one additional mapping would have to be configured at node A--the mapping from node A to the adjacent node B.

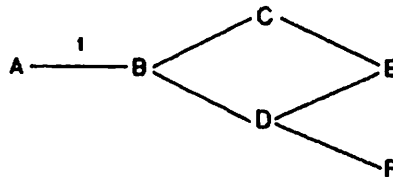


Figure 10-14. Using an @ for Mapping Configuration

Default Value: None

Router Network Interface Configuration

Link Name

The name of the link on this node over which packets to the destination node must be sent. The name of the link is configured separately (see related screens below).

Related Screens

- NETXPORT.NI.*niName*.LINK
This screen configures the link name.
- LINKCONF.*nilink*
This screen configures link attributes

Default Value: None

Adjacent/Non-adjacent

This field indicates whether the destination is an adjacent node to the node being configured (0) or if it is non-adjacent, i.e., the destination must be accessed through intermediate nodes (1).

Default Value: None

Range: 0 or 1

Entry Priority

This field is useful when alternate routes are configured to a destination node. It is the primary means of influencing the choice of route over the router network. Priority is considered before any other route characteristic (direct connect link, dial connection, number of hops, etc.) in choosing a route. Links having higher priority values are chosen over lower priority links.

A default value of 50 allows for the addition of either lower or higher priority nodes or routes.

Default Value: 50

Range: 1-99

Phone Number

This is the telephone number of the destination node. It is required if the destination is local and the link is a dial link. Enter the telephone number as a combination of decimal numbers (0 through 9), dashes, and the following special characters:

- / Separator used for automatic call units that have second dial-tone detect.
- E Optional end-of-number indicator.
- D One second delay (used for European modems and automatic call units that require built-in delays).
- # Defined by local phone system.
- * Defined by local phone system.

Enter ! to disable outbound dialing. A ! is required if the destination node is a personal computer.

Default Value: None

Security String

This is the security string of the destination node. It is relevant only if all of the following are true: the destination is local, the link is a dial link, DIAL ID protocol is enabled, and security is enabled. It is ignored when security is not enabled at the local node.

The security string can contain as many as eight alphanumeric characters. It must be left justified and contain no embedded blanks.

Related Screens:

- NETXPORT.NI.*niName*.LINK.*nilink*
Dial ID protocol is enabled/disabled on this screen.
- NETXPORT.NI.*niName*.PROTOCOL.DIAL
Security validation is enabled/disabled on this screen.

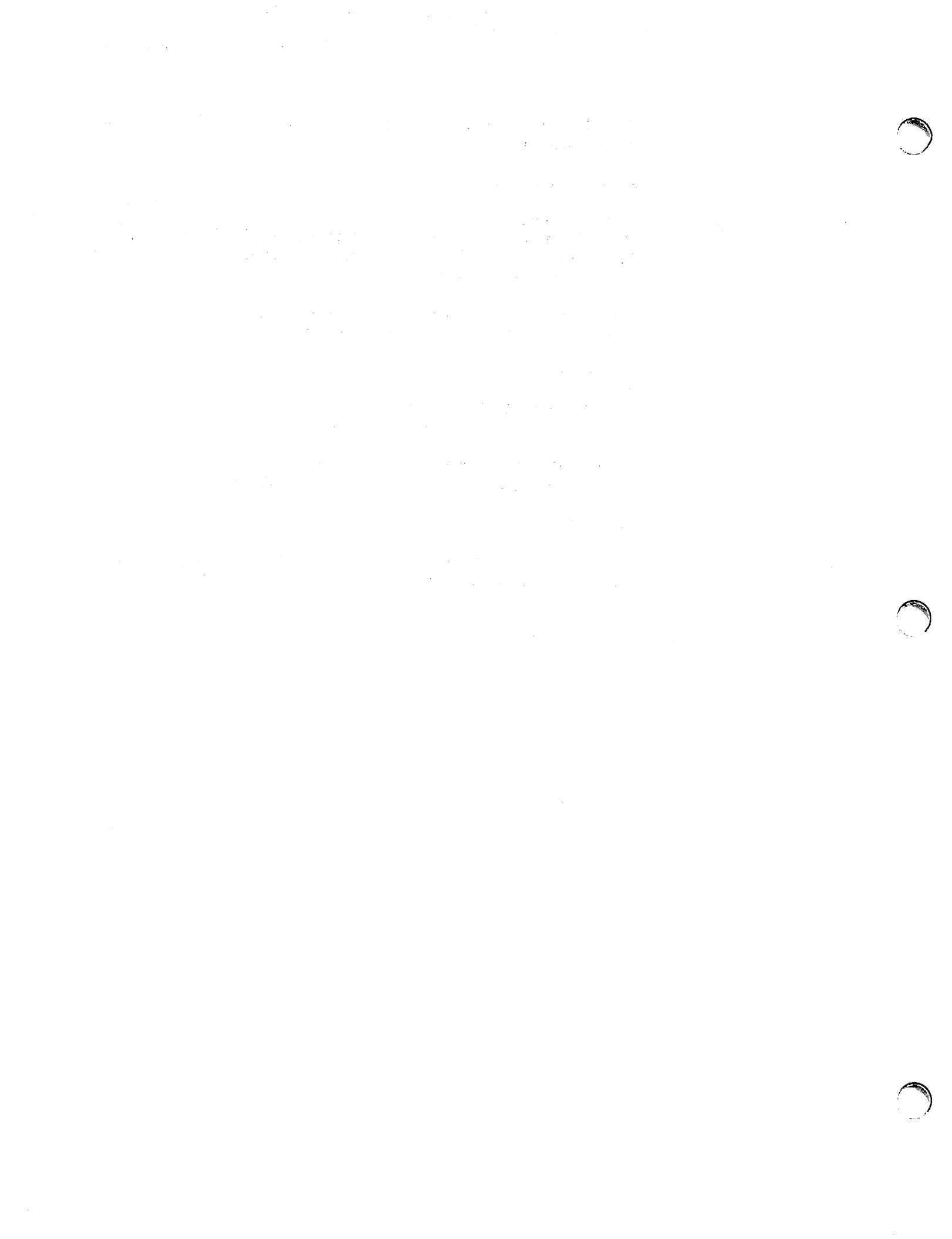
Default Value: HP

Route Disabled

This field may be used to disable routing to the remote node. This might be useful if you are testing another link, and want to temporarily disable this one.

Default Value: N

Range: Y or N



GATEWAY HALF NETWORK INTERFACE CONFIGURATION

SECTION

11

The screens described in this section are used for configuring a node with a gateway half network interface.

There are three main branches of gateway half network interface configuration. These are reached by choosing different function keys displayed on the first screen, called the GATEWAY HALF NETWORK INTERFACE CONFIGURATION screen. All of the gateway half network interface configuration screens are listed below, with their places in the configuration tree indicated by indentation.

GATEWAY HALF NETWORK INTERFACE CONFIGURATION - This screen enables you to configure information about a gateway half network interface, such as the number of inbound and outbound buffers. From this screen, you can proceed to one of three branches of gateway half NI configuration: protocol configuration, link configuration, and internet configuration.

PROTOCOL CONFIGURATION - You will reach this screen if you press **Go To PROTOCOL** on the GATEWAY HALF NETWORK INTERFACE CONFIGURATION screen. This screen allows you to choose to proceed to either IP or DIAL protocol configuration.

IP PROTOCOL CONFIGURATION - This screen, which you will reach by pressing **Go To IP** on the previous screen, enables you to configure the number of store and forward buffers for the network interface, the partner gateway half's IP address, and tuning parameters for the IP protocol.

DIAL ID PROTOCOL CONFIGURATION - This screen enables you to configure information about a dial link that is used by the Dial ID protocol--retransmission information, and whether security is in effect.

SECURITY STRING(S) CONFIGURATION - This screen allows you to specify the security strings used by the Dial ID protocol.

GATEWAY HALF NETWORK INTERFACE LINK - This screen, which you will reach by pressing **Go To LINK** on the GATEWAY HALF NETWORK INTERFACE CONFIGURATION screen, allows you to specify the name of the link (as previously configured in the LINK CONFIGURATION screen), and whether the link is a direct dial link or a direct connect link.

DIRECT CONNECT LINK CONFIGURATION - This screen, which NMMGR displays when you specify a direct connect link in the previous screen, allows you to enter information pertaining to the direct connect link.

GATEWAY HALF DIAL LINK CONFIGURATION - This screen, which NMMGR displays when you specify a direct dial link in the previous screen, allows you to enable or disable the Dial ID protocol.

NEIGHBOR GATEWAYS - This screen, which you will reach by pressing **Go To INTERNET** on the GATEWAY HALF NETWORK INTERFACE CONFIGURATION screen, permits you to specify a gateway name to represent the node's partner gateway half.

NEIGHBOR GATEWAY REACHABLE NETWORKS - This screen provides data about the networks that can be reached through the partner gateway half specified on the previous screen.

NOTE

Configurable fields described in this manual are required unless otherwise stated.

Fields described as "HP modifiable" should be changed only upon the recommendation of your HP representative.

On the screens shown in this section, fields that must be configured when performing guided configuration are underlined.

GATEWAY HALF NETWORK INTERFACE CONFIGURATION

The gateway-half network interface (NI) interfaces the upper layers of the transport protocol to the data link layer. The screen shown in Figure 11-1 supplies the information required for that interface. The screen is displayed when you select an NI name and the NI type GATEHALF at the Network Interface Configuration screen (Figure 8-9) and press **F5** **Add** or **F6** **Update**. It is also displayed when you type the path name:

@.NETXPORT.NI.*niName*

in the command window of any screen and press **ENTER**, where the *niName* is the configured gateway-half NI name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

From this screen you proceed to the screens used to configure the gateway-half network interface.

```

NNMGR/3000 (X.05.06) GATEWAY HALF NETWORK INTERFACE CONFIGURATION      Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path:  NETXPORT.NI.niName

[256]  Number Of Inbound Buffers
[256]  Number Of Outbound Buffers
[    ]  Idle Device Timeout Value (Minutes)
        0 = Timer Disabled For All Devices

File:  filename.NET.SYS

Go To  Go To  Go To
PROTOCOL LINK  INTERNET

Update  Refresh  Prior
Data   Screen  Screen
  
```

Figure 11-1. Gateway-Half Network Interface Configuration Screen

Fields

Number of Inbound Buffers

This field specifies the number of buffers to be allocated for inbound data. Buffer configuration is based on the number of TCP connections that will use a given network interface. An allocation of two buffers per connection will suffice for typical usage.

The default value is based on the assumption that the Network Manager desires to allow no more than the default number of TCP connections (128) to use the gateway-half NI (see Related Screens, below). Hence the default is $128 * 2 = 256$ inbound buffers. When there is more than one NI, this value should probably be adjusted downward, since the connections might reasonably be expected to be spread over all the NIs rather than be concentrated over only one NI. If the number of TCP connections is changed from the default value, the number of inbound buffers for all NIs should be reconsidered.

Whenever there are not enough buffers to support inbound traffic, an IP log message will indicate that the node is congested and the packet had to be discarded. (See the *NS3000/V Error Message and Recovery Manual* for the exact IP log location and message.) Repeated occurrence of this log message indicates that more inbound buffers should be configured.

Related Screens:

- NETXPORT.GPROT.TCP

The maximum number of TCP Connections is configured here. The default value is 128.

Default Value: 256

Range: 32-2048

Number of Outbound Buffers

This field specifies the number of buffers to be allocated for outbound data. Outbound buffers are used for outbound data packets and are held by the transport until acknowledged by the destination. Not allocating enough outbound buffers may adversely affect TCP throughput. Calculation of the default value is the same as described above for inbound buffers.

Related Screens:

-NETXPORT.GPROT.TCP

The default value for maximum TCP connections is configured here. If it is increased, the number of outbound buffers must also be increased.

Default: 256

Range: 32-2048

**Idle Device
Timeout Value (Mins)**

If the Idle Device Timer has been enabled (see related screens below), and if there is no activity during this time interval, the device is considered to be inactive and will be shutdown. A timeout value of zero disables the Idle Device Timer for the link on this network interface. The Idle Device timer is useful for shutting down dial links that have become idle. This field is relevant if the link is a dial link.

Related Screens:

- NETXPORT.NI.niname.LINK.linkname

Enables/disables Idle Device Timer for the device.

- NETXPORT.GPROT.TCP

The Connection Assurance Interval set in this screen must be less than the Idle Device Timeout value configured in the current screen. Note that one value (Connection Assurance) is configured in seconds, the other (Idle Device Timeout) is configured in minutes. You must convert to the same units to compare the values.

Default Value: None

Range: 0-720

PROTOCOL CONFIGURATION

The menu screen in Figure 11-2 is displayed when you press the function key for **Go To PROTOCOL** at the gateway-half Network Interface Configuration screen (Figure 11-1). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.PROTOCOL

in the command window of any screen and press **(ENTER)**, where *niName* is the configured gateway-half NI name.

For the gateway-half NI, you must configure the IP protocol. The Dial protocol must be configured only if you have any switched lines. The **(F1) Go To IP** and **(F2) Go To DIAL** function key labels are displayed.

MMGR/3000 (X.05.06) PROTOCOL CONFIGURATION
Select the next screen and press the corresponding function key.
Command:

Path: NETXPORT.NI.*niName*.PROTOCOL

IP - Configure Internet Protocol
PROBE - Configure PROBE Protocol (LAN Only)
DIAL - Configure DIAL Protocol (Router/Gateway Half Only)
Necessary Only If There Are Any Switched Links

File: filename.NET.SYS

Go To IP **Go To DIAL** **Refresh Screen** **Prior Screen**

Figure 11-2. Protocol Configuration Screen

Choose the protocol to configure and press the corresponding function key.

INTERNET PROTOCOL CONFIGURATION

Internet Protocol information must be supplied for each configured NI. The key field in the screen in Figure 11-3 is the IP Internet Address, which is used in IP routing and datagram delivery algorithms. Data in the other fields are used for internal resource allocation and performance tuning.

The IP Protocol screen is displayed when you press the function key for **Go To IP** at the Protocol Configuration screen (Figure 11-2). It is also displayed when you type the path name:

```
@NETXPORT.NI.niName.PROTOCOL.IP
```

in the command window of any screen and press **ENTER**, where *niName* is the configured gateway-half NI name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

MMGR/3000 (X.05.06) IP PROTOCOL CONFIGURATION		Data: N
When Data Flag is "N", press "Update Data" to create the data record.		
Command:		
Path:	NETXPORT.NI.niName.PROTOCOL.IP	
[20]	Store & Forward Buffers	(Enter 0 To Disable Store & Forward)
[]	IP Internet Address	
[4]	Internal Message Queue Length	
[20]	Fragment Assembly Queue Elements	
File:	filename.NET.SYS	
	Update Data	Refresh Screen
		Prior Screen

Figure 11-3. IP Protocol Configuration Screen

Fields

Store & Forward Buffers

(HP modifiable.) This field allocates buffers to support store-and-forward over the network interface being configured.

You must allocate store-and-forward buffers for all gateway half network interfaces.

This number of store-and-forward buffers is configurable to allow performance tuning for different network types. However, HP recommends that you use the default number of store-and-forward buffers (20), and that you consult your HP representative before modifying this value.

Default Value: 20

Range: 0-50

IP Internet Address

Enter the internet protocol (IP) address for the network interface being configured.

Because you are configuring a gateway half NI, enter the IP address of this gateway half's *partner* gateway half. This is the IP address of the network for which the partner serves as a gateway half. In other words, the address to enter is the network address of the partner's home network.

Addresses are made up of a network portion and a node portion. The supported classes of network addresses have the following forms:

Class C	CΔnnn.nnn.nnnΔxxx
Class B	BΔnnn.nnnΔxxx.xxx
Class A	AΔnnnΔxxx.xxx.xxx

where Δ denotes a blank, and nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address. The leftmost group of nnn has the following ranges for each address class:

Class C:	192-223
Class B:	128-191
Class A:	0-127

Where xxx is a value ranging from 0 to 255, representing the node portion of the address.

Default Value: None

**Internal Message
Queue Length**

(HP modifiable.) This field puts a limit on the number of internal resources that the IP protocol may hold while awaiting some other protocol module action. It is a tuning parameter that should be modified only upon the recommendation of your HP representative.

The default is set to handle most cases; if it is too low for your network, packets will be discarded and you will receive a logging error message. Consult the *NS3000/V Error Message and Recovery Manual* for the specific log message.

Default value: 4

Range: 0-20

**Fragment Assembly
Queue Elements**

(HP modifiable.) This field specifies the maximum number of incomplete message fragments that this IP protocol may hold.

HP recommends that you use the default of 20 for this field. For purposes of tuning your network's performance, and upon the recommendation of your HP representative, you may wish to alter the number of Fragment Assembly Queue Elements.

You may wish to configure a higher value if traffic conditions on your network are less than optimal; e.g., if internet routes are heavily loaded and intermediate nodes are congested. If conditions on your network are less busy, you may wish to configure a lower value. Only configure 0 if no fragmented messages will ever be received by the node you are configuring.

If message fragments are discarded, (indicating that the value configured in this field is too low) a log message will be recorded. Refer to the *NS3000/V Error Message and Recovery Manual* for a description of the message you receive.

Default value: 20

Range: 0-100

DIAL ID PROTOCOL CONFIGURATION

Along with other protocol information, the Dial ID Protocol Configuration screen provides a means of verifying that the remote node is indeed the intended remote node and that both local and remote nodes have proper security access. This screen, shown in Figure 11-4, is displayed when you press **[F2]** for **Go To DIAL** at the Protocol Configuration screen (Figure 11-2). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.PROTOCOL.DIAL

in the command window of any screen and press **[ENTER]**, where *niName* is the configured gateway-half NI name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

MMGR/3000 (X.05.06) DIAL ID PROTOCOL CONFIGURATION          Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:
Path: NETXPORT.NI.niName.PROTOCOL.DIAL

[2]      Maximum Retransmissions Per Packet
[5]      Retransmission Timeout (Secs)
[Y]      Security On (Y/N)

File: filename.NET.SYS

Go To SECURITY  Update Data  Refresh Screen  Prior Screen
    
```

Figure 11-4. Dial Protocol Configuration Screen

Fields

Maximum Retransmissions Per Packet

(HP modifiable.) This is the maximum number of times that a Dial ID Protocol packet will be retransmitted. If the expected response to a packet is not received after this number of retransmissions, the link device it is

using is closed. This value is related to the Retransmission Timeout value discussed below. Multiplying these values results in the total time that passes before a failure is reported (an error message will be recorded).

HP recommends that you alter this value only upon the recommendation of your HP representative. However, note that if the value is set too low, dial connections may fail unnecessarily when response times are temporarily slowed by transient conditions such as an abnormally high volume of traffic. The higher the value, the longer it will take to be notified of a link failure if one occurs.

Default Value: 2

Range: 1-10

**Retransmission
Timeout (Secs)**

(HP modifiable.) The Retransmission Timeout is the time interval that passes between retransmissions of a Dial ID protocol packet.

Multiplying the values configured for Maximum Number of Retransmissions Per Packet (described above) and Retransmission Timeout results in the total time that passes before a failure is reported (an error message will be recorded).

HP recommends that you alter this value only upon the recommendation of your HP representative. However, note that if the value is set too low, dial connections may fail unnecessarily when response times are temporarily slowed by transient conditions such as an abnormally high volume of traffic. The higher the value, the longer it will take to be notified of a link failure if one occurs.

Default Value: 5

Range: 1- 10

Security On (Y/N)

A Y (Yes) value in this field indicates that security strings are to be exchanged and validated between the node being configured and a remote node.

When a dial connection is initiated by a remote node, the security string sent by the remote node is checked against the list of valid security strings configured for the Dial ID Protocol for this network interface. (See Related Screens, below).

When a dial connection is initiated by this node, the local Dial ID protocol sends the destination's security string (as configured on this node) to that node. (Related Screens, below, indicates the pathname of the screen in which you can configure security strings.)

If security validation fails, an error message is logged, where PARM indicates whether the failure was local or remote. (See the *NS3000/V Error Message and Recovery Manual* for a description of any error message

Gateway Half Network Interface Configuration

received.

Related Screens:

- NETXPORT.NI.*niName*.PROTOCOL.DIAL.SECURITY
Security Strings valid for this network are configured in this screen.
- NETXPORT.NI.*niName*.MAPPING.*mapentry*
The remote node's security string is configured in this screen.

Default Value: Y

Range: Y or N

SECURITY STRING(S) CONFIGURATION

The Security String(s) Configuration screen supplies the security string required by the Dial ID protocol for the node you are configuring. (Note that the security string is not required if Dial ID protocol is not enabled.) This screen, shown in Figure 11-5, is displayed if you press **F1** **Go to SECURITY** on the preceding Dial ID Protocol Configuration screen (Figure 11-4). It is also displayed when you type

`@NETXPORT.NI.niName.PROTOCOL.DIAL.SECURITY.`

in the command window of any screen and press **ENTER**, where *niName* is the configured gateway-half NI name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

NNMGR/3000 (X.05.06)
SECURITY STRING(S) CONFIGURATION
Data: N

When Data Flag is "N", press "Update Data" to create the data record.

Command:

Path: NETXPORT.NI.niName.PROTOCOL.DIAL.SECURITY

Configured Security Strings

[HP]	[]	
[]	[]	
[]	[]	
[]	[]	

File: filename.NET.SYS

Update
Data

Refresh
Screen

Prior
Screen

Figure 11-5. Security String Configuration Screen

11-13

Fields

Configured Security Strings

Enter the security string that remote nodes must use to gain dial link access to the node you are configuring. The string can contain up to eight alphanumeric characters, left justified, with no embedded blanks.

Default Value: HP

Related Screen:

- NETXPORT.NI.*niName*.LINK.*niLink*

The Dial ID protocol is enabled/disabled on this screen.

NOTE

To delete a security string, blank out the field that contains the string you want deleted, and press **Update Data**.

GATEWAY HALF NETWORK INTERFACE LINK

The select screen in Figure 11-6 is displayed when you press **F2** **Go To LINK** at the Gateway Half Network Interface Configuration screen (Figure 11-1). It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.LINK

in the command window of any screen and press **ENTER**, where *niName* is the configured gateway half link network interface name.

Use the fields of this select screen in combination with the function keys to perform the desired action.

- To define a new link configuration, specify the link name; then press **F5** **Add**. The path for the selected link name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing link configuration, specify the link name; then press **Update**. The data screen on the path for the specified link is displayed.
- To change the link name of an existing link configuration, specify the link name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Network Links.
- To delete an existing link configuration, use the delete key. Specify the link name, then press **Delete**; when NMMGR prompts you for confirmation, press **Delete** again. The previously configured name is deleted and is no longer displayed in a display field under the labeled Configured Network Links.

```

NNMGR/3000 (X.05.06) GATEWAY HALF NETWORK INTERFACE LINK
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path: NETXPORT.NI.niName.LINK

[ ] Link Name
[ ] New Name

Types: DD - Direct Dial
       DC - Direct Connect
       (if new)

Configured Network Links

Name      Type      Name      Type      Name      Type
[ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ] [ ]

File: filename.NET.SYS

Next Page  Prev Page  Delete  Rename  Add  Update  Refresh Screen  Prior Screen
    
```

Figure 11-6. Network Interface Links Screen

Fields

Link Name

Enter the link name from the link configuration of a gateway half; this enables the Network Transport to associate the correct link with the gateway half network interface. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

The link name is used by the Network Transport when establishing connections and *must* match the link name configured for the link configuration of a gateway half.

Note that only one gateway-half NI may be configured per network.

Types

Enter DD for a direct dial link, or DC for a direct connect link.

New Name

Enter a link name. This new link name is used in place of the current link name for an existing link configuration. The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

DIRECT CONNECT LINK CONFIGURATION

The Direct Connect Link Configuration screen supplies the information required to interface a gateway-half NI to a non-dial link (that is, a leased line or a hardwired connection). This screen, shown in Figure 11-7, is displayed when you select an NI link name and the link type DC at the Gateway Half Network Interface Link screen (Figure 11-6) and press **Add** or **Update**. It is also displayed when you type the path name:

@NETXPORT.NI.*niName*.LINK.*nilink*

in the command window of any screen and press **ENTER**, where *niName* is the configured gateway-half NI name, and *nilink* is the configured gateway-half NI link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **N**.

NNNGR/3000 (X.05.06) DIRECT CONNECT LINK CONFIGURATION		Data: N
When Data Flag is "N", press "Update Data" to create the data record.		
Command:		
Path:	NETXPORT.NI. <i>niName</i> .LINK. <i>nilink</i>	
<input type="checkbox"/>	Start Device On Network Initialization (Y/N)	
<input type="checkbox"/>	Enable Idle Device Timer	
File: filename.NET.SYS		
<input type="button" value="F5"/>	<input type="button" value="F6"/>	<input type="button" value="F7"/>
<input type="button" value="F8"/>	<input type="button" value="F9"/>	<input type="button" value="F10"/>
<input type="button" value="F11"/>	<input type="button" value="F12"/>	<input type="button" value="F13"/>
<input type="button" value="F14"/>	<input type="button" value="F15"/>	<input type="button" value="F16"/>
<input type="button" value="F17"/>	<input type="button" value="F18"/>	<input type="button" value="F19"/>
<input type="button" value="F20"/>	<input type="button" value="F21"/>	<input type="button" value="F22"/>
<input type="button" value="F23"/>	<input type="button" value="F24"/>	<input type="button" value="F25"/>
<input type="button" value="F26"/>	<input type="button" value="F27"/>	<input type="button" value="F28"/>
<input type="button" value="F29"/>	<input type="button" value="F30"/>	<input type="button" value="F31"/>
<input type="button" value="F32"/>	<input type="button" value="F33"/>	<input type="button" value="F34"/>
<input type="button" value="F35"/>	<input type="button" value="F36"/>	<input type="button" value="F37"/>
<input type="button" value="F38"/>	<input type="button" value="F39"/>	<input type="button" value="F40"/>
<input type="button" value="F41"/>	<input type="button" value="F42"/>	<input type="button" value="F43"/>
<input type="button" value="F44"/>	<input type="button" value="F45"/>	<input type="button" value="F46"/>
<input type="button" value="F47"/>	<input type="button" value="F48"/>	<input type="button" value="F49"/>
<input type="button" value="F50"/>	<input type="button" value="F51"/>	<input type="button" value="F52"/>
<input type="button" value="F53"/>	<input type="button" value="F54"/>	<input type="button" value="F55"/>
<input type="button" value="F56"/>	<input type="button" value="F57"/>	<input type="button" value="F58"/>
<input type="button" value="F59"/>	<input type="button" value="F60"/>	<input type="button" value="F61"/>
<input type="button" value="F62"/>	<input type="button" value="F63"/>	<input type="button" value="F64"/>
<input type="button" value="F65"/>	<input type="button" value="F66"/>	<input type="button" value="F67"/>
<input type="button" value="F68"/>	<input type="button" value="F69"/>	<input type="button" value="F70"/>
<input type="button" value="F71"/>	<input type="button" value="F72"/>	<input type="button" value="F73"/>
<input type="button" value="F74"/>	<input type="button" value="F75"/>	<input type="button" value="F76"/>
<input type="button" value="F77"/>	<input type="button" value="F78"/>	<input type="button" value="F79"/>
<input type="button" value="F80"/>	<input type="button" value="F81"/>	<input type="button" value="F82"/>
<input type="button" value="F83"/>	<input type="button" value="F84"/>	<input type="button" value="F85"/>
<input type="button" value="F86"/>	<input type="button" value="F87"/>	<input type="button" value="F88"/>
<input type="button" value="F89"/>	<input type="button" value="F90"/>	<input type="button" value="F91"/>
<input type="button" value="F92"/>	<input type="button" value="F93"/>	<input type="button" value="F94"/>
<input type="button" value="F95"/>	<input type="button" value="F96"/>	<input type="button" value="F97"/>
<input type="button" value="F98"/>	<input type="button" value="F99"/>	<input type="button" value="F100"/>

Figure 11-7. Direct Connect Link Configuration Screen

Fields

**Start Device
On Network
Initialization (Y/N)**

A Y (Yes) value means that the device is to be started when a NETCONTROL START command is issued for the network interface being configured. An N (No) means that a NETCONTROL ADDLINK command must be used to start the device.

Default Value: Y

Range: Y or N

**Enable Idle
Device Timer**

This field specifies whether the device is to be disconnected automatically if no packets have been received or transmitted over the link during a specified time period. This field is relevant only if a timeout value has been entered in the network interface screen listed below

Related screens:

- NETXPORT.NI.*niName*

The Idle Device Timeout value is configured on this screen.

Default Value: N

Range: Y or N

GATEWAY HALF DIAL LINK CONFIGURATION

Dial link configuration provides the information necessary to interface the gateway-half NI to a dial link. This screen, shown in Figure 11-8, is displayed when you select an NI link name and link type DD at the Gateway Half Network Interface Link screen (Figure 11-6) and press **Add** or **Update**. It is also displayed when you type the path name:

```
@NETXPORT.NI.niName.LINK.nilink
```

in the command window of any screen and press , where *niName* is the configured gateway-half NI name, and *nilink* is the configured gateway-half NI link name.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

```

NNMGR/3000 (X:05.06) GATEWAY HALF DIAL LINK CONFIGURATION           Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:
Path: NETXPORT.NI.niName.LINK.nilink

 Enable DIAL ID Protocol (Y/N)
 Phone Number
 Security String
 Start Device On Gateway Half Initialization (Y/N)
 Enable Idle Device Timer (Y/N)

File: filename.NET.SYS

```

Figure 11-8. Gateway Half Dial Link Configuration Screen

Fields

Enable Dial ID Protocol

A Y (Yes) value activates the Dial ID Protocol for a dial link. The Dial ID protocol verifies the identity of a remote node and insures that both local and remote nodes have the required security access.

The Dial ID Protocol should be disabled (by entering N [NO]) only to connect a dial link to a remote node that does not support the Dial ID Protocol (that is, a non-HP node).

Related Screens:

- NETXPORT.NI.*niName*.LINK
Configures a link name and type. Is on path to this screen.
- NETXPORT.NI.*niName*.PROTOCOL.DIAL.SECURITY
Configures security strings for this node.

Default Value: Y

Range: Y or N

Phone Number

This is the telephone number of this node's partner gateway half. Enter the telephone number as a combination of decimal numbers (0 through 9), dashes, and the following special characters:

/ Separator used for automatic call units that have second dial-tone detect.

E Optional end-of-number indicator.

D One second delay (used for European modems and automatic call units that require built-in delays).

Defined by local phone system.

* Defined by local phone system.

Enter ! to disable outbound dialing. A ! is required if the destination node is a personal computer.

Default Value: None

Security String

This is the security string of this node's partner gateway half. It is relevant if and the Dial ID protocol is enabled and security is enabled. The security screen can contain as many as eight alphanumeric characters. It must be left justified and contain no embedded blanks.

Related Screens:

- NETXPORT.NI.*gatename*.LINK.*linkname*
Dial ID protocol is enabled/disabled here
- NETXPORT.NI.*gatename*.PROTOCOL.DIAL
Security validation is enabled/disabled here.

Default Value: HP

Start Device

A Y (Yes) value means that the device is to be started when a NETCONTROL START command is issued for this network interface. A N (No) means that a NETCONTROL ADDLINK command must be used to start the device.

Default Value: Y

Range: Y or N

**Enable Idle
Device Timer**

This field specifies whether the device is to be disconnected automatically if no packets have been received or transmitted over the link during a specified time period. It is relevant only if a nonzero timeout value has been entered in the Gateway Half NI screen (see related screens below).

Related Screens:

- NETXPORT.NI.*niName*

Configures router network interface information. The value configured for the Idle Device Timeout is configured on this screen.

Default Value: Y

Range: Y or N

NEIGHBOR GATEWAYS

The select screen in Figure 11-9 is displayed when you press the function key for **Go To INTERNET** at the Gateway-Half Network Interface Configuration screen (Figure 11-1). It is also displayed when you type the path name:

`@NETXPORT.NI.niName.INTERNET`

in the command window of any screen and press **(ENTER)**, where the *niName* is the configured gateway-half NI name.

Use the fields and the function keys of this select screen to perform the desired action.

- To define a new gateway configuration, specify the gateway name; then press **Add**. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed.
- To modify an existing gateway configuration, specify the gateway name; then press **Update**. The data screen on the path for the specified gateway is displayed.
- To change the gateway name of an existing gateway configuration, specify the gateway name and a new name; then press **Rename**. The previously configured name is replaced, and the screen displays the new name in a display field under the label Configured Gateways.
- To delete an existing gateway configuration, use the delete key. Specify the gateway name, then press **Delete**; when NMMGR prompts you for confirmation, press **Delete** again. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Gateways.

NMGR/3000 (X.05.06) NEIGHBOR GATEWAYS
 Type in name of item to Update, Delete, or Rename; or Add a new item.
 Command:

Path: NETXPORT.NI.niName.INTERNET

Gateway Name
 New Name

Configured Gateways

--	--	--	--	--	--

File: filename.NET.SYS

Figure 11-9. Neighbor Gateways Screen

Fields

Gateway Name

Enter a name to represent this node's partner gateway half, through which one or more remote networks can be reached. A gateway name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

New Name

(Required only when renaming.) Enter a gateway name to represent this node's partner gateway half. This new gateway name is used in place of the current gateway name for an existing gateway configuration. The name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

NOTE

The information configured in this screen can extend to more than 1 page, if necessary, to allow configuration of more than 10 reachable networks. Press **Next Page** to proceed to a new page. Press **Prev Page** to display a prior page. Use **First Page** to display the first page (for example, if you are viewing the third page, pressing **First Page** will immediately display the first page). Press **Last Page** to display the last page of reachable networks that has been configured. To consolidate reachable networks entries, press **Condense Data**.

Fields**Neighbor Gateway
IP Internet Address**

Enter the IP address of this node's partner gateway half. This is the IP address of the partner's home network, and is the same IP address that you have already configured in the Internet Protocol Configuration screen for the current NI.

Addresses are made up of a network portion and a node portion. The possible classes of network addresses have the following forms (Δ=a space):

```
Class C   CΔnnn.nnn.nnnΔxxx
Class B   BΔnnn.nnnΔxxx.xxx
Class A   AΔnnnΔxxx.xxx.xxx
```

where nnn is a value ranging from 0 to 255, representing eight bits of the network portion of an address, and xxx is a value ranging from 0 to 255, representing the node portion of the address. The leftmost group of nnn has the following ranges for each address class:

```
Class C:  192-223
Class B:  128-191
Class A:   0-127
```

Default Value: None

Related Screens:

- NETXPORT.NI.niNamePROTOCOL.IP

The network address (network portion of the IP address) configured in this screen must match the Neighbor Gateway IP Internet Address configured in the current screen.

**Configured Reachable
Networks IP Network
Address**

Enter the internet addresses of the remote networks that can be reached through the gateway half whose network address is configured in the previous field. (Enter one address per line.) Only the internet portion of the network address is significant for this field (see the description of the Neighbor Gateway IP Internet Address field for valid formats of internet

Gateway Half Network Interface Configuration

addresses). The node portion must be entered; however, it may be set to all zeros.

Configured Reachable Networks Hops

Enter the internet hop count to the reachable network whose IP address is configured to the left of the Hops field. (The internet hop count is the number of full internet gateways that will be used to route a message to the destination network. If two partner gateway halves are used as part of the internet route, they are counted as one hop.)

Hop count is used internally to determine which neighbor gateway (if more than one exists) is on the shortest path to the remote network. If more than one gateway can reach a given remote network, and the number of hops to the remote network is equal for each gateway, you can determine which gateway the Network Transport will use by configuring an artificially high hop count. The transport always uses the gateway with the smallest hop count.

If the same hop count value is configured for multiple gateways, then the Network Transport will choose internally from among the routes with equal hop counts.

Default Value: None

Range: 1-32767

NOTE

To delete a reachable network entry, fill the field to be deleted with blanks and press **Update Data**.

LOOPBACK NETWORK INTERFACE CONFIGURATION

SECTION

12

The screens described in this section are used for configuring the loopback network interface. There is only one branch of loopback network interface configuration. This is the protocol configuration branch, which can be reached by pressing the **Go To PROTOCOL** key on the LOOPBACK NETWORK INTERFACE CONFIGURATION SCREEN. All of the loopback network interface configuration screens are listed below, with their places in the configuration tree indicated by indentation.

LOOPBACK NETWORK INTERFACE CONFIGURATION - This screen enables you to configure information about a loopback network interface, such as network segment size and the number of buffers to be allocated for loopback. From this screen, you can proceed to the protocol configuration branch.

PROTOCOL CONFIGURATION - You will reach this screen if you press **Go To PROTOCOL** on the LOOPBACK NETWORK INTERFACE CONFIGURATION screen. This screen allows you to choose to proceed to IP protocol configuration.

IP PROTOCOL CONFIGURATION - This screen, which you will reach by pressing **Go To IP** on the previous screen, contains loopback default values which should not be changed.

NOTE

Configurable fields described in this manual are required unless otherwise stated.

Fields described as "HP modifiable" should be changed only upon the recommendation of your HP representative.

On the screens shown in this section, fields that must be configured when performing guided configuration are underlined.

LOOPBACK NETWORK INTERFACE CONFIGURATION

The screen in Figure 12-1 is displayed when you select an NI name and the NI type LOOP at the Network Interface Configuration Screen (Figure 8-9) and press **Add** or **Update**. It is also displayed when you type the path name:

`@.NETXPORT.NI.niName`

in the command window of any screen and press **ENTER**, where the *niName* is the configured loopback NI name.

Whenever a transport user makes a connection to a user process on the same node, all outbound packets on this connection are turned around at the NI level and passed back up through the protocol stack to the destination user. This screen supplies information necessary for this operation, performed by the Loopback NI.

You must press **Update Data** to transfer the data displayed on the screen to the configuration file you are creating or updating. You verify that the data record has been created by checking that the **Data** flag is set to **Y**.

From this screen you proceed to other screens used to configure the loopback network interface.

```
MMNGR/3000 (X.05.06) LOOPBACK NETWORK INTERFACE CONFIGURATION      Data: N
When Data Flag is "N", press "Update Data" to create the data record.
Command:

Path: NETXPORT.NI.niName

[1024] Network Segment Size (Bytes)
[256]  Number Of Buffers

File: filename.NET.SYS

[Go To] [      ] [      ] [      ] [      ] [Update] [Refresh] [Prior]
[PROTOCOL] [      ] [      ] [      ] [      ] [Data] [Screen] [Screen]
```

Figure 12-1. Loopback Network Interface Configuration Screen

Press the **Go To PROTOCOL** function key.

Fields

Network Segment Size

(HP modifiable) This is the size of the physical buffer for the loopback network interface. No fragmenting or fragment assembly is performed on the loopback NI. There is no limitation that only single physical buffers (not chained buffers, for example) can be passed across the I/O interface to the board, because outbound data is turned around at the NI layer. Therefore, if user data exceeds the physical buffer size, it is put into logical buffers (chained physical buffers) that are the size of the user data.

Default value: 1024

Range: 1024-4224

Number Of Buffers

This field specifies the number of buffers to be allocated for loopback. For the loopback NI, there is no differentiation between outbound and inbound buffers because an outbound buffer, when it is turned around at the NI level, becomes an inbound buffer. As with other network types, buffer configuration is based on the number of TCP connections that will use the network interface. An allocation of two buffers per connection will suffice for typical usage.

The default value is based on the assumption that the Network Manager desires to allow no more than the default number of TCP connections (see related screens below) to use the Loopback NI. Therefore, the default is 128 (default TCP connections) * 2 = 256 buffers. When there is more than one NI, this value should probably be adjusted downward because the connections might reasonably be expected to be spread over all the NIs rather than be concentrated over only one NI. If you change the number of TCP connections from the default value, you should reconsider the number of inbound buffers for all NIs.

Related Screens

NETXPORT.GPROT.TCP

Maximum Number of Connections (default value of 128) is configured on this related screen.

Default value: 256

Range: 32-2048

PROTOCOL CONFIGURATION

The menu screen in Figure 12-2 is displayed when you press the function key for **Go To PROTOCOL** at the Loopback Network Interface Configuration Screen (Figure 12-1). It is also displayed when you type the path name:

`@NETXPORT.NI.niName.PROTOCOL`

in the command window of any screen and press **ENTER**, where *niName* is the configured loopback NI name.

For the loopback NI, you must configure the IP protocol. The **Go To IP** function key label is displayed.

NMMGR/3000 (X.05.06) PROTOCOL CONFIGURATION
Select the next screen and press the corresponding function key.
Command:

Path: NETXPORT.NI.niName.PROTOCOL

IP - Configure Internet Protocol
PROBE - Configure PROBE Protocol (LAN Only)
DIAL - Configure DIAL Protocol (Router/Gateway Half Only)
Necessary Only If There Are Any Switched Links

File: filename.NET.SYS

Go To IP Refresh Screen Prior Screen

Figure 12-2. Protocol Configuration Screen

Press the **Go To IP** function key.

Loopback Network Interface Configuration

Fields

Store & Forward Buffers	No store-and-forward buffers need to be configured for loopback. Default value: 0
IP Internet Address	The loopback address is always E 255.255.255.255. Default value: E 255.255.255.255
Internal Message Queue Length	This field should be 0 for loopback. Default value: 0
Fragment Assembly Queue Elements	This field should be 0 for loopback. Default value: 0

Logging is configured for the purpose of recording events such as errors and console commands. You configure logging for each of the subsystems of NS3000 and for NS3000 links. Each subsystem includes different classes of events (such as internal errors). You can record logging to a disc file, the system console and the logon device of a *user.account*. If you configure a logging class so that logging is recorded to a *user.account*, the user will receive logged messages any time there is an active session for that *user.account*. Table 13-1 provides a summary of the logging classes and guidelines for configuration.

The logging configuration for the network transport (subsystem ID 3) *must* be in the same configuration file as the network transport configuration, which *must* be in the group NET of the account SYS. The recommended filename for the actual configuration file that contains the link and network transport configuration is NSCONF.NET.SYS. If you use a different filename, you need to specify the configuration filename with the CONF keyword each time you use the NETCONTROL START command to initiate the network connection. Refer to the "Commands" section in Volume II.

The logging configuration for Network IPC (subsystem ID 5), Network Services (subsystem ID 6) and Link Manager (subsystem ID 8) *must* be in the same configuration file, which *must* be named NMCONFIG.PUB.SYS. This file is shared with other data communication subsystems that use NMS, such as SNA NRJE. If you do not want to manually configure logging, Guided Configuration, described in Section 6, will configure logging data for you. Logging data for subsystem IDs 5, 6 and 8 will be placed in NMCONFIG.PUB.SYS, while logging data for the network transport (subsystem ID 3) will be placed in your other configuration file (recommended name of NSCONF.NET.SYS).

Always work on a copy of your configuration file, not the actual file.

Follow these steps to reach the logging configuration screens for manual configuration.

- Issue the run command for NMMGR; the Open Configuration/Directory File Screen is displayed.
- Enter the name of the configuration file to be created or updated in the Configuration file name field.
- Press the appropriate function key (**Open Config** or **Create Config**); the Main Menu Screen is displayed.
- Press the function key for **Go To CONFIG**; the Configuration Screen is displayed.
- Press the function key for **Go To LOGGING**; the Logging Configuration Screen is displayed.

For more information on these steps, refer to "Getting Started with NMMGR" in Section 5.

Logging Configuration

Three screens are used for logging configuration. These screens are listed below.

LOGGING CONFIGURATION - This screen allows you to add, delete, rename or update a subsystem ID logging configuration.

LOGGING CONFIGURATION: LOGGING CLASSES - This screen allows you to select the classes of logging events you wish configure for each subsystem.

LOGGING CONFIGURATION: CLASS DATA - This screen allows you to configure where you want logging events listed for a particular logging class.

NOTE

NetIPC logging is activated at system startup, Network Services logging is activated when the Network Services are initiated (NSCONTROL START command), Link Manager logging is activated when you initiate the Network Transport (NETCONTROL START), and Network Transport logging is activated with NETCONTROL START. (Guided configuration, described in Section 6, automatically configures logging for you.) You may change logging configuration using NMMGR. For a new logging configuration to take effect for a specific subsystem, the subsystem must be deactivated and restarted. The steps that must be taken for each subsystem are:

Subsystem	Steps
Network Transport	NETCONTROL STOP (if already active) NETCONTROL START
NetIPC (sockets)	restart the system (warmstart, coolstart, update start or coldstart)
Network Services	NSCONTROL STOP (if already active) NSCONTROL START
Link Manager	NETCONTROL STOP (if active) SNACONTROL STOP; NODE= <i>nodename</i> repeat until all SNA nodes are stopped SNACONTROL START; NODE= <i>nodename</i> NETCONTROL START

TABLE 13-1. LOGGING CONFIGURATION GUIDELINES

Subsystem Name	Class Name	Events	Enable Console Logging?	Enable Disc Logging?
SUB0003 Network Transport	CLAS0001	Serious Internal Error -- Causes SYSFAIL #969.	YES	YES
	CLAS0002	Internal Error/Operator Attention	YES	YES
	CLAS0003	Non-Critical Errors.	NO	YES
	CLAS0004	Nodal Messages (Start/Stop).	YES	YES
	CLAS0005	Informative Messages.	NO	NO
	CLAS0006	Statistical Information.	NO	YES
SUB0005 Network IPC	CLAS0000	Internal Errors.	YES	YES
	CLAS0001	Resource Errors.	NO	YES
	CLAS0002	Informative Messages.	NO	NO
SUB0006 Network Services	CLAS0002	Resource Errors.	NO	YES
	CLAS0003	Internal Errors.	YES	YES
	CLAS0004	Detailed Events. (Enable with NSCONTROL LOG.)	NO	YES
	CLAS0005	NetIPC Internal Errors.	YES	YES
SUB0008 Link Manager PC Link Manager	CLAS0000	Internal Errors.	YES	YES
	CLAS0001			

The logging classes are described in detail in Section 3 of Volume II. How to use the log messages for troubleshooting is described in the *NS3000/V Error Message and Recovery Manual*, and how to format the log file for examination is described in Section 3 of Volume II.

LOGGING SUBSYSTEMS SELECTION

The screen in Figure 13-1 is displayed when you press the function key for **Go To LOGGING** at the Configuration Screen. It is also displayed when you type the path name:

@LOGGING

in the command window of any screen and press **(ENTER)**.

Use the fields and the function keys of the select screen to perform the desired action.

- To select a new subsystem ID for logging configuration, enter the subsystem ID number, then press **Add**. The path for the selected subsystem ID is added to the configuration file, and the Logging Classes Screen on that path is displayed. For NS3000 and NS3000 links, valid subsystem IDs are SUB0003 (Network Transport), SUB0005 (Network IPC), SUB0006 (Network Services), and SUB0008 (Link Manager). NMMGR prompts you for the correct format of a subsystem ID (SUBxxxx) but does not check that the subsystem ID you enter is a valid NS3000 or NS3000 link subsystem ID.
- To modify an existing subsystem ID logging configuration, specify the subsystem ID; then press **Update**. The Logging Classes Screen on the path for the specified subsystem ID is displayed.
- To change the name of an existing subsystem ID logging configuration, specify the subsystem ID and a new subsystem ID; then press **Rename**. The new subsystem ID replaces the previously configured subsystem ID.
- To delete an existing subsystem ID logging configuration, specify the subsystem ID, then press **Delete**. The previously configured subsystem ID is deleted.

NNMGR/3000 (A.01.00) LOGGING CONFIGURATION
 Type in name of item to Update, Delete, or Rename; or Add a new item.
 Command:

Path: LOGGING

Subsystem name
 New name

Subsystems Configured for Logging

--	--	--	--	--	--

File: filename.group.acct

Figure 13-1. Logging Configuration Screen

LOGGING CLASSES SELECTION

The screen in Figure 13-2 is displayed after you specify a subsystem ID on the Logging Configuration Screen (Figure 13-1) and press **Add** or **Update**. It is also displayed when you type:

@LOGGING.SUBbbbb

in the command window of any screen and press enter, where **SUBbbbb** is the subsystem ID number of the configured subsystem.

The Logging Classes Screen allows you to select the classes of logging events you wish to configure for each subsystem.

Use the fields and the function keys of the select screen to perform the desired action.

- To define a new logging class to configure, specify the class name, then press **Add**. The path for the selected class name is added to the configuration file and the data screen on the path for the specified class is displayed. Refer to Table 13-1 for valid classes of each NS3000 subsystem and an NS3000 link. NMMGR prompts you for the correct format of a class name (**CLASbbbb**) but does not check that the class name you enter is valid for the subsystem you are configuring. Use Table 13-1 to check that a class name is valid for the subsystem you are configuring.
- To modify an existing class configuration, specify the class name; then press **Update**. The data screen on the path for the specified class name is displayed.
- To change the name of an existing class configuration, specify the class name and a new name; then press **Rename**. The new class name replaces the previously configured class name.
- To delete an existing class configuration, specify the class name, then press **Delete**. The previously configured class name is deleted.

MMGR/3000 (A.01.00) LOGGING CONFIGURATION: LOGGING CLASSES
Type in name of item to Update, Delete, or Rename; or Add a new item.
Command:

Path: LOGGING.SUBbbbb

Class name
 New name

Configured Logging Classes (Under Subsystem)

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

File: filename.group.acct

<input type="button" value="Next Page"/>	<input type="button" value="Prev Page"/>	<input type="button" value="Delete"/>	<input type="button" value="Rename"/>	<input type="button" value="Add"/>	<input type="button" value="Update"/>	<input type="button" value="Refresh Screen"/>	<input type="button" value="Prior Screen"/>
--	--	---------------------------------------	---------------------------------------	------------------------------------	---------------------------------------	---	---

Figure 13-2. Logging Classes Screen

Fields

Enable Console Logging?

(Required.) Enter Y (YES) if you want logging events for this class to be displayed at the system console, N (NO) otherwise.

Refer to Table 13-1 for guidelines.

Default: N.

Enable Disc Logging?

(Required.) Enter Y (YES) if you want logging events for this class to be recorded in a disc file, N (NO) otherwise. The filename that NMS uses is NMLGnnnn.PUB.SYS, where *nnnn* is a number from 0000 to 9999. This file is used for logging by all logging classes in all subsystems. At each MPE system startup, or when a file is full, NMS creates a new NMLGnnnn.PUB.SYS file, naming each successive logging file by incrementing *nnnn*. When NMLG9999.PUB.SYS is full, NMS names the next logging file NMLG0000.PUB.SYS

Refer to Table 13-1 for guidelines.

Default: Y.

Current number of users enabled for logging

(Display only.) This field is provided for your information.

Users enabled for logging

You can display logging events for this class at users' list devices. Enter as many as three user names in the form *user.account*. Use only alphanumeric characters; you cannot use MPE wildcard characters. NMMGR sorts this list alphabetically and deletes duplicate entries after you press **Update Data**.

NOTE

The logging configuration guidelines in Table 13-1 should be followed unless your HP representative tells you otherwise. Not following these guidelines may result in the degradation of system performance.



A network directory contains information required for one node to communicate with another node in the same catenet. This catenet-wide data is managed through two interfaces--VPLUS screens for interactively configuring the network directory, and a command-driven interface to collect and merge directory information from remote nodes into the directory on the local node.

NMMGR provides the following functions regarding the network directory.

- The ability to add, update and delete entries in the directory by node name. This can be used by a Network Manager to maintain a master network directory.
- A means of presenting directory information for review and inspection.
- The ability to merge a remote directory with a directory on the local node.
- A mechanism to automatically update directories on a group of remote nodes by using a background stream job, controlled from a central administrative node. Central administrative nodes are described in more detail later in this section.

The file structure that accompanies the network directory functionality is quite different from that used throughout the rest of NMMGR. The directory resides in its own file. With the directory, there is no screen-to-record correspondence and no concept of a hierarchical file organized as a tree structure with associated paths.

NOTE

The network directory uses a KSAM file pair. Therefore, if copying the directory, be sure to copy both the data file and the key file.

WHAT A NETWORK DIRECTORY PROVIDES

A Network Directory is a repository for information about nodes in a catenet. Each entry in a directory consists of a node name and one or more path reports, called a path report list. A path report list contains the basic information about a node. These path reports are used by the transport to establish internetwork connections.

Not all nodes require a network directory. A node on a LAN can determine connection information about a node on the same LAN by multicasting a Probe request to the target node. The target node, in response to a Probe request, will supply the connection information by multicasting a Probe reply back to the requesting node. The Probe request/reply mechanism is sufficient to obtain connection requirements in a LAN environment.

The non-LAN network interface types supported by NS3000 do not use demand requests such as Probe. Therefore, a directory of information about all nodes in the catenet is required to provide the same type of information that LAN Probe requests provide.

Probe requests can be used only when the source and destination nodes are on the same LAN. Also, they must both be HP nodes because non-HP nodes do not support Probe. Not all LAN nodes that support the Probe protocol need to contain a network directory because they can request the use of a directory from another node, called a proxy server, on the same LAN. A proxy server is a node on a LAN that contains a network directory and has been configured as a proxy server. By using the Probe protocol, a LAN node without a directory can multicast a request for a proxy server. For good measure, you should designate at least two nodes on a LAN to be proxy servers.

For details on the configuration of path resolution methods (Probe, Proxy Server, Network Directory) for a given node, refer to the Global Transport Configuration Screen in Section 8.

Path Report Lists

A path report list describes the addressing information and protocol stacks for a given node. Protocol stacks define the layers in a machine's architecture, and the protocols in those layers, that information can pass through. An example of a protocol stack is TCP with checksum error checking (level 4) over IP (level 3i) over IEEE802.3 (level 3s), commonly indicated in the format: TCP.IP.IEEE802.3.

In the network directory, node names must be unique so that a single path report list can be identified. Many of the protocols on different hosts will be the same, but the addresses of the machines will not be the same.

A path report list is broken down into path reports. One path report list comprises all path reports for a given node. A node has one IP address and normally one path report for each network it belongs to. A node may be a member of as many as eight networks. The following figure shows the organization of path reports in the network directory.

```

NODE 1
  IPAddr 1
    Path(s)
  IPAddr 2
    Path(s)
  ...
  IPAddr 8
    Path(s)
NODE 2
  IPAddr 1
    Path(s)
  ...
NODE n

```

Figure 14-1. Organization of Path Reports

Global and Local Entries

Path report lists can be configured as either *Global* or *Local* entries in the network directory. Global entries (the default) can be merged into other directories.

Local entries are introduced for configuring localized network directory entries, thus providing a mechanism to restrict directory data from being propagated throughout the network. Let us consider some situations where this type of restriction could be useful. Suppose a network manager wants to change the configuration for users on a single host, but not for everyone else. He can configure two network directory entries--one Local, used by host users, and one Global, used by everyone else when establishing connections to the host. For example, suppose Node A sets up a new link to Node C, but Node A doesn't want other nodes (already connected to A) to know about Node C until the new link is tested. Users on Node A can configure a Local entry, which will contain information about the new link not included in the Global entry configured for users on other nodes. Other uses of local entries could include adding node names for local-node use only, or being able to direct which way to access remote nodes depending on your configuration of local entries.

When both local and global entries exist in the directory, the Network Transport will use the LOCAL entry.

Whenever a user activates the Network Transport subsystem on a node, a path report list describing the current node is automatically generated and entered into the local configuration file. The path report can be copied from the configuration file into the Network Directory using the MERGEDIR command, described in detail later in this section. The MERGEDIR command allows a user to configure the directory easily in most cases. Exceptions are configuring non-HP nodes and first-time links, where information cannot be taken from a remote directory file and merged, but must be entered manually.

The MERGEDIR command is part of a maintenance interface provided primarily to support the updating of directories from within a batch job. Using this method, a job or series of jobs can be scheduled at regular intervals to copy and then merge remote directories into the local-system directory. In this way, the collecting and merging of network-wide data is somewhat automated.

Roles and Interfaces

The network directory interface you use--screens or commands--will depend on your job function and whether you are creating or updating a directory. In general, the network directory configuration screens will be used by node managers when creating directories, and the maintenance mode interface (commands) will be used by a catenet administrator and network managers when updating directories.

The reason that screens, not commands, are used to *create* a directory is that a new node is at first unknown to existing nodes. This means that an existing node cannot use only commands to merge its directory to a new node. The node manager of a new node must use configuration screens to manually enter path report information about at least one existing node. Then, the new node would be able to merge its directory with the directory of the existing node, provided that someone also enters path report information about the new node into the directory of the existing node.

When a new node is added to a network, or when an existing node changes its configuration, the network manager must be notified of the new path report information. This exchange of information should take place within each network in the catenet so that, periodically, each network manager can pass this information to the catenet administrator. The catenet administrator can then stream a job, using commands from the maintenance mode interface, to update the central administrative node on each network. Each network should have one node designated as a central administrative node, as shown in Figure 14-2. This is the node that will be updated first, in terms of any global information that can be shared among all nodes on its network. This can include internet routing information in addition to network directory information.

Figure 14-2 shows the central administrative nodes of two router networks that are connected by a gateway-half link.

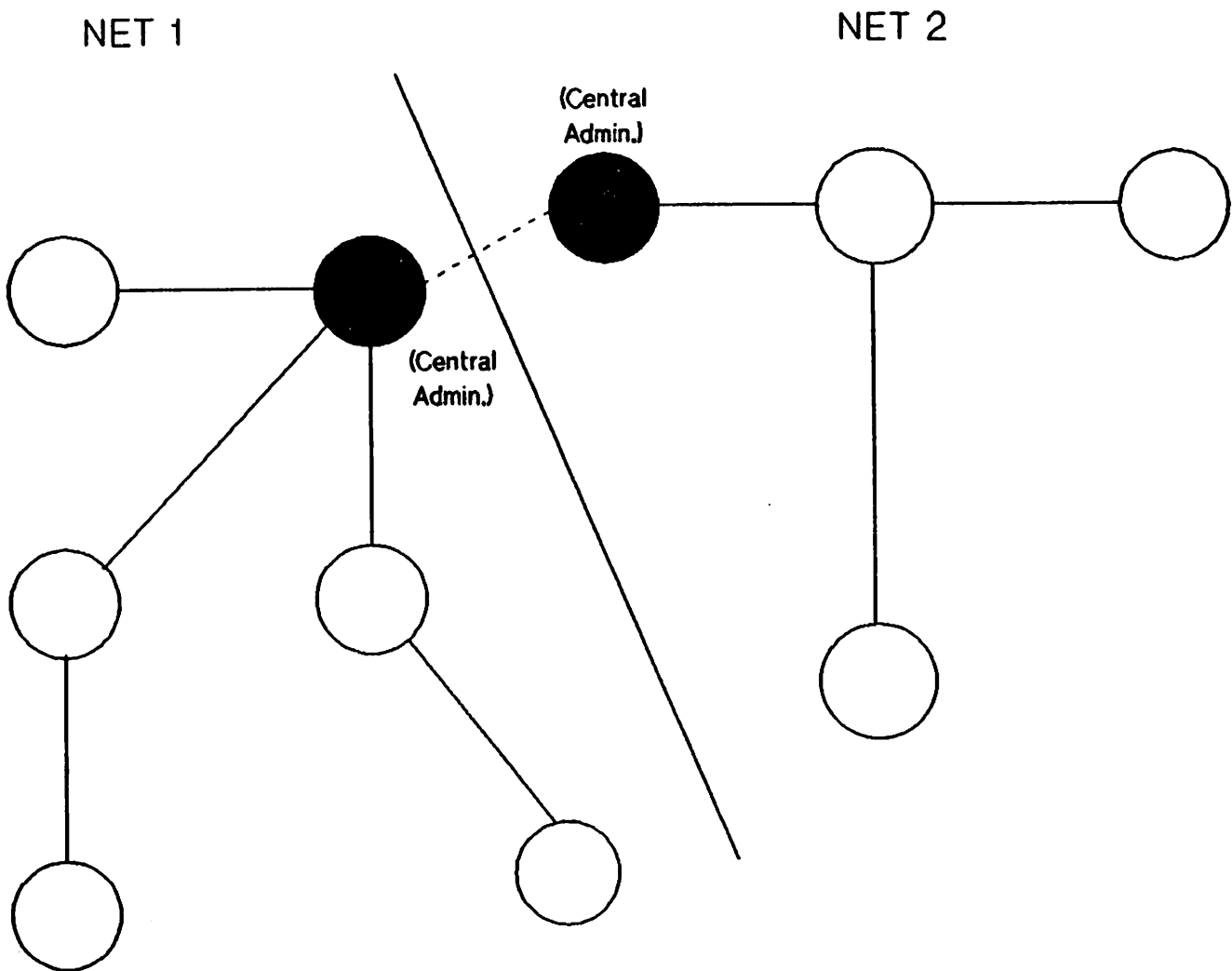


Figure 14-2. Central Administrative Nodes

Once the central administrative node on each network has been updated with new catenet-wide information, these nodes can be used to update all other nodes. Each network manager can stream a job to merge the newly updated directory from the central administrative node into the other directories on the network.

This is just a general discussion of how directories can be updated on a periodic basis. Of course, a specific directory may need to be updated sooner. For example, suppose you add a new node and manually configure its directory. Now, you have path report lists about other nodes, but they do not have your path report list. If you need to set up immediate communication with a node or group of nodes and cannot wait until the periodic update, you can send your connection information to the desired nodes so that they can enter your path report list. Or, you can send your connection information to one directly connected node. In this case, the directory of the directly connected node (first-time link situation) can be updated manually, then merged into other directories to include information about the new node.

CONFIGURATION SCREENS

The figure below shows the relationship of the various VPLUS screens used in configuring the directory through the NMMGR block mode interface:

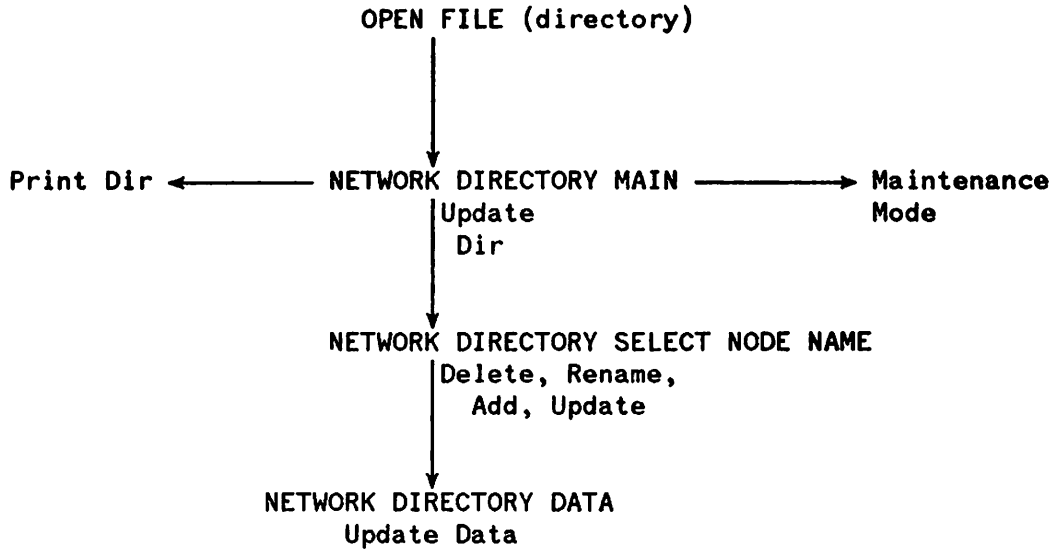


Figure 14-3. Network Directory Screens

Following are the configuration screens and descriptions of the fields on each screen. There are two ways to access the Network Directory functions: 1) open or create a directory file on the initial NMMGR screen, the Open Configuration/Directory File Screen, 2) issue the NETDIR command from any screen, at any time *after* having opened a network directory file. Either action will bring you to the first screen in sequence, the Network Directory Main Screen.

NETWORK DIRECTORY MAIN SCREEN

This screen is displayed when you press the function key for **Open Directory** or **Create Directory** at the Open Configuration/Directory File Screen. This screen is the main select screen from which all directory functions are accessed. The currently opened directory is displayed at the bottom of this screen and all subsequent Network Directory screens. The percentage of the Network Directory that is full is shown in the lower right corner of the screen.

```

NNMGR/3000 (A.02.00) NETWORK DIRECTORY MAIN
Select a function and press the corresponding function key.
Command:

UPDATE      -  Modify the directory (Add, Delete, Update).
PRINT       -  Print the directory to FORMLIST.
MAINTENANCE -  Enter maintenance mode interface (Merge, Expand, etc.)

                                                    Directory is 3 % full

Directory: NSDIR.PUB.SYS
UPDATE  PRINT  MAINT
Dir     Dir    Mode
Refresh Prior
Screen  Screen

```

Figure 14-4. Network Directory Main Screen

Press **F1**, Update Dir to modify the contents of the directory by adding, deleting and updating node names and path reports. If you press this function key, you will be taken to another screen, the Select Node Name Screen, from which you can visit the Network Directory Data Screen. The Network Directory Data Screen allows you to manually configure path reports about other nodes in the catenet.

Although you often will use job streams or simple commands for adding information to your network directory, there are times when manual configuration is required or desirable. It is required when a new node has been added to the catenet, and you wish to update another node's directory with information about this new node. You cannot use the MERGEDIR command until this new information has been added to the existing directory. Therefore, you need to physically receive the path report lists from the node manager of the new node or from that node's network manager. After obtaining this information, you can use the screens to configure the path reports about the new node. Once you have done this, you can use MERGEDIR in the future for updating purposes because you now have this new node's connection information in your network directory.

Network Directory

Whenever you do not have access to the necessary configuration file or directory file, you are required to use the screens for configuring directory information.

There may also be situations when you choose to use the screens to update your file even when other methods are available. For example, if you are updating one path report list, it might be easier to use the screens than to use commands.

Press **F2**, **Print Dir** to print out a copy of the directory to formal designator FORMLIST, device class LP. The output is the same as for the LISTDIR command. See the "LISTDIR Command Sample Output" subsection for an example of LISTDIR output. You can use a file equation for FORMLIST to redirect the output to another device class or disc file. To set a file equation without leaving NMMGR, use the appropriate MPE command in the command window

Press **F3**, **Maint Mode** to enter the command interface to perform directory merging or to expand the size of your directory. Once entered, you can return to this point only by issuing the maintenance mode EXIT command. Within the maintenance mode interface, command input is read from the formal designator NMMGR CMD, which defaults to \$STDINX.

Network Directory

Press **F6**, **Update** to update path reports for the named node. This includes deleting part, but not all, of a node's path report list. You are taken to the Network Directory Data Screen.

Fields

Node Name

The name of the node on which to perform a function. This field can be used in two ways, depending on which function key you use.

Use the **Add**, **Delete**, **Rename** and **Update** functions as described above to change the current information in your network directory. When used in conjunction with these fields, the Node Name field must contain a fully qualified node name.

The Node Name field serves a different purpose when used with the **Prev Page** and **Next Page** functions. When used with these function keys, the Node Name field is used to browse through a specified part of your network directory. You can enter part of a node name in this field to designate which node names you want displayed. For example, if you enter the value **MAY**, and press **Next Page**, the list of nodes will begin with the first matching node name--**MAYTAG.FINANCE.IND**, for example-- and continue through the rest of the alphabet until all node names between the letters **MAY** and **Z** are listed.

Your node names do not need to be fully qualified with domain and organization fields when used with the **Prev Page** and **Next Page** functions.

Default value: None

Global?

The Global/Local setting for Node Name. The acceptable values are **Y** or **N**. When the **Prev Page** and **Next Page** function keys are used, only node names whose Global/Local setting matches the value in this field will be displayed. Therefore, set this field accordingly when displaying node names.

Default Value: Y

New Name

New name to be assigned to the node with the **Rename** function. The only time this field is used is when you use **Rename**.

Default value: None

New Global

The Global/Local flag setting for the node named in the **New Name** field. The acceptable values are **Y** or **N**. The only time this field is used is when you use **Rename**. The **New Name** field can be left blank if you wish to change only the Global/Local setting.

Default value: None

Configured Node Names & Global Flag

Display-only fields that show node names and their Global/Local Flag settings that are already configured in the directory.

Fields

Transport Services

These three fields describe the Transport Services that should be configured in each path. All customers should have TCP and PXP configured. The Checksum setting indicates whether checksumming is optional (N) or required (Y) for TCP

Note that the selection of Transport Services here must match the settings in the remote node's configuration file. The path of the data screen that contains TCP configuration is NETXPORT.GPROT.TCP, and the path of the data screen that contains PXP configuration is NETXPORT.GPROT.PXP. Because the same data must appear on more than one screen, it would be safest to use the default values to help avoid mismatched values.

Mark the selected services with a Y or an N. The Transport Services and their default settings are:

TCP: Transmission Control Protocol (default Y)

TCP Checksumming optional or required (default N)

PXP: Packet Exchange Protocol (default Y)

IP Address

One IP address should be entered for each LAN or Router network interface configured on the node. Each address must match an IP address configured in the node's configuration file. The path of the screen in the configuration file that contains IP addresses is NETXPORT.NI.*niname*.PROTOCOL.IP.

Default Value: None

Type

A number indicating the type of path to configure:

1: IP. This path type should be selected when the network interface type is ROUTER, or LAN with the Probe protocol configured.

2: IP/IEEE802.3. This path type should be selected when the network interface type is a LAN and the node is a non-HP node, which does not support the Probe protocol.

Additional Address

A lower-level address, which depends on the Type.

Type 1 paths do not contain lower-level addressing information. You can leave the field blank, or the keyword "NONE" can be entered.

Path type 2 requires a station address, which is a string of six hexadecimal bytes, separated by dashes (XX-XX-XX-XX-XX-XX). This path type is used only for a LAN non-HP node, which does not support the Probe protocol. The station address must be the same as the station address entered in the node's configuration file (screen path LINKCONF.*linkname* for IEEE802.3; field Local Node Address in Hex).

DIRECTORY MAINTENANCE MODE INTERFACE

Several commands are available for updating information in a network directory. These commands primarily will be used within batch jobs for updating directory information on remote nodes.

The main features of this utility are:

- It generates a job stream to sequentially update a list of nodes.
- The list of nodes to update is user-defined.
- The process provides logging information.
- The process is "recoverable."
- Commands executed on the remote system are user-defined.

You provide a list of node names that are to be updated (which can be easily generated) in addition to the name of a command file to be executed from the NMMGR Maintenance Mode interface. From these two files, a job stream file is generated which, when executed, attempts to log on to each node named in the list and apply the commands read from the command file. The success or failure status of each nodal update is recorded in the node list file, along with the date and time of the event. This node list "control" file may be used again to retry updates on failed nodes, after the source of the failure has been determined and corrected.

In order to use these commands on a remote node, your local node's network directory file must contain an entry for the node whose directory you wish to update. Without an entry, you would not be able to log on to the remote node because you would not have its connection information. For this reason, the commands are generally used for updating directories on existing nodes. However, it is possible that these commands can be used to create a directory on a remote node. To accomplish this, the node manager of this new node would have to verbally notify you of this new node's existence. You then would have to enter the new node's connection information into your network directory. Once this information is entered into your directory, you have the capability to log on to the new node and merge your entire directory to create a version of this directory on the new node.

The network directory command interface is directly accessible by running NMMGR.PUB.SYS from a stream job, by pressing the **Maint Mode** key at the Network Directory Main Screen, or by running NMMGR.PUB.SYS with a file equation for the formal designator NMMGRCMD set to a command file. An example of such an equation is :FILE NMMGRCMD=CMDFILE.

Command input is echoed to \$STDLIST if run from within a stream job or when the input is read from a command file. Blank command lines may be entered freely.

OPENDIR Command

The OPENDIR command is used to gain access to a Network Directory file. For example, suppose your node's configuration has changed, and you want to update a remote node's directory to reflect this change. You can log on to the remote node and open its directory file using the OPENDIR command. Syntax:

```
OPENDIR dirname
```

The format for *dirname* is a standard MPE file system name: FILENAME[.GROUP[.ACCOUNT]]. A file lockword cannot be specified. A file equation may be used.

Any currently opened directory is closed and *dirname* is opened for read/write and share access. If the directory does not exist, then an attempt to create it is made; the file is then opened for read/write and share access.

The capacity of the network directory is 500 entries.

DELETENODE Command

The DELETENODE command removes an entry from the directory. For example, suppose you have logged on to a remote node and opened its directory using the OPENDIR command. Using DELETENODE, you can now delete a node from this remote directory. Syntax:

```
DELETENODE [nodename] [;{LOCAL }  
                  {GLOBAL }]
```

If you omit the *nodename* option, all path reports for all nodes will be deleted.

If you omit the *nodename* option while running the DELETENODE command from a session, the confirmation message Are you sure? will be displayed, requiring a response. However, if you are running a batch job, no opportunity for confirmation is available. Therefore, be especially careful not to omit the *nodename* option unless you really intend to delete all entries in the opened directory.

When the *nodename* option is supplied, only the path reports for the specified node will be deleted.

LOCAL and GLOBAL are optional and qualify which entry is to be deleted when the same node name has a LOCAL entry and a GLOBAL entry.

MERGEDIR Command

The MERGEDIR command is used to merge one or more entries from one directory file into the currently opened directory file, or to merge a single entry from a configuration file into the opened directory file.

Syntax:

```
MERGEDIR {otherdir [,nodename]} [;{LOCAL  
GLOBAL}] [;{KEEP  
NOKEEP  
TIMESTAMP}]
```

The parameter *otherdir* is the name of the directory from which entries are to be merged into the opened directory. The option *nodename* is the name of a single node entry to be merged; if omitted, all entries in *otherdir* are merged.

The parameter *configfile* is the name of a node's configuration file from which to merge the path report list of the node. As a rule, you should perform this type of merge on the same node's network directory immediately after you have activated the network transport. When the network transport is activated, a path report list is automatically entered into the configuration file. By performing this type of merge, you are bringing the path report of the node into the network directory of the same node. A node having connection information about itself is not really needed except for loopback, but having it in the directory is necessary so that this information will be included if this directory is merged into the directory of another node. The option *nodename* cannot be supplied if merging from a configuration file.

Both of the file names must be standard MPE file system names. Lockwords are not permitted. A file equation may be used for *otherdir*, but not for *configfile*.

Either *otherdir* or *configfile*, but not both, may be specified.

LOCAL and GLOBAL define which class of entry is to be merged if the source is a directory file, and define the flag setting in the target directory if the source is a configuration file. The default is GLOBAL.

The last three options, which can be specified only when merging from another network directory file, define the manner in which duplicate entries are to be handled.

- | | |
|-----------|---|
| KEEP | Duplicate entries found in <i>otherdir</i> are ignored; the corresponding entries in <i>dirname</i> are not changed. |
| NOKEEP | Unconditionally replaces duplicate entries in <i>dirname</i> with the corresponding entries from <i>otherdir</i> . |
| TIMESTAMP | Replaces duplicate entries in <i>dirname</i> only when timestamp information indicates that a corresponding entry in <i>otherdir</i> was created more recently. |

If no option is specified, TIMESTAMP is assumed.

The node name of each duplicate entry is displayed, along with the action taken, either REPLACED or UNCHANGED.

Entries that exist in *otherdir* (or *configfile*), but not in *dirname*, are entered into *dirname* and are displayed along with the word ADDED.

After all entries have been examined, a summary is displayed, indicating the total number of entries added and replaced.

LISTDIR Command

The LISTDIR command displays information about entries configured in the directory.

Syntax:

```
LISTDIR [nodename]
```

If the *nodename* option is omitted, all entries in the directory are listed.

If the *nodename* option is supplied, the information about this node will be displayed.

The output is directed to formal designator FORMLIST, which defaults to \$STDLIST, but may be redirected with a file equation. See the "LISTDIR Command Sample Output" subsection for an example of LISTDIR output.

EXPANDDIR Command

The EXPANDDIR command increases the capacity of the currently opened directory file.

Syntax:

```
EXPANDDIR numrecs
```

The parameter *numrecs* is the number of records to be added to the network directory file. The number of records used by one node's network directory entry is one greater than the number of network addresses belonging to the node.

NOTE

To run this command, you must be logged on to the account that contains the directory file, and you must have exclusive access to the file. Given this second constraint, the standard network directory file NSDIR.NET.SYS may not be expanded while the network transport is activated because the transport needs access to this directory. Therefore, the transport must be stopped to increase the capacity of this directory file.

HELP Command

The HELP command displays help text about MPE commands and network directory commands.

Syntax:

```
HELP [commandname [,qualifier]]
```

Typing the HELP command by itself allows you to enter the MPE help facility. At this point, an overview of available commands is displayed, and command names may be entered at the prompt. Type EXIT to return to the NMMGR prompt.

The *commandname* option may be included to obtain an overview and the syntax for a specific command. In addition, one of the optional qualifiers-- PARMS, OPERATION, EXAMPLE, or ALL-- may be included to receive more detailed information about a command. You are returned to NMMGR's prompt after help text is displayed.

:MPE Command

Syntax:

```
:mpecommand
```

The parameter *mpecommand* is any command that can be executed by means of the MPE COMMAND intrinsic. Examples of how this can be useful include embedding comments in a sequence of commands using *:comment...*, or executing *:listf* or *:tell*, or executing *:file* for redirecting output of the LISTDIR command.

EXIT Command

The EXIT command terminates the command interface.

Syntax:

```
EXIT
```

If you have invoked the interface from an NMMGR screen, you are returned to the Network Directory Main Screen if a directory file was left open upon exit; if no file is currently open, you are returned to the Open Configuration File/Directory Screen.

If you have invoked the interface directly from the MPE command interpreter, the EXIT command closes any opened directory file, and the program terminates.

MAKESTREAM Command

The MAKESTREAM command generates a stream job to update remote directories or configuration files.

Syntax:

```
MAKESTREAM streamfile, nodefile, cmdfile
```

All three file names must be in standard MPE file name format.

The parameter *streamfile* is the name of a file to receive the job stream text. The file must not already exist.

The parameter *nodefile* is the name of an ASCII editor-type file that contains a list of nodes to be updated. It also serves as a log file. Note that the file name must be qualified with group and account names to the extent that the job (default logon: NETADMIN.SYS) requires it.

The simplest way to generate this file is to redirect the output of a LISTDIR command into an ASCII file:

```
NMMGR> :file formlist=nodelist;dev=disc (RETURN)
NMMGR> listdir (RETURN)
NMMGR> :reset formlist (RETURN)
```

The file is processed by the MAKESTREAM command as follows:

1. Only lines that begin with an alphabetic character in the first column are considered node name entries; all other lines are deleted.

2. For those lines that qualify in the step above, the node name is delimited by the first blank encountered. All information after the node name is ignored and stripped away.
3. Locally designated node names -- those names followed by a single space, then (L) -- are discarded.
4. Duplicate node names are deleted.
5. The logging information string "NOT UPDATED" is added to the list for each node name.

A sample processed file is shown below:

ANIMAL.FINANCE.IND	NOT UPDATED
ASTRO.MARKETING.IND	NOT UPDATED
CECIL.FINANCE.IND	NOT UPDATED
RODAN.MARKETING.IND	NOT UPDATED
SAKURA.MARKETING.IND	NOT UPDATED
STANDALONE.MARKETING.IND	NOT UPDATED
TIGGER.FINANCE.IND	NOT UPDATED
VENUS.FINANCE.IND	NOT UPDATED

These are the nodes shown in Figure 14-7, a two-network catenet. Let us assume that these nodes are entries in the directory on ANIMAL.FINANCE.IND, which we have designated as the central administrative node of NET1. Suppose we want to use the directory on ANIMAL to update only those nodes on the same network, NET1. We would need to edit *nodefile* manually to remove the NET2 node names. We also would remove the name ANIMAL because we are assuming its directory has been updated and we are using it to update other directories. Meanwhile, the network manager of NET2 could perform a parallel function to update only the NET2 nodes, using SAKURA as the central administrative node on NET2. (In many cases, however, one central administrative node could be used to update all nodes in the catenet, meaning that *nodefile* would not need to be edited.)

The parameter *cmdfile* is the name of an NMMGR Maintenance Mode command file. This name also must be qualified with group and account names to the extent that the job will require them. Below is an example of a command file that could be used to merge the local directory file NSDIR.NET.SYS with directory files of the same name on other nodes (listed in *nodefile*).

```
OPENDIR NSDIR.NET.SYS
:FILE SOURCE=NSDIR.NET.SYS:$BACK
MERGEDIR *SOURCE
EXIT
```

When using \$BACK, the network directory on the remote node must have the local node name configured.

Typical commands included in a command file are MERGEDIR, COPYCONF and DELETENODE. Any command, however, may be used.

Once the job stream has been created using MAKESTREAM, it may be optionally customized, then executed. You may change certain parameters in the job stream that are defaulted, like the remote logon string. Another default is that progress messages are sent to OPERATOR.SYS. MAKESTREAM supplies a default logon of NETADMIN.SYS,NET with no user, group or account passwords. If you have very demanding security needs, you can substitute a different logon for each node that will be updated. If defaults are changed, the appropriate user/account capabilities are assumed to be in place. (For example, updating a network directory requires NA capability; copying configuration file information requires NM capability; both actions require BA and IA capability.)

Each node listed in *nodefile* is logged onto with a REMOTE HELLO. Files local to the node on which the stream job is run may be accessed remotely using RFA and file equations. The NMMGR Maintenance Mode process is run on the *remote* side of the connection.

Each line entry in *nodefile* is updated with the logging string "UPDATED" if all commands are executed successfully. After the completion of the job stream, *nodefile* may be inspected for the results of all updates. A sample, based on using ANIMAL in Figure 14-7 to update the other NET1 nodes, is shown below:

CECIL.FINANCE.IND	UPDATED	10/21/86	4:55 PM
TIGGER.FINANCE.IND	UPDATED	10/21/86	5:11 PM
VENUS.FINANCE.IND	NOT UPDATED	10/21/86	4:49 PM

Any nodes that could not be updated are noted; the job stream should be consulted to determine the cause of a failure. Once the problem has been corrected, the same job can be re-streamed. Only for those nodes with the logging string "NOT UPDATED" will a logon and update be attempted. This process can be repeated until all nodes have been satisfactorily updated.

The stream job can be re-created each time an update is desired, or the same job can be used after editing the nodefile to reset the UPDATED strings to NOT UPDATED. For highly customized environments, the latter will be easiest.

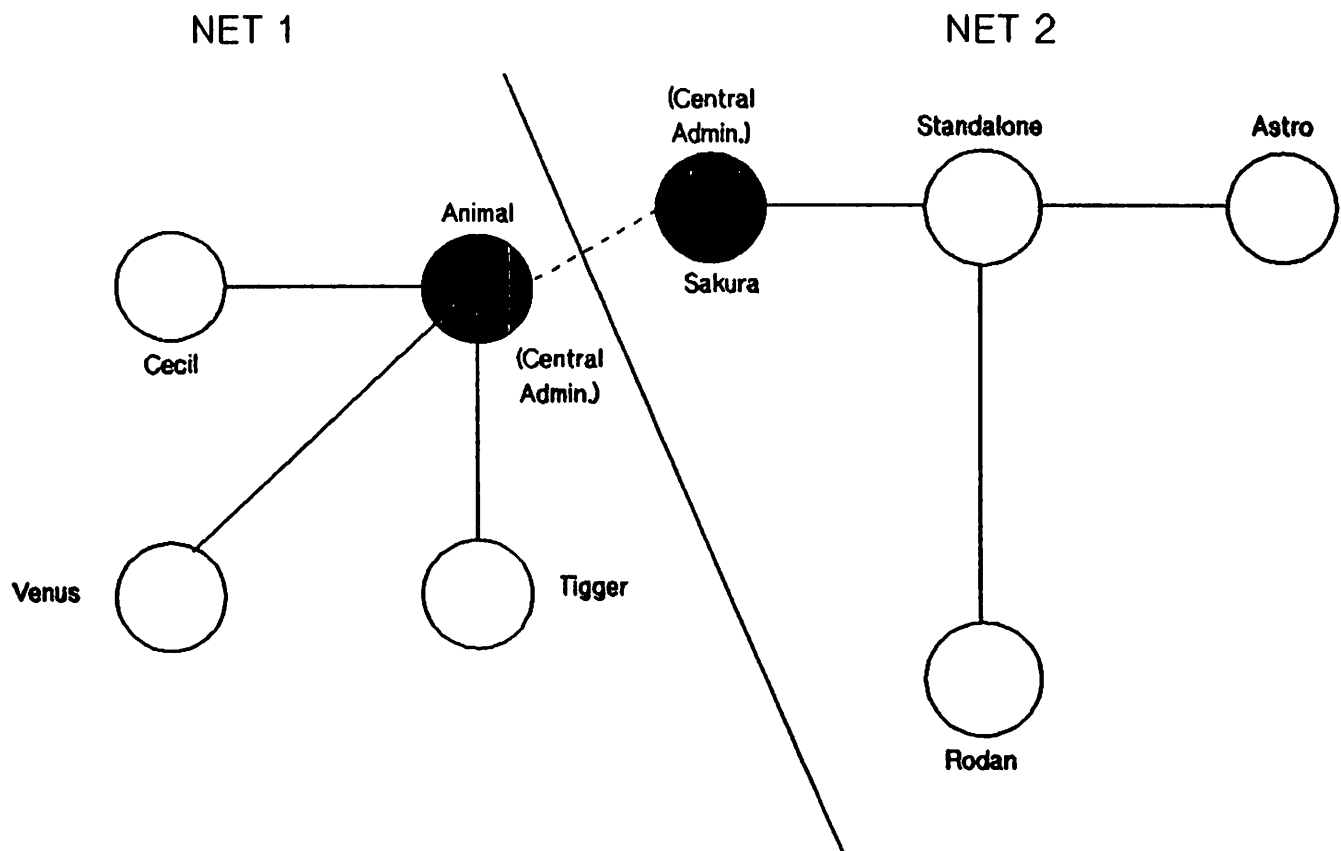


Figure 14-7. Two-network Catenet

LISTDIR COMMAND SAMPLE OUTPUT

The following is a sample listing produced by the NMMGR Maintenance Mode Interface LISTDIR command and the **PRINT Dir** key of the Network Directory Main Screen.

The top of the listing contains information that pertains to the directory as a whole, including its name, when and where it was most recently updated, and the amount of space available.

Each entry in the directory is listed alphabetically with its local/global classification. For each entry, the name, an indication if it is a local entry (L), and one to eight path reports are shown. For each path report, the IP Address, network type, additional address and Transport Services (if applicable) are shown.

GLOBAL NETWORK DIRECTORY INFORMATION

```

Directory File:      NSDIR.NET.SYS
Modification Date:  FRI, AUG 22, 1986, 12:32 PM
Modification Node:  ERNIE.DCL.IND
Records Used:       20
Records Available:  980
Capacity:           2% full
    
```

Node Name	IP Address	Net Type	Additional Addr	T C P C H X P K P
ERNIE.DCL.IND	C 192.001.000 004	IP	NONE	X X
TIGGER.DCL.IND	C 203.154.017 006	IP/IEEE802.3	14-2B-20-4E-C9-53	X X
	C 198.001.000 007	IP	NONE	X X

WORKSHEETS

APPENDIX

A

This appendix contains worksheets necessary for configuration of nodes in your catenet. Do not fill out these sheets, but make copies as needed. All necessary tables and required fields are included, as well as blank sheets for all necessary maps.

References to tables and maps are generic in this appendix. For example, references are made to the Router Network Map. If your catenet contains two router networks, you will have two router network maps, but each map will include a unique network name.

Worksheets

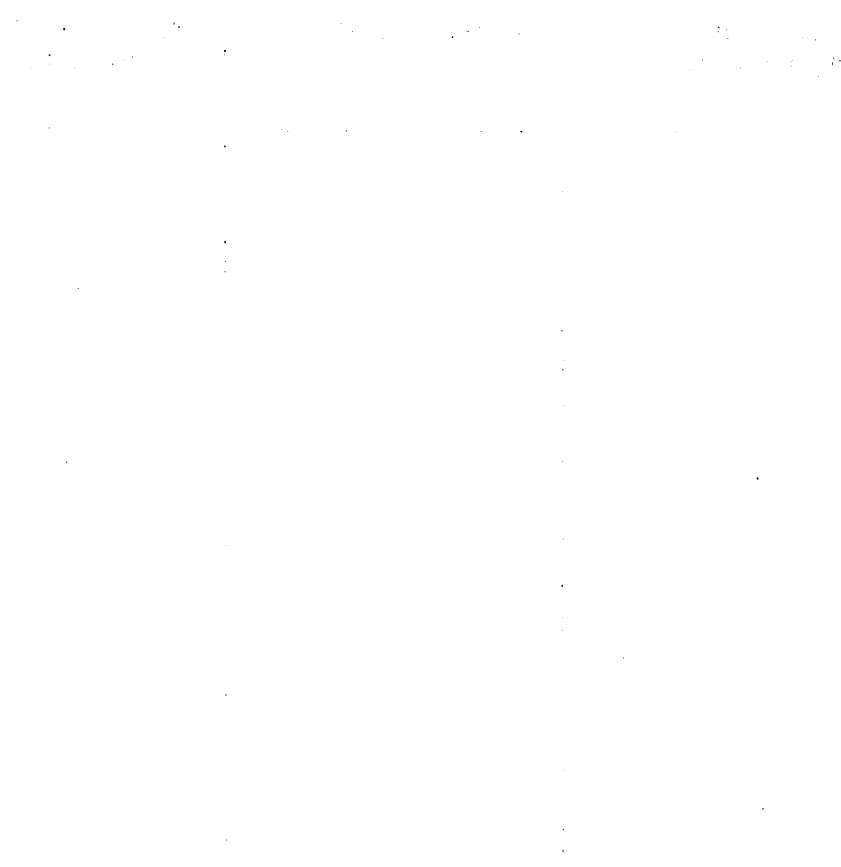
CATENET MAP

CATENET TABLE

NETWORK	NETWORK TYPE (LAN, ROUTER)	IP NETWORK ADDRESS	IMPLEMENTATION PRIORITY

Worksheets

LAN NETWORK MAP



LAN NETWORK TABLE

NETWORK NAME:

IP NETWORK ADDRESS:

NODE NAME	IP NODE ADDRESS	PROXY SERVER (Y/N)	GATEWAY NODE (Y/N)	IMPLEMENTATION PRIORITY

LAN INTERNET ROUTING TABLE

NETWORK NAME:

IP NETWORK ADDRESS:

THROUGH GATEWAY NODE	IP NODE ADDRESS	DESTINATION NETWORK/ADDRESS	HOPS NEEDED TO REACH DESTINATION NETWORK

ROUTER NETWORK MAP

ROUTER NETWORK TABLE

NETWORK NAME:

IP NETWORK ADDRESS:

NODE NAME	IP NODE ADDRESS	CENTRAL ADMIN. NODE? (Y/N)	GATEWAY NODE (Y/N)	IMPLEMENTATION PRIORITY

ROUTER INTERNET ROUTING TABLE

NETWORK NAME:

IP NETWORK ADDRESS:

THROUGH GATEWAY NODE	IP NODE ADDRESS	DESTINATION NETWORK/ADDRESS	HOPS NEEDED TO REACH DESTINATION NETWORK

GATEWAY-HALF MAP



GATEWAY-HALF NETWORK INTERFACE TABLE

NETWORK NAMES:

GATEWAY NODE	FULL IP ADDRESS OF PARTNER	CONNECTED NETWORK	LINK NAME

After you choose to perform Guided Configuration, you select the **Go To NET CON** function key to perform first-time configuration of a node. You then select an NI name and press the appropriate topology function key. For NI names, use the network names on the network maps. This way, you will be able to keep track of the NI names you enter. You will then visit the Node Name Configuration Screen, shown below. (This screen is always visited during loopback guided configuration, but is visited for LAN, router, PC-router and gateway half guided configurations only if a node name has not already been configured.)

NOTE

References to figure numbers and page numbers pertain to Volume I.

NODE NAME CONFIGURATION (NETXPORT.NODE.NAME) Fig. 8-3, p. 8-5

Node Name _____

Name of the node you are configuring. Must be in the form *node.domain.organization*.

LAN NODE INTERNET ROUTING

NODE NAME:

IP ADDRESS:

NETWORK NAME:

GATEWAY NODE/IP ADDRESS	DESTINATION NETWORKS/ IP ADDRESSES	HOP COUNT

LAN CONFIGURATION SCREENS

LINK CONFIGURATION (LINKCONF) Fig. 7-1, p. 7-4

Link Name _____

Assign a link name that is eight alphanumeric characters or fewer, the first character must be alphabetic.

LAN802.3 LINK DATA (LINKCONF.*linkname*) Fig. 7-2, p. 7-6

Logical Device _____

The ldev number of the LANIC that will be configured in SYSDUMP.

PROBE PROTOCOL CONFIGURATION (NETXPORT.NI *niName*.PROTOCOL.PROBE) Fig. 9-4, p. 9-10

Proxy Enabled _____

Answer Y if this node will be a proxy server (will have a network directory). Refer to LAN Network Map.

IP PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.IP) Fig. 9-3, p. 9-7

IP Address _____

Full IP address of the node being configured. Refer to LAN Network Table.

LAN CONFIGURATION SCREENS (cont'd)

Note: This page contains information for one gateway. Before you proceed, make copies of this page for additional gateways. During Guided Configuration, press the **Next Screen** function key when finished configuring information for a gateway. This returns you to the first screen shown on this page. If you are finished for all gateways, press the **Next Screen** key again.

NEIGHBOR GATEWAYS (NETXPORT.NI.*niName*.INTERNET) Fig. 9-7, p. 9-18

Gateway Name _____

Assign a name (maximum eight characters) to reference a gateway that is on the network to which the node belongs. Refer to Catenet Map and LAN Network Map.

NEIGHBOR GATEWAY REACHABLE NETWORKS (NETXPORT.NI.*niName*.INTERNET.*gatewayn*)
Fig. 9-8, p. 9-19

Neighbor Gateway IP Internet Address _____

Full IP address of the gateway node. Refer to LAN Network Table.

IP Network Address

_____ (1)

_____ (2)

_____ (3)

_____ (4)

The IP addresses of all reachable networks in the catenet, through the gateway node named above. Refer to LAN Node Internet Routing Table. You need to fill out a node portion for each IP Network Address, even though the node portion is ignored. You can simply enter zeros for these node portions.

Hops

_____ (1)

_____ (2)

_____ (3)

_____ (4)

Refer to LAN Node Internet Routing Table for Hop Count. The numbers in parentheses correspond to the numbers regarding IP network addresses.

SUBSEQUENT LAN NODES

If you are adding a LAN node, be sure to complete this information and update the corresponding maps and tables.

Link Name _____

Logical Device _____

Proxy Enabled? _____

IP Address of the node being configured

Gateway Names 1) _____ 2) _____ 3) _____

Neighbor Gateway IP Internet Addresses

1) _____ 2) _____ 3) _____

For first gateway:

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

Be sure to add IP network addresses and hops for other specified gateways.

ROUTER NODE INTRANET ROUTING TABLE

NODE NAME:

IP ADDRESS:

NETWORK NAME:

DESTINATION NODE	LINK NAME	DESTINATION NODE'S IP ADDRESS	ENTRY PRIORITY

ROUTER NODE INTERNET ROUTING

NODE NAME:

IP ADDRESS:

NETWORK NAME:

GATEWAY NODE/IP ADDRESS	DESTINATION NETWORKS/ IP ADDRESSES	HOP COUNT

ROUTER CONFIGURATION SCREENS

LINK CONFIGURATION (LINKCONF) Fig. 7-1, p. 7-4

Link Name _____

Assign a link name that is eight characters or fewer. The first character must be alphabetic. This link name corresponds to one link the node has configured. After you have been taken to all the necessary screens for this link, Guided Configuration will bring you back to this screen to configure any other links for this node. The fields on this page and the first field on the next page may need to be copied so that you can fill out the appropriate information for other links. Refer to Router Network Map. When you are finished configuring the links for this node, press the **Next Screen** function key.

Type: ASNP, LAP-B or BSC Circle one.

ASNP LINK DATA (LINKCONF.*linkname*) Fig. 7-12, p. 7-27

Logical Device _____

The ldev number that will be configured in SYSDUMP.

OR

LAP-B LINK DATA (LINKCONF.*linkname*) Fig. 7-9, p. 7-19

Logical device _____

The ldev number that will be configured in SYSDUMP.

Local Mode (5=DTE, 6=DCE, 11=HP Point to Point) _____

HP recommends that you use the default, HP Point to Point. If so, both sides of the link must be configured as HP Point to Point.

OR

BISYNC LINK DATA (LINKCONF.*linkname*) Fig. 7-6, p. 7-11

Logical Device _____

The ldev number that will be configured in SYSDUMP

ROUTER CONFIGURATION SCREENS (cont'd)

NETWORK INTERFACE LINKS (NETXPORT.NI.*niName*.LINK) Fig. 10-6, p. 10-17

Type _____

DD--Direct Dial, DC--Direct Connect, or SD--Shared Dial

DIRECT CONNECT LINK CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 10-7, p. 10-19

No fields required to configure.

OR

ROUTER DIAL LINK CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 10-8, p. 10-21

No fields required to configure.

ROUTER NETWORK INTERFACE CONFIGURATION (NETXPORT.NI.*niName*) Fig. 10-1, p. 10-3

Network Hop Count _____

The greatest possible number of intermediate nodes between the two nodes farthest apart on the network. See Router Network Map.

Idle Device Timeout Value (Minutes) _____

For dial links, this is the number of minutes a device can remain idle (no traffic) before shutting down. A value of zero will disable the idle device timer for all devices on this network interface. (Enter 0 for Direct Connect links.)

IP PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.IP) Fig. 10-3, p. 10-8

IP Address _____

Full IP address of the node being configured. Refer to Router Network Table.

ROUTER CONFIGURATION SCREENS (cont'd)

Note: Mapping configuration is required for each local link the node can use to reach each remote node on the router network. Therefore, make enough copies of this sheet before you fill in any information. After configuring mapping information for one node, Guided Configuration will bring you back to the first screen on this page. Repeat the process until you have completed all mapping configuration, then press the **Next Screen** function key.

MAPPING CONFIGURATION (NETXPORT.NI.*niName*.MAPPING) Fig. 10-12, p. 10-30

Router Node Name _____

Assign a name (maximum eight characters) to represent a node you wish to be able to reach from your node. Refer to Router Node Intranet Routing Table.

ROUTER REACHABLE NODES (NETXPORT.NI.*niName*.MAPPING.*mapentry*) Fig. 10-13, p. 10-32

IP Internet Address _____

Full IP address of the destination node named above. Refer to Router Node Intranet Routing Table.

Link Name _____

Name of the link used to reach the destination node. Must match a link name that you configured on the link configuration screen. If more than one link is required to reach the destination node, list only the first link to be used.

Adjacent (0)/ Non-adjacent (1) _____

If the destination node is not directly connected to the link just named, enter 1. Otherwise, enter 0. Refer to Router Network Map.

Entry Priority _____

Used when alternate local links are configured to reach a remote node. Refer to the Router Node Intranet Routing Table. If no alternate links will be configured, use the default of 50 for the priority so that you allow for possible additions with higher or lower priority numbers.

Phone Number _____

The phone number of the destination node is required if the destination node is directly connected to the other end of the link and if the link is a direct dial or a shared dial link.

ROUTER CONFIGURATION SCREENS (cont'd)

Note: This page contains information for one gateway. Before you proceed, make copies of this page for additional gateways. During Guided Configuration, press the **Next Screen** function key when finished configuring information for a gateway. This returns you to the first screen shown on this page. If you are finished for all gateways, press the **Next Screen** key again.

NEIGHBOR GATEWAYS (NETXPORT.NI.niName.INTERNET) Fig. 10-9, p. 10-24

Gateway Name _____

Assign a name (maximum eight characters) to reference a gateway that is on the network to which the node belongs. Refer to Catenet Map and Router Network Map.

NEIGHBOR GATEWAY REACHABLE NETWORKS (NETXPORT.NI.niName.INTERNET.gatewayn) Fig. 10-10, p. 10-25

Neighbor Gateway IP Internet Address _____

Full IP address of the gateway node. Refer to Router Network Table.

IP Network Address

_____ (1)

_____ (2)

_____ (3)

_____ (4)

The IP addresses of all reachable networks in the catenet, through the gateway node named above. Refer to Router Node Internet Routing Table. You need to fill out a node portion for each IP Network Address, even though the node portion is ignored. You can simply enter zeros for these node portions.

Hops

_____ (1)

_____ (2)

_____ (3)

_____ (4)

Refer to Router Node Internet Routing Table for Hop Count. The numbers in parentheses correspond to the numbers regarding IP network addresses.

SUBSEQUENT ROUTER NODES

If you are adding a router node, be sure to complete this information and update the corresponding maps and tables.

Link Name _____

Type = ASNP, LAP-B or BSC Circle one.

Logical Device _____

DTE/DCE for LAP-B _____

Is link Direct Dial, Direct Connect, or Shared Dial? _____
(Must repeat all of above information for all links belonging to the node.)

Network Hop Count _____

Idle Device Timeout Value _____

IP Address of the node being configured

Router Node Name _____
(This name is for mapping information to follow; the name represents a destination node on the network.)

IP Internet Address of the destination node _____

Link name used to reach the destination node _____

Adjacent (0)/ Non-adjacent (1) _____

Entry Priority _____

Phone Number _____

From Router Node Name, above, to this point, information must be repeated for all mappings to be configured.

See next page for additional router fields.

SUBSEQUENT ROUTER NODES (cont'd)

Gateway Names 1) _____ 2) _____ 3) _____

Neighbor Gateway IP Internet Addresses

1) _____ 2) _____ 3) _____

For first gateway:

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

Be sure to add IP network addresses and hops for other specified gateways.

NODE WORKSHEET

GATEWAY-HALF NODE INTERNET ROUTING TABLE

NAME OF GATEWAY-HALF NODE:

IP ADDRESS:

NETWORK NAME:

CONNECTED GATEWAY-HALF NODE/ IP ADDRESS	GATEWAY-HALF LINK NAME	DESTINATION NETWORKS/ IP ADDRESSES	HOP COUNT

GATEWAY-HALF CONFIGURATION SCREENS

GLOBAL TRANSPORT CONFIGURATION (NETXPORT.GLOBAL) Fig. 8-4, p. 8-7

Home Network Name _____

Enter the name of a network the node belongs to; the node must have a corresponding LAN or Router NI name configured. Refer to the appropriate maps. If the node belongs to more than one network, the home network should be the one that will allow the greatest number of destination networks a short return path to the node.

LINK CONFIGURATION (LINKCONF) Fig. 7-1, p. 7-4

Link Name _____

Assign a link name that is eight alphanumeric characters or fewer; the first character must be alphabetic. Refer to Gateway-Half Map.

Type: ASNP, LAP-B, BSC Circle one.

ASNP LINK DATA (LINKCONF.*linkname*) Fig. 7-12, p. 7-27

Logical Device _____

The ldev number that will be configured in SYSDUMP.

OR

LAP-B LINK DATA (LINKCONF.*linkname*) Fig. 7-9, p. 7-19

Logical Device _____

The ldev number that will be configured in SYSDUMP.

Local Mode (5=DTE, 6=DCE, 11=HP Point to Point) _____

HP recommends that you use the default, HP Point to Point. If so, both sides of the link must be configured as HP Point to Point.

OR

BISYNC LINK DATA (LINKCONF.*linkname*) Fig. 7-6, p. 7-11

Logical Device _____

The ldev number that will be configured in SYSDUMP.

GATEWAY-HALF CONFIGURATION SCREENS (cont'd)

NETWORK INTERFACE LINKS (NETXPORT.NI.*niName*.LINK) Fig. 11-6, p. 11-16

Type _____

DD--Direct Dial, or DC--Direct Connect

GATEWAY-HALF DIAL LINK CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 11-8, p. 11-19

Gateway Phone _____

The phone number of the remote gateway-half node.

Security String _____

Security String of the remote gateway-half node.

OR

DIRECT CONNECT CONFIGURATION (NETXPORT.NI.*niName*.LINK.*linkname*) Fig. 11-7, p. 11-17

No fields required to configure.

GATEWAY-HALF NETWORK INTERFACE CONFIGURATION (NETXPORT.NI.*niName*) Fig. 11-1, p. 11-3

Idle Device Timeout Value (Minutes) _____

For dial links, this is the number of minutes a device can remain idle (no traffic) before shutting down. A value of zero will disable the idle device timer for all devices on this network interface. (Enter 0 for Direct Connect links.)

IP PROTOCOL CONFIGURATION (NETXPORT.NI.*niName*.PROTOCOL.IP) Fig. 11-3, p. 11-7

IP Address _____

Full IP address of the partner gateway-half node (the node connected to the gateway half being configured). Refer to Gateway-Half Network Interface Table.

GATEWAY-HALF CONFIGURATION SCREENS (cont'd)

NEIGHBOR GATEWAYS (NETXPORT.NI.*niName*.INTERNET) Fig. 11-9, p. 11-23

Gateway Name _____

Assign a name (maximum eight characters) to reference a gateway half that is connected to the node by the gateway-half link previously named. Refer to Catenet Map and Gateway-Half Map.

NEIGHBOR GATEWAY REACHABLE NETWORKS (NETXPORT.NI.*niName*.INTERNET.*gatewayn*) Fig. 11-10, p. 11-24

Neighbor Gateway IP Internet Address _____

Full IP address of the gateway node named above. Refer to Gateway-Half Network Interface Table. This address will match the address configured in the IP Address field listed above.

IP Network Address

- _____ (1)
- _____ (2)
- _____ (3)
- _____ (4)

The IP addresses of all reachable networks in the catenet, through the gateway node named above. Refer to Gateway-Half Node Internet Routing Table. You need to fill out a node portion for each IP Network Address, even though the node portion is ignored. You can simply enter zeros for these node portions.

Hops

- _____ (1)
- _____ (2)
- _____ (3)
- _____ (4)

Refer to Gateway Half Node Internet Routing Table for Hop Count. The numbers in parentheses correspond to the numbers regarding IP network addresses.

SUBSEQUENT GATEWAY-HALF NODES

Home Network Name _____

Link Name _____

Type = ASNP, LAP-B or BSC Circle one.

Logical Device _____

DTE/DCE for LAP-B _____

Is link Direct Dial or Direct Connect _____

If Dial, phone number of remote gateway-half node _____

If Dial, security string of remote gateway-half node _____

Idle Device Timeout Value _____

IP Address of partner gateway half

Gateway name _____

Neighbor Gateway IP Internet Address

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

IP Network Address _____ Hops _____

NETWORK DIRECTORY INFORMATION

After reading the Network Directory section (Section 14), you can complete the information below for all nodes you wish to manually configure into your network directory file.

*Type: 1=IP, 2=IP/LAN802.3

Node Name	Global or Local	IP Address	Type*	Additional Address
--------------	--------------------	------------	-------	-----------------------

SUPPORTED MODEMS

APPENDIX

B

The following modems are supported for NS Point-to-Point 3000/V links:

Line speed (bits/sec)	Modem	Link Protocol
4800	AT&T 2248A	LAP-B
4800	AT&T Dataphone 4800 or AT&T 208B-compatible modems	BSC
9600	CODEX 2640	LAP-B
56000	GTE L500A DSU	LAP-B

AT&T 2248A is the only modem supported for use with LAP-B over full-duplex dial links. Autodial capability is supported by the Bell 801C Auto Call Unit.

The following modems are supported for Asynchronous SERIAL Network links, which use the ASNIP protocol:

Line speed	Modem
1200	Hayes 1200 (HP 92005A) or any other 1200 baud modem that is ATP-compatible
2400	Hayes 2400 (HP 92005B)
2400	U.S. Robotics Courier 2400
1200	HP Remote Support Link modem (HP 3712A)

Autodial capability is supported by the Hayes and U.S. Robotics modems. To use autodial, Hayes 1200 baud modems and U.S. Robotics Courier 2400 modems must use the switch settings shown in Figure B-1; the Hayes 2400 baud modem must receive the commands shown in Figure B-2.

For modem settings for manual dial links, refer to the documentation provided with your modem.

**HAYES SMARTMODEM 1200/U.S. ROBOTICS COURIER
2400 for Asynchronous SERIAL Network Link**

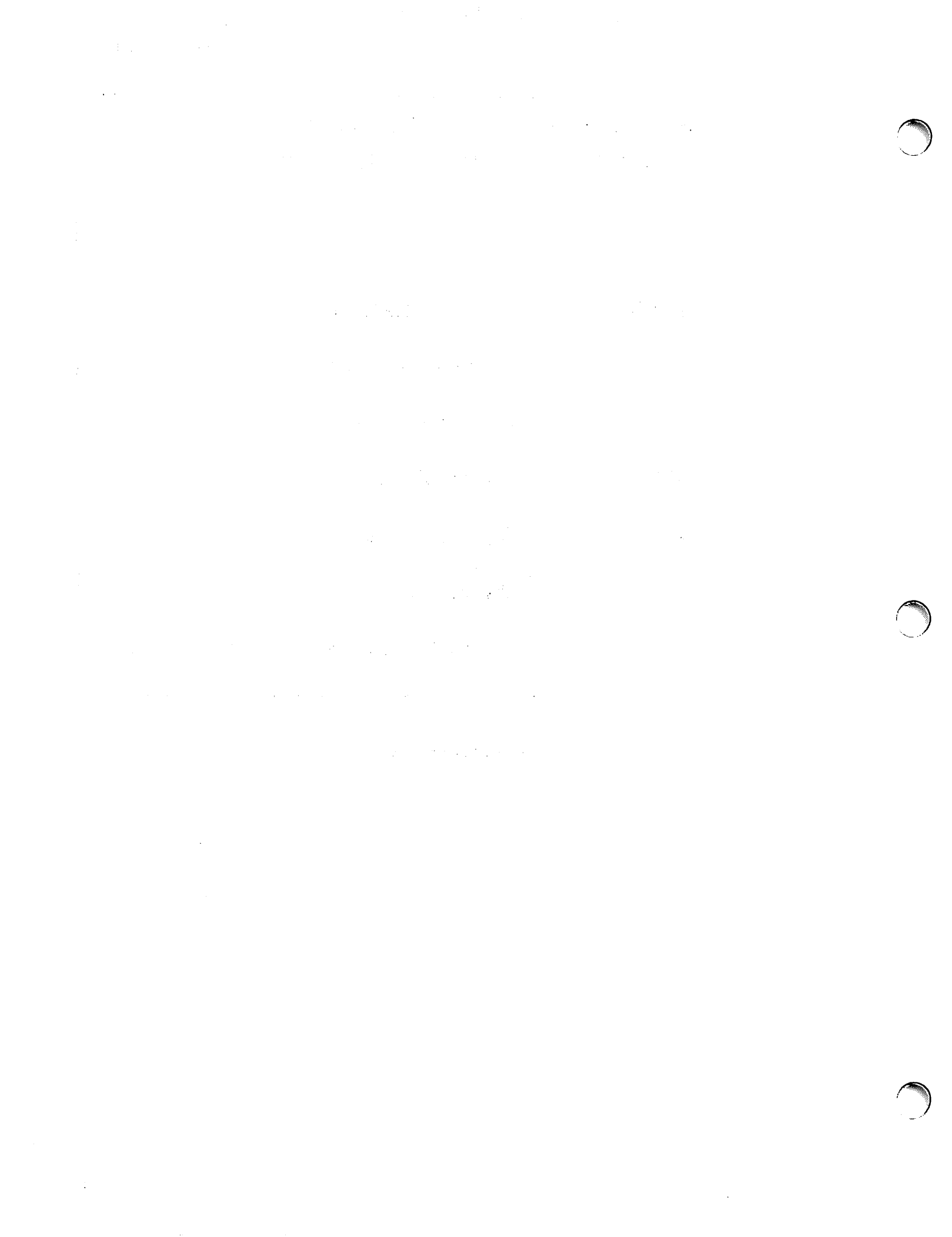
Switch	Setting	Meaning
Switch 1	UP	Supports RS-232C DTR lead
Switch 2	DOWN	Digit result codes
Switch 3	DOWN	Result codes displayed
Switch 4	DOWN	No echo unless half-duplex is selected and modem is on-line
Switch 5	DOWN	Modem will not auto answer a call
Switch 6	UP	Reads status of the RS-232C Carrier Detect lead (Carrier Detection enabled)
Switch 7	UP	Setting for single line telephone installations connected to an RJ 11 jack
Switch 8	DOWN	Enables modem command recognition
Switch 9	UP or DOWN	
Switch 10	UP or DOWN	

Figure B-1. Autodial Switch Settings, Hayes 1200/U.S. Robotics 2400

HAYES SMARTMODEM 2400 for Asynchronous SERIAL Network Link

<u>Command</u>	<u>Meaning</u>
AT&F	Set to factory setting
AT&C1	Reads status of carrier
AT&D3	Support DTR Lead
ATV	Digit result codes
ATE0	Disable echo
AT&W	Write active to nonvolatile memory

Figure B-2. Autodial Commands, Hayes 2400



CONVERTING CONFIGURATION FILES

APPENDIX

C

NMMGRVER.PUB.SYS is a conversion program that enables earlier versions of subsystems to be used with the current version of NMS.

You need to convert files if you open an existing configuration file while using NMMGR and receive this message:

```
Version mismatch found on specified subsystem. Please run NMMGRVER.  
                                                    (NMGERR 53)
```

Also, you need to convert files if you are performing NETCONTROL and receive the following class 2 logging message at the console:

```
Bad CONFIG File Version
```

USING THE CONVERSION PROGRAM

To use this, do the following:

1. Make a backup copy of the existing configuration files before proceeding.

2. Execute NMMGRVER.PUB.SYS by entering:

```
:RUN NMMGRVER.PUB.SYS
```

```
NMS Configuration File Conversion Utility 32099-11018 A.02.00  
(C) Hewlett-Packard Co. 1985
```

3. Respond to the dialogue:

```
Fileset to be scanned?
```

by either pressing the **RETURN** key, which ends the conversion program, or by entering one of the following filesets:

```
filename [.groupname [.acctname]]  
file prefix @ [.groupname [.acctname]]  
@ [.groupname [.acctname]]  
@.@ [.acctname]  
@.@.@
```

Converting Configuration Files

NMMGRVER searches for files of type NCONF in the specified fileset For each file found, it asks:

OK to convert filename.groupname.acctname?

Enter either Y for yes or N for no.

Pressing the **(RETURN)** key is the same as entering N for no.

4. Continue to enter either Y, N, or **(RETURN)** until you have converted all files.
5. Use NMMGR (A. 02. 00) for configuration, if needed.

PC-TO-HP 3000 COMMUNICATION

APPENDIX

D

This appendix summarizes the tasks required for connecting personal computers (PCs) to HP 3000s over ThinLAN/3000, StarLAN/3000 and Asynchronous SERIAL networking links. Connecting PCs and HP 3000s over these links enables PC users to take advantage of Hewlett-Packard software products that make resources and programs operating on the HP 3000 available to PCs. For full details about the HP 3000 tasks that this appendix summarizes, read and follow the instructions given earlier in this manual.

NOTE

This appendix discusses the tasks required for the configuration of an HP 3000 connected to a PC workstation over a ThinLAN/3000, StarLAN/3000 or Asynchronous SERIAL Network Link. For workstation configuration tasks, refer to either the *HP ThinLAN Workstation Installation and Configuration Guide for PCs* (part no. 50909-90040), the *HP StarLAN PC Workstation Installation and Configuration Guide* (part no. 50906-90040), or the *HP SERIAL Network Workstation Installation and Configuration Guide* (part no. 50911-90040). For PC server configuration tasks, refer to either the *HP ThinLAN PC Server Installation, Configuration, and Operation Guide* (part no. 50907-90000) or the *HP StarLAN PC Server Installation, Configuration and Operation Guide* (part no. 50904-90000).

The procedures summarized in this appendix will normally be completed by the individual responsible for managing the networking capabilities of the HP 3000--usually the HP 3000 network manager or HP 3000 system manager. The actual titles and responsibilities of people at your installation may differ from those used here.

Your HP systems engineer may already have completed some or all of these procedures for your network installation. Consult your systems engineer to determine which tasks, if any, already have been completed.

REQUIREMENTS FOR THINLAN/3000, STARLAN/3000, SERIAL LINKS

Software Required

Resource Sharing and virtual terminal access require several Hewlett-Packard software packages. The following lists indicate the software required for different uses of PCs and HP 3000s.

HP 3000 Server Software

An HP 3000 is used as a server with Resource Sharing to provide shared discs, shared printers, and an HP 3000 backup facility. The following software is required for the HP 3000:

- Expanded System Table Microcode (except for the Series 37)
- MPE V/E (UB-Delta-1 MIT) Operating System or later version for ThinLAN; UB-Delta-1 MIT or later for StarLAN.
- NS3000/V Network Services or the services software included with either ThinLAN/3000 Link or StarLAN/3000 Link.
- Productivity Services/3000 Resource Sharing

HP 3000 Host Software

An HP 3000 is used as a host over ThinLAN/3000 Link, StarLAN/3000 Link or Asynchronous SERIAL Network Link for products such as Information Access and AdvanceMail. The following software is required on the HP 3000 when operating as a host over these links:

- Expanded System Table Microcode (except for the Series 37)
- MPE V/E (UB-Delta-1 MIT) Operating System or later version for ThinLAN and StarLAN (Note: If AdvanceLink is the only host-to-PC product in use, the U-MIT version of MPE V/E is acceptable.) For SERIAL, UB-Delta-3 MIT or later is needed.
- NS3000/V Network Services or the services software included with either ThinLAN/3000 Link, StarLAN/3000 Link, or Asynchronous SERIAL Network Link.

Software for a PC Workstation Using Server Resources

A PC used as a workstation on the network can use the network to perform certain tasks. The following software is required for the PC if it is using a PC server's or HP 3000 server's shared resources:

For ThinLAN

- Version 3.1 or later (Version 3.2 recommended) of the DOS operating system and utilities
- Version A.03.00 or later of the HP ThinLAN User Link Software for Vectra/IBM PCs or Version A.03.00 or later of the HP ThinLAN User Link Software for Touchscreen PCs

For StarLAN

- Version 3.1 or later (Version 3.2 recommended) of the DOS operating system and utilities, and
- Version A.01.00 or later of the HP StarLAN User Link Software for Vectra/IBM PCs

For SERIAL

- Version 3.1 or 3.2 of the DOS operating system and utilities.
- Version A.01.00 or later of the HP SERIAL Network User Link Software for Vectra/IBM PCs or Version A.03.00 or later of the HP SERIAL Network User Link Software for Touchscreen PCs

Software for a PC Workstation Used as a Terminal

A PC workstation can use AdvanceLink to communicate with an HP 3000 host computer as though the workstation were a terminal connected to the HP 3000 by RS-232 cable. When used as a terminal, the following software is required for the PC:

For ThinLAN

- Version 3.1 or later (Version 3.2 recommended) of the DOS operating system and utilities
- Version A.03.00 or later of the HP ThinLAN User Link Software for Vectra/IBM PCs or Version A.03.00 or later of the HP ThinLAN User Link Software for Touchscreen PCs
- Version A.03.02 or later of the HP AdvanceLink (for HP Touchscreen PCs) or HP AdvanceLink 2392 (for HP Vectra PCs and IBM PC/XT/ATs).

For StarLAN

- Version 3.1 or later (Version 3.2 recommended) of the DOS operating system and utilities
- Version A.01.00 or later of the HP StarLAN User Link Software for Vectra/IBM PCs
- HP AdvanceLink 2392 (for HP Vectra PCs and IBM PC/XT/ATs).

For SERIAL

- Version 3.1 or 3.2 of the DOS operating system and utilities.
- Version A.01.00 or later of the HP SERIAL Network User Link Software for Vectra/IBM PCs or Version A.03.00 or later of the HP SERIAL Network User Link Software for Touchscreen PCs.
- Version A.03.02 or later of the HP AdvanceLink (for HP Touchscreen PCs) or HP AdvanceLink 2392 (for HP Vectra PCs and IBM PC/XT/ATs).

NOTE

A PC being used as both a terminal and as a workstation sharing a server's resources requires the software listed under "For a PC Workstation Used as a Terminal." One copy of DOS and utilities and either HP ThinLAN User Link Software, HP StarLAN User Link Software, or HP SERIAL Network User Link Software is needed for each workstation.

Related Publications

You should refer to the following Hewlett-Packard documentation when configuring a PC workstation or HP 3000:

HP ThinLAN for PCs

- *HP ThinLAN Workstation Installation and Configuration Guide for PCs* (part no. 50909-90040)
- *HP ThinLAN Planning and Hardware Guide for PCs* (part no. 50909-90020)

HP StarLAN for PCs

- *HP StarLAN PC Workstation Installation and Configuration Guide* (part no. 50906-90040)
- *HP StarLAN Planning Guide for PCs* (part no. 50906-90020)
- *HP StarLAN Hardware Installation Manual for PCs* (part no. 5959-2222)

HP SERIAL Network

- *HP SERIAL Planning and Hardware Guide* (part no. 50911-90020)
- *HP SERIAL Network Workstation Installation and Configuration Guide* (part no. 50911-90040)
- *HP StarLAN Quick Reference* (part no. 5959-2227)
- *Quick Task Reference Card* (part no. 5959-1504)

Resource Sharing

- *Resource Sharing: System Management* (part no. 32597-90001)
- *Resource Sharing: Utilities* (part no. 32597-90002)

NS3000/V Links

- *NS3000/V Network Manager Reference Manual* (part no. 32344-90002)

Other HP manuals describe additional products that use the HP 3000 as a host. Consult your HP representative for information on additional products and the publications that describe them.

NOTE

Although this appendix outlines required PC configuration tasks, the tasks are described in detail in only the manuals listed above for HP ThinLAN for PCs, HP StarLAN for PCs and HP SERIAL networks. The specific manual or sections of this manual to which you should refer for more information about a particular task are noted throughout this appendix.

Hardware and Software Installation

Before you can attempt the procedures summarized in this appendix, the installation of certain hardware and software already must be completed on either each PC workstation being configured or on the HP 3000. Before you begin the procedures summarized on the following pages, make sure that:

For HP 3000s

- A hardware card (LANIC for IEEE802.3 networks, ATP for SERIAL networks) is properly installed in the backplane of the HP 3000
- Resource Sharing is installed on the HP 3000, if Resource Sharing will be used.
- (For Resource Sharing only) Public shared discs and shared printers, if applicable, have been set up on the HP 3000 with the RESMGR utility
- Modems for remote HP SERIAL Network Links have been set up.

For PC Workstations

- The network is planned as described in the *HP ThinLAN Planning and Hardware Guide for PCs*, the *HP StarLAN Planning Guide for PCs* or the *HP SERIAL Planning and Hardware Guide*, and a "User Reference Worksheet" has been filled out for each workstation.
- The required network hardware is set up, as described in the *HP ThinLAN Planning and Hardware Guide for PCs*, the *HP StarLAN Hardware Installation Manual for PCs*, or the *HP SERIAL Planning and Hardware Guide*.
- Each workstation's software is installed, either on work discs or on a fixed disc, as described in the *HP ThinLAN Workstation Installation and Configuration Guide for PCs*, the *HP StarLAN PC Workstation Installation and Configuration Guide*, or the *HP SERIAL Network Workstation Installation and Configuration Guide*.

If PC servers are also being used as part of the network, they should also be configured before the tasks described in this appendix are begun. For more information on configuring PC servers, refer to either the *HP ThinLAN PC Server Installation, Configuration, and Operation Guide* or the *HP StarLAN PC Server Installation, Configuration, and Operation Guide*.

HP 3000 Logon and Shortname Correspondence

The PC network manager and HP 3000 system manager should agree upon HP 3000 account pathnames (user logons, groups, accounts, and access permissions) and corresponding shortnames before the tasks summarized in the following pages are begun.

CONFIGURATION PROCEDURES SUMMARY

The following sections summarize the tasks that must be completed to configure PC workstations and HP 3000s in order to use the HP 3000 as a server to PC workstations (via Resource Sharing), to use HP AdvanceLink, and for other software products that use the HP 3000 as a host.

The configuration tasks can be divided as shown in the table below and as described in the following sections.

Task	Done By	Reference
Configuring the PC workstation with the USRCONFIG utility and loading PC workstation network software	PC network manager	<p><u>For ThinLAN</u>-- <i>HP ThinLAN Workstation Installation and Configuration Guide for PCs</i></p> <p><u>For StarLAN</u>-- <i>HP StarLAN PC Workstation Installation and Configuration Guide</i></p> <p><u>For SERIAL</u>-- <i>HP SERIAL Network Workstation Installation and Configuration Guide</i></p>
Configuring the HP 3000	HP 3000 network manager	<p>Sections 5-14 of this manual</p> <p><i>Resource Sharing: System Management (for Resource Sharing only)</i></p>
Assigning HP 3000 Logons	HP 3000 system manager	<i>System Operation and Resource Management Reference Manual</i>

PC Workstation Tasks

After the HP 3000 has been configured, configure the PC workstation and load PC workstation network software. Refer to the manuals listed above.

Configuring the HP 3000

(HP 3000 network manager)

Two utilities are used to configure the HP 3000: SYSDUMP and NMMGR. SYSDUMP is used to configure the hardware card that has been installed in the backplane of the HP 3000.

NOTE

A hardware card must be installed on the HP 3000 before any further configuration tasks can be performed. Consult your HP 3000 network manager or HP Systems Engineer for more information.

Refer to Section 4 of this volume for instructions on configuring the hardware card with SYSDUMP.

Once the hardware card has been installed, configuring the HP 3000 to support Resource Sharing, AdvanceLink, or other products that use the HP 3000 as a host consists of two main tasks:

- Configuring additional virtual terminals (VTERMs) with the SYSDUMP utility
- Configuring the HP 3000 as part of an NS3000/V network with the NMMGR utility. (Note: this appendix assumes that the HP 3000 has not been previously configured as a node on an NS3000/V network. If the HP 3000 *has* been configured already, some configuration changes may be required. These are noted later in this appendix.)

Configuring Additional Virtual Terminals

To configure additional virtual terminal (VTERM) devices, you must run the HP 3000 SYSDUMP utility. The following paragraphs explain how to determine the number of additional VTERMs needed:

At least one additional VTERM is required for each PC workstation. This includes PCs that are using the HP 3000 as a server, as a host for various application software, and for PCs using AdvanceLink for terminal access to the HP 3000.

You may choose to configure more VTERMs than will be currently required by your network installation so that if PC workstations are later added to the network, you will not always have to reconfigure the number of VTERMs. HP suggests that to allow for your network's future growth, you use a formula such as the following to determine the number of additional VTERMs to configure:

1. Calculate a value based on the number of PCs using the HP 3000 as a server: For the first PC using the HP 3000 as a server, the number of virtual terminals required is 6. Each additional PC using the HP 3000 as a server (via Resource Sharing) requires 1.5 additional VTERMs.

2. Calculate a value based on the number of PCs using AdvanceLink or other software using the HP 3000 as a host: For each PC using AdvanceLink or other software using the HP 3000 as a host, the number of virtual terminals required is 1.
3. Add the values determined in steps 1 and 2, and round up to the next highest whole number if necessary.

For example, if four PC workstations will be using Resource Sharing and two of those will be using AdvanceLink, and a fifth PC will be using only AdvanceLink, you would configure:

4 PCs using Resource Sharing: $6 + 1.5 + 1.5 + 1.5 = 10.5$

3 PCs (total) using AdvanceLink: $1 + 1 + 1 = 3.0$

Total: 13.5

Rounded up = 14 VTERMs

Refer to Section 4 for information on running SYSDUMP for network configuration.

Configuring the HP 3000 Network Configuration File (NSCONF.NET.SYS)

This subsection describes the minimum tasks that must be performed to configure an HP 3000 as a node on an NS3000/V IEEE802.3 network or an NS3000/V Asynchronous SERIAL network. For details, refer to sections 5-10, 13 and 14.

Consult your HP 3000 network manager or your HP systems engineer before attempting the tasks described here.

NMMGR is a screen-based utility. This means that as you press function keys or type in commands, a series of display screens appear at your terminal. Various fields displayed within each screen correspond to configurable items; configuration occurs when values are typed into the fields and recorded.

The following tables contain two types of fields in the Item column. One type is a field that must be user-configured as part of a minimum network configuration. These are items for which no default value is supplied. Guided Configuration visits all screens that include such items. The other type is a field that has a default value but may need to be changed depending on the size of the network. The tables include the type of the item in the Requirement Status column. The screen on which an item appears is listed in the Screen column.

To reach screens not visited by guided configuration, you need to use manual configuration. See Section 5 for details.

NOTE

If your HP 3000 is already part of an NS3000/V network, you may have to alter some fields in the following tables, but you will not need to configure the HP 3000 node name, IP address, or LDEV number, as they will have been configured already.

Internet screens and LAN mapping screens are not shown in the table because they are not necessary for this discussion of PC-to-HP 3000 communication. However, when configuring the HP 3000 as part of a LAN, mapping must be configured about any nodes on the LAN that do not support the Probe Protocol (e.g. non-HP 3000 nodes). Internet routing screens, no matter what network type, must be visited if you want the HP 3000 to be able to communicate with other networks that are part of the same catenet. See sections 9 and 10 for more information.

Also, the Probe Protocol screen is not included in the LAN table. This screen, described in detail in Section 9, is used when you want to configure an HP 3000 as a proxy server containing directory information about all nodes in the catenet.

The term "node name" in this appendix has the same meaning as "computer name" in HP networking PC manuals.

For ThinLAN and StarLAN Networks

Screen	Item	Requirement Status
GUIDED NETWORK INTERFACE CONFIGURATION	Network interface name.	Required.
NODE NAME CONFIGURATION	HP 3000 node name.	Required. Keep track of this node name, including its <i>domain</i> and <i>organization</i> fields, because you will need it during configuration of a PC workstation with the USRCONFIG utility.
LINK CONFIGURATION	Link Name.	Required.
LINK CONFIGURATION: IEEE 802.3 LINK DATA	LANIC card's LDEV number.	Required.
IP PROTOCOL CONFIGURATION	HP 3000 IP address.	Required.

For ThinLAN and StarLAN Networks (continued)

Screen	Item	Requirement Status
<p>GLOBAL TRANSPORT CONFIGURATION</p>	<p>Maximum directly connected nodes and maximum inbound destinations. (Values for these fields should be greater than or equal to the number of nodes, including PC workstations and PC servers, in the network.)</p>	<p>Use the default unless number of network nodes (including PC workstations and servers) exceeds 100.</p>
<p>TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION</p>	<p>Maximum number of connections.</p>	<p>Use the default unless maximum number of connections in use at one time will exceed 128 (the default). This value should allow for two connections for each concurrent usage of Resource Sharing and one connection for each concurrent usage of other network applications and services.</p>
<p>LAN802.3 NETWORK INTERFACE CONFIGURATION</p>	<p>Maximum number of nodes in network (to include all PC workstations and servers).</p> <p>Number of outbound buffers.</p>	<p>Use the default unless number of nodes in network exceeds 100 (the default).</p> <p>Use the default unless maximum number of connections configured in TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION screen is greater than 128.</p>

For SERIAL Networks

Screen	Item	Requirement Status
GUIDED NETWORK INTERFACE CONFIGURATION	Network Interface Name.	Required.
NODE NAME CONFIGURATION	HP 3000 node name.	Required. Keep track of this node name, including its <i>domain</i> and <i>organization</i> fields, because you will need it when you configure the PC workstation with the USRCONFIG utility.
LINK CONFIGURATION SCREEN	Link Name.	Required.
LINK CONFIGURATION: ASNP LINK DATA	Logical Device (LDEV) number. Subtype (hardwired, modem, European modem).	Required. Check that the default is correct for your implementation.
ROUTER NETWORK INTERFACE LINKS	Link name and link type to be established between the HP 3000 and the PC workstation. NMMGR offers three options to indicate the type of link to be established: Direct Connect, Shared Dial, and Direct Dial.	Required. This value must also be entered in the USRCONFIG utility.
IP PROTOCOL CONFIGURATION	HP 3000 IP address.	Required.

For SERIAL Networks (continued)

Screen	Item	Requirement Status
<p>GLOBAL TRANSPORT CONFIGURATION</p>	<p>Maximum directly connected nodes and maximum inbound destinations. (Values for these fields should be greater than or equal to the number of nodes, including PC workstations and PC servers, in the network.)</p>	<p>Use the default unless number of network nodes (including PC workstations and servers) exceeds 100.</p>
<p>TRANSMISSION CONTROL PROTOCOL (TCP) CONFIGURATION</p>	<p>Maximum number of connections.</p>	<p>Use the default unless maximum number of connections in use at one time will exceed 128 (the default). This value should allow for two connections for each concurrent usage of Resource Sharing and one connection for each concurrent usage of other network applications and services.</p>
<p>DIAL ID PROTOCOL CONFIGURATION</p>	<p>YES/NO decision for an HP 3000 security string.</p>	<p>If you want a security string, enter yes. If you do not want a security string, enter no. The YES or NO entry, must also be entered in the USRCONFIG utility.</p>
<p>SECURITY STRING(S) CONFIGURATION</p>	<p>HP 3000 security string.</p>	<p>Required if the Security On Field has been set to YES.</p>

For SERIAL Networks (continued)

Screen	Item	Requirement Status
ROUTER MAPPING CONFIGURATION	Node name of the PC workstation (or a name to represent a route to the PC workstation.)	Required for NMMGR. The actual nodename of the workstation is required in the USRCONFIG utility.
ROUTER REACHABLE NODES	The IP address of the PC workstation. Link Name. Entry priority.	Required. This value must also be entered in the USRCONFIG utility. Required. Use default unless more than one phone number has been allocated to a single IP address.

NOTE

An HP 3000 on a SERIAL network also must have a network directory configured. On an IEEE802.3 network, a directory needs to be configured only if the HP 3000 will be a proxy server. Section 14 describes the network directory. The network directory must contain the node name of each PC connected to an HP 3000, as well as the proper IP address associated with the PC.

For information on configuring additional items, as well as complete information on configuring with NMMGR, refer to sections 5-14.

For information on configuring the HP 3000 as a node on the network in order to operate Resource Sharing, refer to *Resource Sharing: System Management*.

Assigning HP 3000 Logons

(HP 3000 system manager)

For each PC user using AdvanceLink or AdvanceLink 2392 for HP 3000 access, the HP 3000 System Manager should assign a user logon. Refer to the *System Operation and Resource Management Reference Manual* for information about assigning user logons.

For each PC user using Resource Sharing, assign Resource Sharing automatic logons with the RESMGR utility. Refer to *Resource Sharing: Utilities* for more information.

PC-To-HP 3000 Communication

The configuration of PC user logons may vary for different application software products. Refer to the documentation provided for a particular product for information about logon configuration.

DS vs NS INP Configuration

APPENDIX

E

The SYSDUMP items described in the following table used to configure an INP for a DS point-to-point link must be examined for consistency with NS if you choose to use the same INP for an NS point-to-point link. Note that some values entered in SYSDUMP are overridden in NMMGR for an NS link.

Table E-1. DS vs NS INP Configuration

Item in SYSDUMP	DS Default	NMMGR (NS) Default	NMMGR Screens, Fields, and Comments
Subtype	none	-	Not configurable. NMMGR overrides any value entered in SYSDUMP
Receive Timeout	20 sec.	-	Not configurable (usually overridden by subsystem)
Local Timeout	60 sec.	60 sec. (for LAP-B) BSC not configurable	Local timeout field on LAP-B Link Data screen
Connect Timeout	300 sec. for dial links, 120 for non-dial links	900 sec. (for LAP-B and BSC)	Connect Timeout field in LAP-B Link Data screen, or BSC Link Data screen
Speed Changeable	none	none	For NS links must enter <u>YES</u> in SYSDUMP.
Dial Facility	none	autodial (LAP-B & BSC)	Manual or Autodial field in LAP-B Link Phone Data screen, or BSC Link Phone Data screen.
Transmission Mode	none	-	Not configurable. Hard-coded: LAP-B: full duplex BSC: half duplex
Transmission Speed	none; value is specified in bytes/second	9600 bits/second	Line speed in bits/second field LAP-B Link Data screen, or BSC Link Data screen

Table E-1. DS vs NS INP Configuration

Item in SYSDUMP	DS Default	NMMGR (NS) Default	NMMGR Screens, Fields and Comments
Phonelist/ Phone Number	none	none	Phone Number field in Router Reachable Nodes screen or Gateway Dial Link Configuration screen.
Local/Remote ID Sequence	none	none	Security String field in Router Reachable Nodes screen, or Gateway Dial Link Configuration screen. For an INP used both as a DS and a NS link, local/remote ID sequences are ignored by NS but are still valid for DS.
Virtual terminal configured for INP DRT#	none	none	For NS links, back reference to the console. Do not back reference to a DS link INP.

GLOSSARY

A

address - in networking, a numerical identifier defined and used by a particular protocol and associated software to distinguish one node from another.

address resolution - in NS networks, the mapping of node names to IP addresses and the mapping of IP addresses to subnet addresses.

adjacent - describes a node on a router network that is connected to another node by a single link, with no intervening nodes.

Advanced Terminal Processor (ATP) - a hardware card that fits into the backplane of the HP 3000 and that provides a physical layer interface for Asynchronous SERIAL Network Links.

Asynchronous Serial Network Protocol (ASNP) - a Data Link Layer protocol used for Asynchronous SERIAL Network Links.

ASNP - see Asynchronous Serial Network Protocol

ATP - see Advanced Terminal Processor

autodial - describes a dial link in which the remote node's telephone number is automatically dialed by modem or other device with this capability.

AUI cable - Attachment Unit Interface cable, a cable joining the LANIC to the MAU (Media Attachment Unit) for coaxial cable IEEE 802.3 local area network links.

B

Bisynchronous Communication protocol - see BSC protocol.

boundary - see network boundary.

broadcast - a method of communication in which all nodes on the network share the same communications channel (referred to as the communications bus). Messages are transmitted to all nodes on the same bus at the same time. IEEE 802.3 networks are broadcast networks.

brother branching - the process of proceeding to another screen in NMMGR by using the NEXT command. The screen displayed after entering NEXT will be one on the same hierarchal level as the current screen in the configuration tree structure.

BSC protocol - a data link layer protocol that can be used over NS Point-to-Point 3000/V Links that use dial links (switched lines). BSC is an acronym for the Bisynchronous Communication protocol.

buffer - a logical grouping of a system's memory resources used by NS3000/V.

C

catenet - a group of computer networks that are connected to one another.

Catenet Administrator - the person having responsibility for coordinating network management tasks among all networks in the catenet.

catenet lifecycle - see lifecycle, network/catenet

central administrative node - a node designated as the node in the catenet to be the first one updated with new or changed internet routing and network directory information about any other nodes in the network.

Communications Services (CS/3000) - software included with NS3000/V links that provides some diagnostic and link management software.

computer name - term used in some HP networking documentation to refer to node name. (See node name.)

computer network - a group of computer systems connected in such a way that they can exchange information and share resources.

configuration - the process of defining the characteristics of the network in software. Two kinds of configuration must be performed for each node in an NS3000/V network: system configuration, accomplished with the SYSDUMP utility, and network configuration, accomplished with the NMMGR utility.

CSLIST - a utility that lists version numbers for the software modules of the CS/3000 subsystem, and provides information on the INP and LANIC download files.

CSDUMP - A utility that formats files created by the CSTRACE utility, which traces link activities.

DADCONF.PUB.SYS configuration file - a file that must be installed to allow initialization of purchased network services. This file must be created after system configuration has occurred, and the SYSDUMP tapes are loaded, and before network configuration with NMMGR.

D

data screen - a type of screen displayed by NMMGR that allows you to configure data.

Dial ID protocol - a proprietary Hewlett-Packard protocol that provides security checking and address exchange for dial links.

dial link - a connection between network nodes made through public telephone lines.

direct path branching - the process of proceeding from screen to screen in NMMGR by entering path names in the Path: field.

directly connected - describes nodes that are members of the same network.

distributed network - a computer network in which connected systems are independent and equally in control of the network's operation.

DSLIS - a utility that lists the version numbers of software modules that are part of the DS subsystem of NS3000/V.

DSDUMP - a utility that can format link trace files created with CSTRACE. Formatting with DSDUMP rather than CSDUMP provides more information on the data link and network level activities when the BSC or X.25 protocols are in use.

DSM - the INP Diagnostic Support Monitor, a utility used to test INP cards.

driver - software that controls I/O devices, including NS3000/V links.

E

entry, network directory - the data in a network directory that consists of a node's name and its path report list.

entry priority - the ranking used to identify the most desirable to the least desirable routes used to reach a given remote node from a given local node in a router network.

environment - a session established on a remote node.

F

full gateway - a node that is a member of more than one network. Because it is a member of more than one network, the node can pass messages from one network to another.

G

gateway - a node that can provide communication between networks. A gateway can be either a full gateway or a gateway half.

gateway half - a node that, in conjunction with another node on another network, performs the function of a gateway. Together, two gateway halves can link two networks in the same catenet.

gateway half link - A link that joins two nodes that form a gateway half pair. The link must be configured as the link used for the gateway half network interface at each of the two nodes. The NS Point-to-Point 3000/V Link and the Asynchronous SERIAL Network Link can be used as gateway half links.

gateway half pair - a set of two nodes that are joined by a gateway half link. Each node in the pair must have a gateway half network interface configured, using that link.

gateway node - a node used to connect networks in the same catenet. To be a gateway node on an NS3000/V network, a node must be configured as part of more than one network, or must be configured as a gateway half in conjunction with another gateway half node on another network.

general protocols - protocols used by an NS3000/V node regardless of link type: these are the IPU (IP Update), TCP, and PXP protocols.

global entry - a network directory entry that can be merged into other directories, and that can therefore be used by other nodes in the network.

Guided Configuration - a method of configuring a node in which a subset of the complete NMMGR interface is presented, and in which defaults of configurable values are used automatically.

H

hop count - see internet hop count and intranet hop count.

I

IEEE 802.3 - a standard for a broadcast local area network published by the Institute for Electrical and Electronics Engineers (IEEE).

IEEE 802.3 networks - networks whose operation is based on the IEEE 802.3 standard for local area networks. ThinLAN/3000, LAN3000/V, and StarLAN/3000 are NS3000/V links that can be used to create IEEE 802.3 networks.

inbound - pertaining to data being received at a given node.

INPDPAN - INP Dump Analysis, a utility that generates a formatted dump of an INP log file. An INP log file is generated when an error occurs; it contains the contents of the INP memory.

Intelligent Network Processor (INP) - a hardware card that fits into the backplane of the HP 3000 and provides a physical layer interface for NS Point-to-Point 3000/V Links. The INP is also used for DS links; however, a single INP cannot provide an interface for an NS link and a DS link concurrently.

internet communication - communication that occurs between networks.

Internet Protocol (IP) - a protocol used to provide routing among different networks in the same catenet, as well as among nodes in the same router network. The Internet Protocol corresponds to layer 3, the Network Layer, of the OSI model.

internet hop count - the number of gateways that are used to route a message to its destination network.

intranet communication - communication that occurs between nodes in a single network.

intranet hop count - the number of intermediate nodes that lie between a source and destination node on the same router network.

IP address - an address used by the Internet Protocol to perform internet routing, and used to provide intranet addresses in NS3000/V router networks.

IP - see Internet Protocol.

IPC line test - a software program that tests whether the Network Transport is operating correctly.

L

LANDPAN - LANIC Dump Analysis, a utility that generates a formatted dump of a LANIC log file. The LANIC log file is produced when an error occurs; it contains the contents of the LANIC memory.

LANIC - see Local Area Network Interface Controller

LANIC Self-Test - a ROM-based program on the LANIC card that tests and reports the status of LANIC hardware.

LANDIAG - LAN Node Diagnostic, an interactive utility designed to help identify malfunctioning hardware components of the LAN3000/V Link.

LAP-B (Link Access Procedure, Balanced) protocol - a data link layer protocol that can be used by NS Point-to-Point 3000/V Links. LAP-B must be used over direct-connect NS Point-to-Point 3000/V Links.

leased line - data-grade telephone lines leased directly to a subscriber and allocated specifically for the subscriber's needs.

lifecycle, network/catenet management - the stages of development of a network or catenet. The four stages consist of design, implementation, operation, and tuning and growth.

line speed - a measure of the rate at which data passes through a physical link (usually measured in bits or kilobits per second).

link product - one of the NS3000/V Links: the NS Point-to-Point 3000/V Link, the ThinLAN/3000 Link (including the LAN3000/V thick cable option), and the Asynchronous SERIAL Network Link. Each link product consists of software and hardware that together perform the functions of layers 1 through 4 of the OSI 7-layer networking model.

Link Support Services - an NS3000/V software subsystem that opens, closes, and otherwise controls physical links.

Local Area Network Interface Controller (LANIC) - a hardware card that fits into the backplane of the HP 3000 and provides a physical layer interface for IEEE 802.3 local area networks.

local entry - a network directory entry that cannot be distributed to other nodes in the network.

local node - the node (computer that is part of a network) that you are currently using or referring to.

logging - the process of recording the usage of network resources. NS3000/V logging is performed at three levels: network, event, and link levels.

log class - a designation indicating the subset of information that will be logged.

loopback - the routing of messages originating from a node to that node itself.

M

manual dial - describes a dial connection in which the remote node's telephone number must be physically entered by someone such as the system operator

map, catenet or network - a drawing of a network or catenet that shows its topology, node and network names, addresses, network boundaries (for a catenet map), and link types.

mapping - A set of characteristics that describe a route taken by messages to reach a destination node. This set of characteristics is configured with NMMGR at every node on a router network. One mapping is configured at each node for every other node on the network to which messages will be sent.

MAU - Media Attachment Unit, a device attached to a coaxial cable for a LAN3000/V Link. The MAU provides physical and electrical connection from the AUI cable to the coaxial cable.

menu screen - a type of screen displayed by NMMGR that allows you to select an NMMGR function, such as proceeding to a certain configuration branch, refreshing the screen display, or returning to the previously displayed screen.

MPE-V - Multiprogramming Executive V, the operating system of Series 37 through 70 HP 3000s and MICRO 3000s. NS3000/V operates in conjunction with the MPE-V operating system.

N

name - In the context of NS3000/V networks, a name is a character string used to identify some portion or component of a network or catenet.

neighbor gateway - a gateway that is in the same network as a given node.

neighbor node - a node that is in the same network as a given node.

NetIPC - Network Interprocess Communication, software that enables programs to access network transport protocols.

network - see computer network.

network address - the network portion of the IP address. The IP address consists of a network portion and a node portion.

network architecture - the plan that defines the characteristics and interactions of the hardware and software used to create a network.

network boundary - the logical division between networks in a catenet.

network directory - a file containing information required for one node to communicate with another node in the catenet. The active network directory on a node must be named NSDIR.NET.SYS.

network interface - the collective software that provides an interface between a system and a network. A node will possess a network interface for each of the networks to which it belongs, and for each of the gateway half links of which it is a part.

network management - the collective tasks required to design, install, configure, maintain, and if necessary, change a network.

network management lifecycle - see *lifecycle, network/catenet*

network manager - the person responsible for performing and coordinating network management tasks for an entire network.

Network Transport - software that corresponds to layers 3 and 4 of the OSI network architecture model. The function of this software is to send data out over the appropriate communications link, and to receive incoming data, and to route the incoming or outgoing data to the appropriate destination node.

NFT - Network File Transfer, the Network Service that transfers disc files between nodes on the network.

NMCONFIG.PUB.SYS configuration file - The configuration file containing information needed for link level and NetIPC logging.

NMDUMP - a utility used to format log and trace files.

NMMAINT - a utility that lists the software module version numbers for all HP AdvanceNet products, including NS3000/V.

NMMGR - see *Node Management Configurator*

node - a computer that is part of a network.

node address - the node portion of the IP address, which consists of a node portion and a network portion.

Node Management Configurator (NMMGR) - an NS3000/V software subsystem that enables you to configure each node on a network.

Node Management Services - an NS3000/V software subsystem that provides configuration file version checking and logging.

Node Manager - the person responsible for performing network management tasks for a node on a network.

node name - a character string used to identify each system that is a node in a network or catenet. Each node name in a network or catenet must be unique; however, a single node can be identified by more than one node name.

non-adjacent - describes a node on a router network that is separated from a given node by intervening, or intermediate nodes.

NSCONF.NET.SYS - Default name, and name recommended by HP for the network transport configuration file residing on each node. This name is used throughout the *NS3000/V Network Manager Reference Manual* to refer to this configuration file.

NSDIR.NET.SYS - Name of the active network directory file. For convenience, this name is used throughout the *NS3000/V Network Manager Reference Manual* to refer to the network directory file.

NS3000/V - a Hewlett-Packard data communications product that provides networking capabilities for HP 3000 minicomputers. NS3000/V also provides communication between HP 3000s and other types of computers

NS3000/V Network Services - software applications that can be used to access data, initiate processes, and exchange information among nodes in the network. The services are: RPM, VT, RFA, RDBA, NFT, and PTOP.

NS3000/V Link - software and hardware that provides the connection between nodes on a network. Four NS3000/V links are available: the NS Point-to-Point 3000/V Link, the ThinLAN/3000 Link (including the ThickLAN thick cable option), StarLAN/3000 Link, and the Asynchronous SERIAL Network Link.

O

outbound - pertaining to data being sent from a given node.

OSI (Open Systems Interconnection) model - a model of network architecture devised by the International Standardards Organization (ISO). The OSI model defines seven layers of a network architecture, each layer performing specified functions.

P

Packet Exchange Protocol (PXP) - a Transport Layer protocol used in NS3000/V links to initially establish communication between nodes when the NetIPC socket registry is used.

partner gateway half - two gateway halves connected by a link and configured to provide communication between two networks are partner gateway halves.

path name - in configuration with NMMGR, a string that can be typed in the "Path:" field of NMMGR display screens that causes another screen to appear. Each screen has a unique path name that corresponds to its location in the hierararchy of configuration screens presented by NMMGR.

path report - a data structure containing name-to-address mapping information for a node, as well as the networking protocols used by the node for its interface to a given network.

path report list - the set of all path reports for a node, which includes path reports for all the networks the node belongs to.

point-to-point network - networks in which messages are transmitted from node to node in the network over a defined route until reaching their destination.

pool - virtual terminals are configured in groups called pools. A pool of virtual terminals is shared by all NS communications devices on a system.

Probe protocol - an HP protocol used by nodes on NS3000/V IEEE 802.3 networks to obtain information about other nodes on the network.

Probe proxy server - a node on an IEEE 802.3 network that possesses a network directory and is therefore used to provide information about nodes on other networks in the catenet to nodes on the IEEE 802.3 network.

protocols - the rules and conventions that define the functions to be performed and the format of messages exchanged by each layer of network architecture.

PTOP - Program-to-Program Communication, the Network Service that allows programs residing on different nodes to exchange information with one another in a master/slave relationship.

PXP - see Packet Exchange Protocol.

Q

QuickVal - a software program that tests whether Network Services are operating correctly between nodes.

R

RDBA - Remote Data Base Access, the Network Service that allows users to access data bases on remote nodes.

reachable network - a network that can be accessed (with additional internet hops possibly required) by a particular gateway.

remote node - a node on the network other than the node you are currently using or referring to.

resolution, of names and addresses - see address resolution.

RFA - Remote File Access, the Network Service that allows users to access files and devices on remote nodes.

RPM - Remote Process Management, the Network Service that allows a process to programmatically initiate and terminate other processes throughout a network from any node on the network.

router network - one of the types of networks that can be created with NS3000/V link products. Router networks are point-to-point networks. The NS Point-to-Point 3000/V Link and the Asynchronous SERIAL Network Link can be used to create router networks.

routing - the process used to determine the path that packets, or pieces of a message, take through a network or catenet to reach a destination node.

S

security string - an alphanumeric character string that functions as a password for dial links. The security string is used by the Dial ID protocol.

select screen - a type of screen displayed by NMMGR that allows you to select identifiers (such as names) to add, delete, rename, or update.

shared dial - describes a dial link that provides connection to more than one remote system, although to only one at a time.

station address - a link-level address used by the IEEE 802.3 protocol that is assigned to every node on an IEEE 802.3 network.

store-and-forward - a technique in which messages are passed from one node to another in a network to reach their destination. Point-to-point networks use the store-and-forward technique to transmit messages.

subnet - another name for a network especially if the network is part of a catenet. The word subnet is also a synonym for intranet

synchronization - the process of creating and modifying network directories so that all directories in the network or catenet are identical or at least contain the information required for the network to operate as planned.

SYSDUMP - the software program that allows you to perform system configuration on HP 3000s.

system configuration - the means of defining to MPE-V the peripheral devices attached to the HP 3000 for the input and output of data, and the parameters required for system operation.

T

TCP - see Transmission Control Protocol

TERMDSM - a utility used to diagnose problems with the ATP. The ATP is a card installed in the HP 3000 for Asynchronous SERIAL Network links.

topology - the physical arrangement of nodes in a network. Some common topologies are bus, star, and ring.

Transmission Control Protocol (TCP) - a network protocol that establishes and maintains connections between nodes. TCP regulates the flow of data, breaks messages into smaller fragments if necessary (and reassembles the fragments at the destination), detects errors, and retransmits messages if errors have been detected.

U

utility, NMMGR - NMMGR utilities, which are accessed from the UTILITY menu screen, consist of Output Configuration File, Compress, Validate, and Configuration Subtree Copy utilities.

V

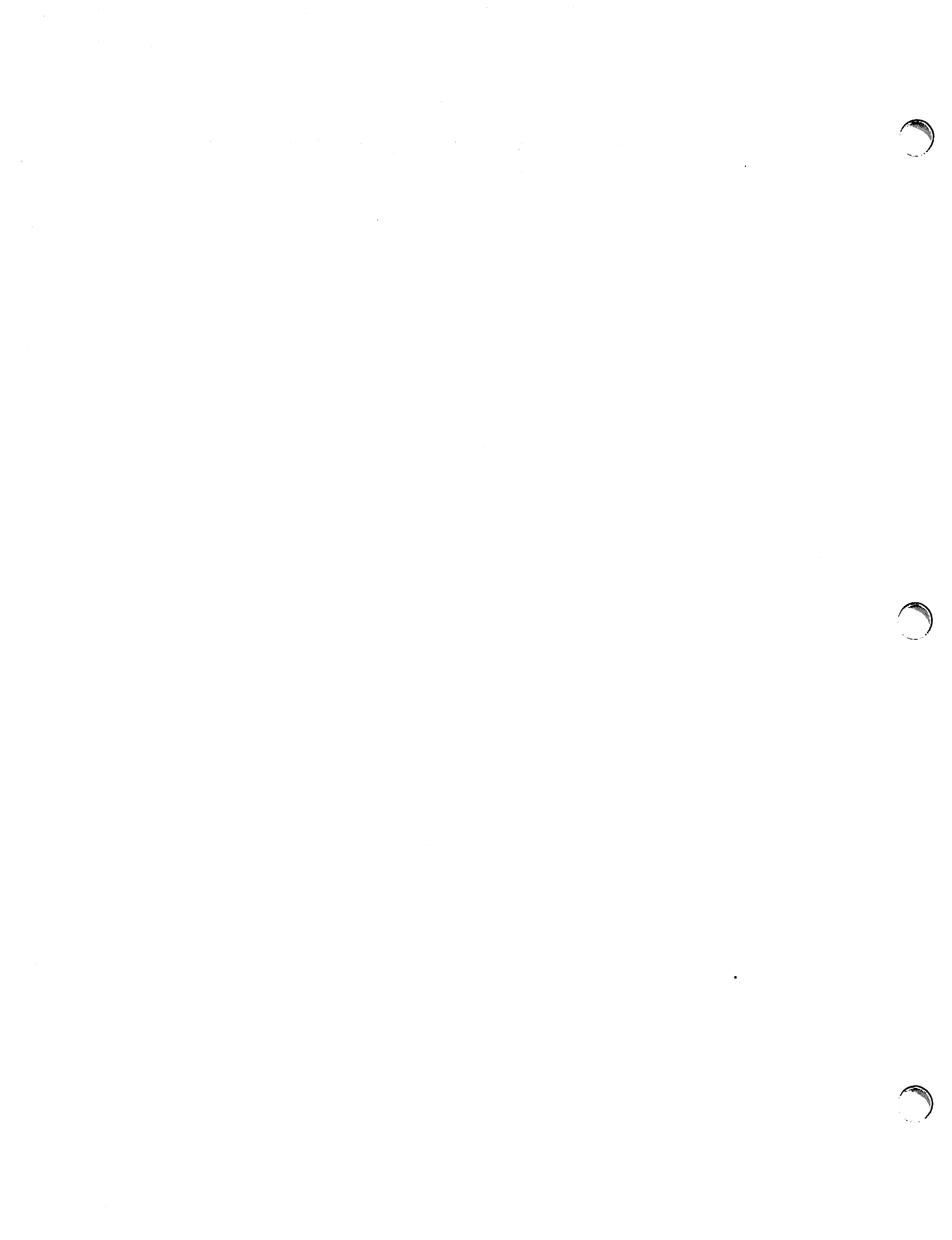
validation - the process of ascertaining whether the transport configuration file has been correctly configured. This is accomplished by using the NMMGR Validate Configuration File screen.

virtual terminal - software that simulates the function of a terminal to MPE. Devices that provide incoming data to a system require the configuration of virtual terminals.

VPLUS - software used to generate screens such as those displayed by NMMGR.

X

XPT line test - a software program that tests whether the Network Transport is operating correctly.



A

address, IP, format of, 3-8
administration, network, overview of, 3-24
alternate gateways, 3-19
alternate links, 3-16
alternate routes, intranet, 3-5
alternate routes, router network, 3-5
assignment, of node names, 3-6
autodial, 3-14
automatic rerouting, 3-16
Add (key), 5-22
Adding a device, 4-21, 4-22
Adding a virtual terminal, 4-21, 4-22
Adding devices
 and maximum number of devices, 4-19, 4-25, 4-27
Addresses
 IEEE 802.3, 3-10
 network, 3-9
 node, 3-10
Architecture
 network, 1-3
 OSI model, 1-4
ARPA, 1-8, 1-11
Asynchronous Serial Network Protocol, 1-12
ASNP link trace data, fields, 7-29
ASNP Link data, 7-27
ASNP, 1-12
ATP, protocols, 1-12
ATP, configuration dialogue, 4-27
AUI, LAN 3000/V Link (ThickLAN), 1-18

B

buffers, 3-13
Binary Synchronous Communication protocol, 1-12
Bisync, 1-12
Brother branching, 5-15
BSC link trace data, fields, 7-15
BSC Link data, 7-11
BSC, 1-12
Buffer size, 4-11

C

central administrative node, 14-4
classes
 internet address, 3-8

- IP address, 3-8
- command window, 5-14
- command, COPYCONF, 5-46
- commands, HELP, 5-7
- configuration files, 3-2
- configuration file, use for address resolution, 3-12
- configuration terminology, 3-13
- configuration updates/gateway half, 6-13, 6-15
- configuration updates/router mapping, 6-13
- configuration updates/router, 6-16
- configuration
 - data, copying, 5-40, 5-46
 - dial ID protocol, 11-10
 - direct connect link, 11-17
 - files, 5-9, 5-27
 - gateway half dial link, 11-19
 - gateway half, 11-3
 - general protocol, 8-10
 - global transport, 8-7
 - internet protocol, 11-7
 - internte protocol, 8-11
 - neighbor gateway reachable networks, 11-24
 - neighbor gateways, 11-22
 - network interface links, 11-15
 - network interface, 8-21
 - packet exchange protocol, 8-14
 - protocol, 11-6
 - PXP, 8-14
 - security strings, 11-13
 - transmission control protocol, 8-17
 - with NMMGR, overview of, 3-26
- configuration, overview of, 3-26
- copying configuration data, 5-40, 5-46
 - dsline connections, 5-43, 5-47
 - type select parameters, 5-46
- current file size (field), 5-33
- Checksum Enabled (screen), 8-15
- Checksum Enabled (field), 8-18
- Commands, NMMGR, 5-16
- Commands, MPE, 2-5
- Communications drivers, 4-25
- Communications Systems, utilities, 2-6
- Compress (screen), 5-33
- Condense Page (key), 5-22
- Configuration Menu screen, 5-12
- Configuration Subtree Copy (screen), 5-40
- Configuration, 3-72
 - examples, 4-34
 - I/O, 4-3
 - logging, 13-1
- Configuration, NS3000/V, 2-10
- Configured Reachable Networks Hops (field), 11-26
- Configured Reachable Networks IP Network Number (field), 11-25
- Connection Assurance Interval (field), 8-20

Correcting Guided Configuration Errors, 6-4
 COLDSTART, 4-33
 COPYCONF, 5-46

D

data flag, 5-23
 data
 dial ID protocol, 11-10
 internet protocol, 11-7
 network interface link, 11-17
 NI link, 11-17
 transmission control protocol, 8-17
 TCP, 8-17
 definitions, of configuration terms, 3-13
 design considerations
 geographical location, 3-29
 line speed, 3-29
 design, network and catenet, 3-29
 destination file (field), 5-41
 destination path (field), 5-41
 dial ID protocol configuration, 11-10
 dial links, 1-13
 dial links, and network design, 3-30
 dial links, terminology for, 3-13
 dial
 autodial, 3-14
 direct, 3-13
 manual, 3-14
 shared, 3-13
 direct connect link configuration, 11-17
 direct connect, 3-14
 direct dial, 3-13
 direct path branching, 5-14
 directly connected, definition of, 3-15
 domain, in node name, 3-6
 downed links, 3-16
 dpath:dfilename (parameter), 5-46
 Data
 internet protocol, 9-7, 10-8, 12-5
 NI link, 9-15, 10-19
 packet exchange protocol, 8-14
 Probe protocol, 9-10
 DARPA, 1-8, 1-11
 Default speed, overriding, 4-23
 Defense Advanced Research Projects Agency, 1-8, 1-11
 Delete (key), 5-22
 Device classes, 4-8
 Device
 adding, 4-21, 4-22
 removing, 4-21, 4-22
 Devices, switched, 4-23
 DELETENODE command, 14-15

Dial ID protocol, 1-13, 3-14
Dial Protocol Configuration (screen), 11-10
Direct Connect Link Configuration (screen), 11-17
DPAN5, 2-4
Drivers
 communications, 4-13, 4-25
Drivers, I/O configuration, 4-8
DRT entry number, 4-5
DRT number, 4-3
DS-compatible links, 1-24
 modem, 1-24
 point-to-point, 1-24
 satellite link, 1-24
 X.25, 1-24
DS-Compatible links, and network design, 3-30
Dump date, 4-32

E

entry priority, 3-16
entry priority, definition of, 3-15
Enable console logging, 13-8
Enable disc logging, 13-8
ENTER (key), 5-14
Error Information (screen), 5-43
Examples, configuration, 4-34
EXIT command, 14-19
EXPANDDIR command, 14-17

F

failures, link, 3-16
format, node name, 3-6
Fields
 ASNP link trace data, 7-29
 BSC link trace data, 7-15
 IEEE 802.3 link trace data, 7-9
 link name, 7-4
 new name, 7-4
 NI links, 9-14, 9-18, 9-23, 10-17, 10-24, 10-31, 11-23
File (field), 5-14
First Page (key), 5-22
Formats, IP addresses, 3-8
Fragment Assembly Queue Elements (field), 11-9
Full Duplex, 4-23

G

gateway half configuration, 11-3
gateway half dial link configuration, 11-19
gateway half partner, 3-15

gateway half partners, 3-32
 gateway halves, and network design, 3-31
 gateway name, 3-7
 gateway, neighbor, definition of, 3-15
 gateways
 and network design, 3-31
 maximum number per network, 3-31
 gateways, alternate, 3-19
 gateways, redirect, 3-21
 gateways, terminology for, 3-15
 guided configuration, overview of, 3-26
 Gateway Half Dial Link Configuration Screen (screen), 11-19
 Gateway-Half Network Interface Configuration (screen), 11-4
 General Protocol Configuration (screen), 8-10
 Global transport configuration, 8-7
 Guided Configuration Tree, 6-3
 Guided Configuration, 6-1
 gateway half, 6-11
 loopback, 6-6
 LAN802.3, 6-7
 Netxport Configuration, 6-5
 Netxport Update, 6-13
 PC router, 6-12
 router, 6-9

H

home network name, 3-7
 hop count
 internet, 3-14
 intranet, 3-14
 Hardware components, LAN 3000/V Link (ThickLAN), 1-18
 Hardware components, ThinLAN, 1-19
 HELP, 5-7
 Home Network Name (field), 8-7
 HP ThinLAN, medium access method, 1-18

I

inbound buffers, definition of, 3-13
 installation, network, overview of, 3-23
 installation, software and hardware, overview of, 3-24
 internet addresses, classes, 3-8
 internet address, format of, 3-8
 internet protocol configuration, 11-7
 internet Protocol (IP) Update Configuration (screen), 8-12
 internet rerouting, 3-19
 internetwork, 1-11
 I/O configuration, 4-3
 device classes, 4-8
 drivers, 4-8
 DRT entry number, 4-5

- logical device number, 4-5
- types and subtypes, 4-6
- ICMP redirect message, 3-21
- ICMP, 3-21
- Idle Device Timeout Value (field), 11-5
- IEEE 802.3 addresses, 3-10
- IEEE 802.3 link trace data, fields, 7-9
- IEEE 802.3 local area network, protocols, 1-12
- IEEE 802.3 Link data, 7-6
- IEEE 802.3
 - link data fields, 7-6
 - link data screen, 7-6
- Initial Retransmission Interval (field), 8-19
- Initialization, NS3000/V, 2-10
- Installation, NS3000, 2-7
- Intelligent Network Processor, 4-22, 4-23
 - adding, 4-21, 4-22
- Internal Message Queue Length (field), 11-9
- Internet protocol data, 9-7, 10-8, 12-5
- Internet protocol update, data, 8-11
- Internet Protocol, 1-8, 1-11
- INP driver, 4-10
- INP, 4-22, 4-23
 - adding, 4-21, 4-22
 - configuration dialogue, 4-22
 - protocols, 1-12
- IP addresses
 - assigning, 3-9
 - classes, 3-8
- IP address, format of, 3-8
- IP Internet Address (field), 11-8
- IP Protocol Configuration (screen), 11-7
- IP, 1-8, 1-111

K

- keep (parameter), 5-46

L

- link failures, 3-16
- link name, 3-7
- link selection, network interface, 11-15
- link software, 1-14
- links, alternate, 3-16
- local node, 3-13
- local, in router link configuration, 3-15
- logging configuration
 - classes, 13-5
 - subsystems, 13-3
- Last Page (key), 5-22
- Layers, 1-3, 1-4

Protocols, 1-3
 LAN 3000/V Link (ThickLAN), 1-15
 AUI, 1-18
 hardware components, 1-18
 LANIC, 1-18
 medium access method, 1-18
 MAU, 1-18
 LAN 3000/V (ThickLAN), software components, 1-19
 LAN802.3 data, NI, 9-3
 LANIC, configuration dialogue, 4-21
 LANIC, LAN 3000/V Link (ThickLAN), 1-18
 LANIC, ThinLAN, 1-19
 LAP-B Link data, 7-19
 LAP-B, 1-12
 Leaving system I/O configuration, 4-21, 4-22
 Leaving SYSDUMP, 4-21, 4-22
 Link configuration screen, 7-3
 Link data
 ASNP, 7-27
 BSC, 7-11
 IEEE 802.3, 7-6
 LAP-B, 7-19
 Link name, 7-4
 Link Name (field), 11-16
 Link selection
 network interface, 9-13, 10-16
 Link Support Services subsystem, 3-2
 LISTDIR command, 14-17, 14-22
 LISTLOG 5, 2-5
 Local Node Name (field), 8-6
 Logging classes, screen, 13-7
 Logging config, .class data screen, 13-8
 Logging configuration
 classes, 13-7
 guidelines, 13-1
 overview, 13-1
 screen, 13-5
 Logical device number, 4-5

M

maintenance mode interface, 14-14
 manual configuration, overview of, 3-26
 manual dial, 3-14
 map, of network or catenet, 3-24
 multicast, for Probe requests, 3-11
 Main Menu screen, 5-6
 Maximum Connection Assurance Retransmissions (field), 8-20
 Maximum Directly Connected Nodes (field), 8-8
 Maximum Gateway Nodes Per Network (field), 8-13
 Maximum Inbound Destinations (field), 8-9
 Maximum number of devices, 4-19, 4-25, 4-27
 Maximum Number of Connections (field), 8-18

Maximum Number of Networks in Catenet (field), 8-12
Maximum Outbound Destinations (field), 8-9
Maximum Retransmissions Per Packet (field), 8-20
Maximum Retransmissions Per Request (field), 8-16
MAKESTREAM command, 14-19
MAU, LAN 3000/V Link (ThickLAN), 1-18
Medium access method, HP ThinLAN, 1-18
Medium access method, LAN 3000/V Link (ThickLAN), 1-18
Menu screens, 5-19
Menu
 general protocol, 8-10
 NI protocol, 9-6, 10-7, 11-6, 12-1
MERGEDIR command, 14-16
Modems, with internal clocking signals, 4-23
MPE commands, 2-4, 2-5
MPE-V, version required, 1-2

N

name
 home network, 3-7
 link, 3-7
 network interface, 3-7
 NI, 3-7
name-to-address resolution, 3-10
names and addresses, 3-5
names, other, 3-7
names, definitions of, 3-5
neighbor gateway reachable networks configuration, 11-24
neighbor gateways configuration, 11-22
neighbor gateway, definition of, 3-15
network administration, overview of, 3-24
network and catenet design, 3-29
network boundary, and design, 3-32
network boundary, definition of, 3-32
network configuration worksheets, 3-33
network design
 and gateways, 3-31
 and network interfaces, 3-31
 dial links, 3-30
 DS-Compatible links, 3-30
 gateway halves, 3-31
 non- HP 3000 nodes, 3-30
 personal computers, 3-30
network directories, synchronization of, 3-27
network directory
 central administrative node, 14-4
 data screen, 14-11
 DELETENODE command, 14-15
 EXIT command, 14-19
 EXPANDDIR command, 14-17
 file structure, 14-1
 for name-to-address resolution, 3-11

- functions of, 14-1
- global entries, 14-3
- HELP command, 14-18
- interfaces, 14-4
- local entries, 14-3
- LISTDIR command, 14-17, 14-22
- maintenance mode interface, 14-14
- Main screen, 14-7
- MAKESTREAM command, 14-19
- MERGEDIR command, 14-16
- OPENDIR command, 14-15
- path report lists, 14-2
- path reports, 14-2
- roles, 14-4
- Select Node Name Screen, 14-9
- network installation, overview of, 3-23
- network interface link configuration, 11-15
- network interface name, 3-7
- network interface
 - configuration, 8-21
 - link data, 11-17
 - link selection, 11-15
 - protocol menu, 11-6
- network interfaces, and network design, 3-31
- network interface, definition of, 3-13
- network links, 1-14
- network manager
 - link level tools, 2-6
 - link level utilities, 2-6
 - network life cycle, 2-3
 - tools, 2-3
- network map, 3-24
- network maps, overview of, 3-33
- network planning and configuration, 3-1
- network startup, overview of, 3-28
- non-HP 3000 nodes, and network design, 3-30
- number of additional records (field), 5-33
- number of free records (field), 5-33
- NCONF files, 5-9
- Neighbor Gateway Reachable Networks (screen), 11-24
- Neighbor Gateways (screen), 11-23
- Network addresses, 3-9
- Network architecture, 1-3
- Network Administration Office, address of, 3-9
- Network Administration Office, of Hewlett Packard, 3-9
- Network Architecture
 - Layers, 1-3
 - OSI model, 1-4
- Network File Transfer, 1-26
- Network interface
 - link data, 9-15, 10-19
 - link selection, 9-13, 10-16
 - links fields, 9-14, 9-18, 9-23, 10-17, 10-24, 10-31, 11-23
 - links screen, 9-14, 9-18, 9-23, 10-17, 10-24, 10-31, 11-23

- LAN802.3 data, 9-3
 - protocol config. screen, 9-6, 10-7, 12-4
- Network Implementation and Support Plan, 3-33
- Network Interface Links (screen), 11-16
- Network Interface Name (field), 8-22
- Network Interface
 - protocol menu, 9-6, 10-7, 12-1
- Network life cycle, 2-3
- Network Layer, 1-11
- Network management, responsibilities of, 2-3
- Network Management, 2-1
- Network Services subsystem, 3-2
- Network Services, 1-1
- Network Transport Configuration Selection (screen), 8-3
- Network Transport subsystem, 3-2
- Network, 1-3
- Netxport Configuration, 6-2
- Netxport Update, 6-2, 6-13
- New Name (field), 11-16
- Next Page (key), 5-22
- NEXT, 5-15
- NFT, 1-26
- NMCONFIG.PUB.SYS configuration file, 3-3
- NMMGR commands, 5-16
- NMMGR Path Commands, 5-14
- NMMGR screens
 - Compress, 5-33
 - Configuration Subtree Copy, 5-40
 - data entry, 5-23
 - Output Configuration File, 5-27
 - simple-select screens, 5-20
 - typed-select, 5-21
 - Utility, 5-26
- NMMGR, 5-1
 - Add (key), 5-22
 - command window, 5-14
 - configuration files, 5-9
 - configuration screens, 5-12
 - Condense Page (key), 5-22
 - data entry screens, 5-23
 - data flag, 5-23
 - Delete (key), 5-22
 - ENTER (key), 5-14
 - file (field), 5-14
 - First Page (key), 5-22
 - Last Page (key), 5-22
 - Next Page (key), 5-22
 - Prev Page (key), 5-22
 - run string, 5-2
 - Refresh Screen (key), 5-19
 - Rename (key), 5-22
 - screen structure, 5-8
 - screens, 5-12
 - simple-select screens, 5-20

- typed-select, 5-21
- utilities, 5-26
- Update Config (key), 5-24
- Update (key), 5-22
- Node addresses, 3-10
- Node Configuration (screen), 8-4
- Node management services, 2-5
- Node management services, commands, 2-5
- Node management services, utilities, 2-5
- Node Management Configurator subsystem, 3-2
- Node Name Configuration (screen), 8-5
- Non-operational links, 3-16
- NS3000/V, 1-26
 - configuration, 3-72
 - environment, 1-26
 - initialization, 2-10
 - I/O configuration, 4-3
 - services, 1-26
 - session, 1-26
 - system configuration, 4-2
 - system requirements, 1-2
- NS3000
 - configuration, 2-10
 - installation, 2-7
- NSCONF.PUB.SYS configuration file, 3-3
- NSDIR.PUB.SYS file, 3-3
- NSDPAN/ETOD, 2-4
- Number of Inbound Buffers (field), 11-4
- Number of Outbound Buffers (field), 11-4

O

- organization, in node name, 3-6
- outbound buffers, definition of, 3-13
- overwrite existing subtree (field), 5-41
- Open Configuration/Directory File screen, 5-3
- OPENDIR command, 14-15
- OSI model, layers, 1-4
- OSI Model, 1-4
- Output Configuration File (screen), 5-27
- Overriding default speed, 4-23

P

- packet exchange protocol
 - configuration, 8-14
 - data, 8-14
- partner, of a gateway half, 3-15
- path report lists, 14-2
- path reports, 14-2
- path report, definition of, 3-11
- personal computers, and network design, 3-30

- personal computers, as nodes, 1-25
- physical layer protocols, 1-12
- planning, of network, catenet, 3-24
- priority, of router network route entries, 3-15
- protocol configuration, 11-6
- protocol, Dial ID, 3-14
- protocols, bisync, 1-24
- protocol, Probe, 3-11
- proxy server, for Probe protocol, 3-11
- Packet Exchange Protocol (PXP) Configuration (screen), 8-15
- Packet Exchange Protocol, 1-11
- Path commands, NMMGR, 5-14
- Phone number, 4-12
- Phonelist, 4-12
- Prev Page (key), 5-22
- Probe protocol, 1-13, 3-11
 - data, 9-10
- Probe proxy server, 3-11
- Program-to-Program Communications, 1-26
- Protocol Configuration (screen), 11-6
- Protocols, 1-3
- PTOP, 1-26
- PXP configuration screen, 8-15
- PXP configuration, 8-14
- PXP, 1-11

R

- reachable networks, definition of, 3-15
- redirect gateways, 3-21
- redirect message, 3-21
- redirection, of internet packets, 3-19
- remote node, 3-13
- remote, in router link configuration, 3-15
- requirements
 - software, 1-2
 - system, 1-2
- rerouting, 3-16
- rerouting, for IEEE 802.3 gateways, 3-21
- rerouting, for router networks, 3-16
- rerouting, internet, 3-19
- resolution, of names and addresses, 3-10
- router links, terminology, 3-14
- router node name, 3-7
- routes, alternate, 3-5
- routing
 - broadcast, 3-5
 - intranet, 3-4
- routing, of messages, 3-4
- RDBA, 1-26
- Refresh Screen (key), 5-19
- Remote Data Base Access, 1-26
- Removing a device, 4-21, 4-22

Rename (key), 5-22
 Retransmission Interval Lower Bound (field), 8-19
 Retransmission Interval Upper Bound (field), 8-19
 Retransmission Interval (field), 8-15

S

screens

configuration menu, 5-12
 Error Information, 5-43
 global transport configuration, 8-7
 General Protocol Configuration, 8-10
 Internet Protocol (IP) Update Configuration, 8-12
 main menu, 5-6
 network interface links, 11-16
 Network Transport Configuration Selection, 8-3
 NI links, 11-16
 Node Configuration, 8-4
 Node Name Configuration, 8-5
 Open Configuration/Directory file, 5-3
 Packet Exchange Protocol (PXP) Configuration, 8-15
 Protocol Configuration, 11-6
 PXP configuration, 8-15
 TCP configuration, 8-18
 Transmission Control Protocol Configuration, 8-18
 validate configuration file, 5-35
 security strings configuration, 11-13
 security string, definition of, 3-14
 shared dial, 3-13
 and network design, 3-30
 software requirements, 1-2
 software, link, 1-14
 software, of NS3000/V, 3-2
 software, required, 3-25
 source file (field), 5-40
 source path (field), 5-41
 spath:filename (parameter), 5-46
 starting the network, overview of, 3-28
 static neighbor node name, 3-7
 store-and-forward buffers, definition of, 3-13
 subsystems, software, 3-2
 synchronization, of network directories, 3-27
 syntax, node name, 3-6
Screens
 IEEE 802.3, 7-6
 link configuration, 7-3
 logging configuration, 13-5
 logging config.class data, 13-8
 logging config.logging classes, 13-7
 NI links, 9-14, 9-18, 9-23, 10-17, 10-24, 10-31, 11-23
 NI protocol config., 9-6, 10-7, 12-4
 Security String Configuration Screen (screen), 11-13
Services

- Network File Transfer, 1-27
- PTOP Communication, 1-27
- Remote Data Base Access, 1-27
- Remote File Access, 1-27
- Remote Process Management, 1-26
- Virtual Terminal, 1-26
- Services, node management, 2-5
- Software components, HP ThinLAN, 1-19
- Software components, LAN 3000/V Link (ThickLAN), 1-19
- Software Dump facility, 2-4
- Speed, overriding default, 4-23
- StarLAN/3000 Link, 1-15
- StarLAN/3000, protocols, 1-12
- StarLAN, 1-15
- Store & Forward Buffers (field), 11-8
- Subtype, 4-22
- Switched devices, 4-23
- System configuration, 4-2
- System I/O configuration
 - leaving, 4-21, 4-22
- SYSDUMP, 2-4, 4-1, 4-2
 - leaving, 4-21, 4-22
- SYSDUMP, configuration with, overview of, 3-26
- SYSDUMP, dialogue, 4-30

T

- terminology, for configuration, 3-13
- transmission control protocol configuration, 8-17
- transmission control protocol data, 8-17
- type select in configuration copy, 5-46
- TCP configuration screen, 8-18
- TCP, 1-11
 - data, 8-17
- ThickLAN, 1-15
- ThinLAN link, software components, 1-19
- ThinLAN/3000 Link, 1-15
- ThinLAN/3000
 - hardware components, 1-19
 - protocols, 1-12
- ThinLAN, 1-15
 - LANIC, 1-19
 - ThinMAU, 1-19
- ThinMAU, ThinLAN, 1-19
- Transmission Control Protocol Configuration (screen), 8-18
- Transmission Control Protocol, 1-11
- Transmission mode, 4-10
- Transmission speed, 4-11
- Transport Layer protocols, 1-11
- Type 16, 4-19
- Type (LOOP, LAN802.3, ROUTER, or GATEHALF) (field), 8-22
- Type, 4-21, 4-22

Types and subtypes, 4-6
Types (field), 11-16

U

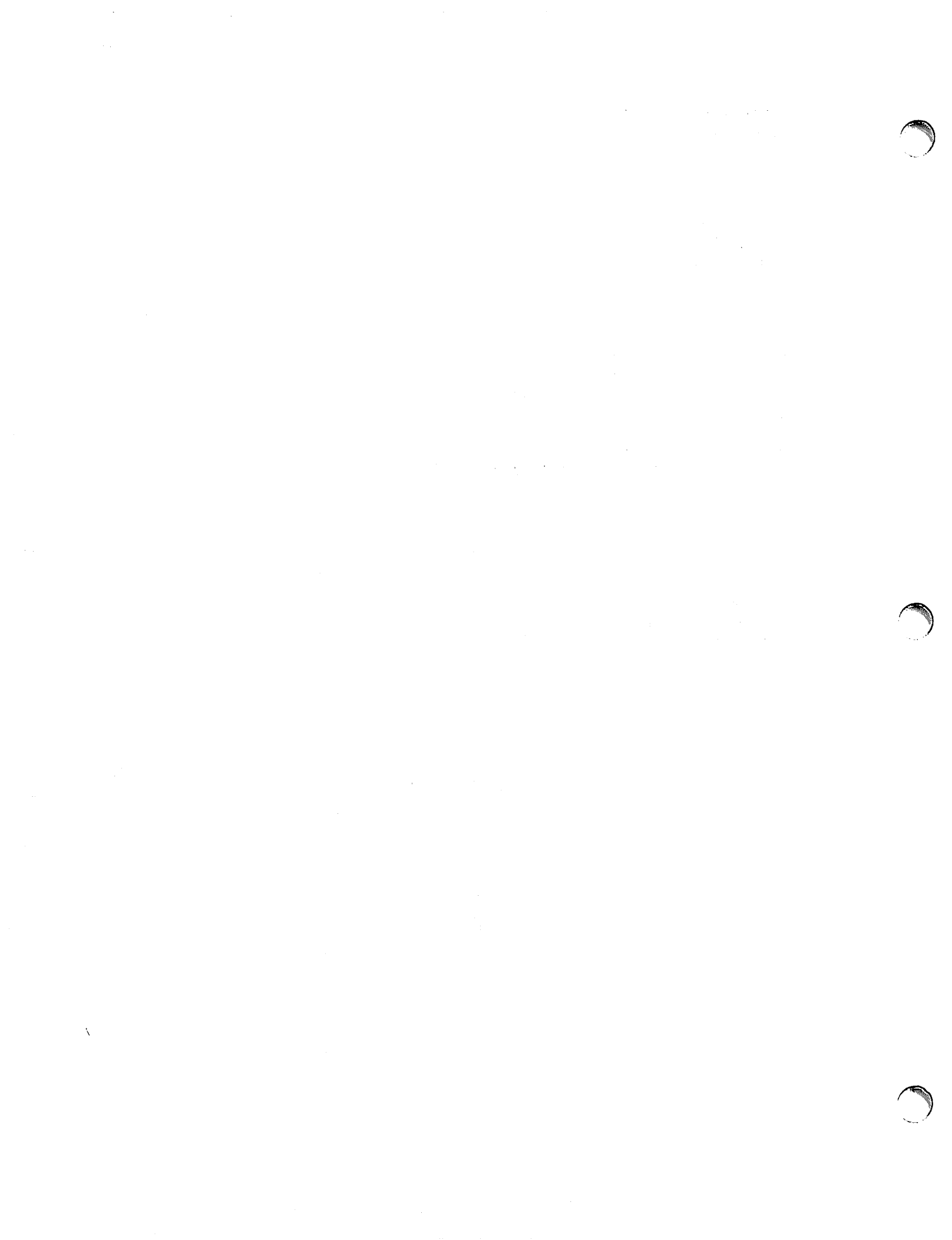
Update (key), 5-22
Users enabled for logging, 13-8
Utility (screen), 5-26

V

validation, of a node, 3-27
verification, of a node, 3-27
Validate Configuration File screen, 5-35
Virtual terminal
 adding, 4-21, 4-22
Virtual terminals, 4-9
Virtual terminal, configuration dialogue, 4-19
Virtual Terminal, 1-26

W

worksheets
 instructions, 3-38
 terminology, 3-36
worksheets, network configuration, overview, 3-33



SALES & SUPPORT OFFICES

Arranged alphabetically by country

1

Product Line Sales/Support Key

Key Product Line

- A** Analytical
- CM** Components
- C** Computer Systems
- E** Electronic Instruments & Measurement Systems
- M** Medical Products
- P** Personal Computation Products
- * Sales only for specific product line
- ** Support only for specific product line

IMPORTANT: These symbols designate general product line capability. They do not insure sales or support availability for all products within a line, at all locations. Contact your local sales office for information regarding locations where HP support is available for specific products.

HEADQUARTERS OFFICES

If there is no sales office listed for your area, contact one of these headquarters offices.

ASIA

Hewlett-Packard Asia Ltd.
47/F, 26 Harbour Rd.,
Wanchai, **HONG KONG**
G.P.O. Box 863, Hong Kong
Tel: 5-8330833
Telex: 76793 HPA HX
Cable: HPASIAL TD

CANADA

Hewlett-Packard (Canada) Ltd.
6877 Goreway Drive
MISSISSAUGA, Ontario L4V 1M8
Tel: (416) 678-9430
Telex: 069-8644

EASTERN EUROPE

Hewlett-Packard Ges.m.b.h.
Liebigasse 1
P.O. Box 72
A-1222 VIENNA, Austria
Tel: (222) 2500-0
Telex: 13 4425 HEPA A

NORTHERN EUROPE

Hewlett-Packard S.A.
V. D. Hooplaan 241
P.O. Box 999
NL-118 LN 15 AMSTELVEEN
The Netherlands
Tel: 20 5479999
Telex: 18919 hpner

SOUTH EAST EUROPE

Hewlett-Packard S.A.
World Trade Center
110 Avenue Louis-Casai
1215 Cointrin, GENEVA, Switzerland
Tel: (022) 98 96 51
Telex: 27225 hpser

Mail Address:

P.O. Box
CH-1217 Meyrin 1

GENEVA

Switzerland

MIDDLE EAST

AND CENTRAL AFRICA

Hewlett-Packard S.A.
Middle East/Central
Africa Sales H.Q.
7, rue du Bois-du-Lan
P.O. Box 364
CH-1217 Meyrin 1

GENEVA

Switzerland

Tel: (022) 83 12 12

Telex: 27835 hmea ch

Telefax: (022) 83 15 35

UNITED KINGDOM

Hewlett-Packard Ltd.
Nine Mile Ride
WOKINGHAM
Berkshire, RG113LL
Tel: 0344 773100
Telex: 848805/848814/848912

UNITED STATES OF AMERICA

Customer Information Center
(800) 752-0900
6:00 AM to 5 PM Pacific Time

EASTERN USA

Hewlett-Packard Co.
4 Choke Cherry Road
ROCKVILLE, MD 20850
Tel: (301) 948-6370

MIDWESTERN USA

Hewlett-Packard Co.
5201 Tollview Drive
ROLLING MEADOWS, IL 60008
Tel: (312) 255-9800

SOUTHERN USA

Hewlett-Packard Co.
2000 South Park Place
ATLANTA, GA 30339
Tel: (404) 955-1500

WESTERN USA

Hewlett-Packard Co.
5161 Lankershim Blvd.
NORTH HOLLYWOOD, CA 91601
Tel: (818) 505-5600

OTHER INTERNATIONAL AREAS

Hewlett-Packard Co.
Intercontinental Headquarters
3495 Deer Creek Road
PALO ALTO, CA 94304
Tel: (415) 857-1501
Telex: 034-8300
Cable: HEWPACK

ALGERIA

Hewlett-Packard Trading S.A.
Bureau de Liaison Alger
Villa des Lions
9, Hai Galtout
DZ-BORDJ EL BAHRI
Tel: 76 03 36
Telex: 63343 dlion dz

ANGOLA

Telectra Angola LDA
Empresa Técnica de Equipamentos
16 rue Cons. Julio de Vilhema
LUANDA
Tel: 35515.35516
Telex: 3134
E,P

ARGENTINA

Hewlett-Packard Argentina S.A.
Montaneses 2140/50
1428 BUENOS AIRES
Tel: 541-11-1441
Telex: 22796 HEW PAC-AR
A,C,E,P
Biotron S.A.C.I.M.e.I.
Av. Paso Colon 221, Piso 9
1399 BUENOS AIRES
Tel: 541-333-490,
541-322-587
Telex: 17595 BIONAR
M

Laboratorio Rodriguez
Corswant S.R.L.

Misiones, 1156 - 1876
Bernal, Oeste

BUENOS AIRES

Tel: 252-3958, 252-4991

A

Intermaco S.R.L.

Florida 537/71

Galeria Jardin - Local 28

1005 BUENOS AIRES

Tel: 393-4471/1928

Telex: 22796 HEW PAC-AR

P (Calculators)

Argentina Esanco S.R.L.

A/ASCO 2328

1416 BUENOS AIRES

Tel: 541-58-1981, 541-59-2767

Telex: 22796 HEW PAC-AR

A

All Computers S.A.

Montaneses 2140/50 5 Piso

1428 BUENOS AIRES

Tel: 781-4030/4039/783-4886

Telex: 18148 Ocme

P

AUSTRALIA

Adelaide, South

Australia Office
Hewlett-Packard Australia Ltd.
153 Greenhill Road
PARKSIDE, S.A. 5063
Tel: 61-8-272-5911
Telex: 82536
Cable: HEWPARD Adelaide
A*,C,CM,E,P

Brisbane, Queensland

Office
Hewlett-Packard Australia Ltd.
10 Payne Road
THE GAP, Queensland 4061
Tel: 61-7-300-4133
Telex: 42133
Cable: HEWPARD Brisbane
A,C,CM,E,M,P

Canberra, Australia

Capital Territory Office
Hewlett-Packard Australia Ltd.
Thynne Street, Fern Hill Park
BRUCE, A.C.T. 2617
P.O. Box 257,
JAMISON, A.C.T. 2614
Tel: 61-62-80-4244
Telex: 62650
Cable: HEWPARD Canberra
C,CM,E,P

Melbourne, Victoria

Office
Hewlett-Packard Australia Ltd.
31-41 Joseph Street
P.O. Box 221
BLACKBURN, Victoria 3130
Tel: 61-3-895-2895
Telex: 31-024
Cable: HEWPARD Melbourne
A,C,CM,E,M,P

Perth, Western Australia

Office
Hewlett-Packard Australia Ltd.
Herdsmen Business Park
CLAREMONT, W.A. 6010
Tel: 61-9-383-2188
Telex: 93859
Cable: HEWPARD Perth
C,CM,E,P

Sydney, New South

Wales Office
Hewlett-Packard Australia Ltd.
17-23 Talavera Road
P.O. Box 308
NORTH RYDE, N.S.W. 2113
Tel: 61-2-888-4444
Telex: 21561
Cable: HEWPARD Sydney
A,C,CM,E,M,P

AUSTRIA

Hewlett-Packard Ges.m.b.h.
Verkaufsbuero Graz
Grottenhofstrasse 94
A-8052 GRAZ
Tel: 43-316-291-5660
Telex: 312375
C,E

Hewlett-Packard Ges.m.b.h.

Liebigasse 1

P.O. Box 72

A-1222 VIENNA

Tel: 43-222-2500

Telex: 134425 HEPA A

A,C,CM,E,M,P

BAHRAIN

Green Salon
P.O. Box 557
MANAMA
Tel: 255503-250950
Telex: 84419
P

Wael Pharmacy

P.O. Box 648

MANAMA

Tel: 256123

Telex: 8550 WAEL BN

E,M

Zayani Computer Systems

218 Shaik Mubarak Building

Government Avenue

P.O. Box 5918

MANAMA

Tel: 276278

Telex: 9015 plans bn

P

BELGIUM

Hewlett-Packard Belgium S.A./N.V.
Blvd de la Woluwe, 100
Woluwedal
B-1200 BRUSSELS
Tel: (02) 32-2-761-31-11
Telex: 23494 hewpac
A,C,CM,E,M,P

BERMUDA

Applied Computer Technologies
Atlantic House Building
P.O. Box HM 2091
Par-La-Ville Road
HAMILTON 5
Tel: 295-1616
Telex: 380 3589/ACT BA
P

BOLIVIA

Arrellano Ltda
Av. 20 de Octubre #2125
Casilla 1383
LA PAZ
Tel: 368541
M

BRAZIL

Hewlett-Packard do Brasil S.A.
Alameda Rio Negro, 750-I. AND.
ALPHAVILLE
06400 Barueri SP
Tel: (011) 421.1311
Telex: (011) 71351 HPBR BR
Cable: HEWPACK Sao Paulo
CM,E

Hewlett-Packard do Brasil S.A.

Praia de Botafago 228-A-614

6. AND.-CONJ. 601

Edificio Argentina - Ala A

22250 RIO DE JANEIRO, RJ

Tel: (021) 552-6422

Telex: 21905 HPBR BR

Cable: HEWPACK Rio de Janeiro

E

Van Den Cientifica Ltda.

Rua Jose Bonifacio, 458

Todos os Santos

20771 RIO DE JANEIRO, RJ

Tel: (021) 593-8223

Telex: 33487 EGLB BR

A

ANAMED I.C.E.I. Ltda.

Rua Vergueiro, 360

04012 SAO PAULO, SP

Tel: (011) 572-1106

Telex: 24720 HPBR BR

M

Datatronix Electronica Ltda.

Av. Pacaembu 746-C11

SAO PAULO, SP

Tel: (118) 280111

CM

BRUNEI

Komputer Wisman Sdn Bhd
G6, Chandrawaseh Cmplx,
Jalan Tutong
P.O. Box 1297,
BANDAR SERI BEGAWAN
NEGARA BRUNI DARUSSALAM
Tel: 673-2-2000-70/26711
C,E,P

CAMEROON
Beriac
B. P. 23
DOUALA
Tel: 420153
Telex: 5351
C,P

CANADA**Alberta**

Hewlett-Packard (Canada) Ltd.
3030 3rd Avenue N.E.
CALGARY, Alberta T2A 6T7
Tel: (403) 235-3100
A,C,CM,E*,M,P*
Hewlett-Packard (Canada) Ltd.
11120-178th Street
EDMONTON, Alberta T5S 1P2
Tel: (403) 486-6666
A,C,CM,E,M,P

British Columbia

Hewlett-Packard (Canada) Ltd.
10691 Shellbridge Way
RICHMOND,
British Columbia V6X 2W8
Tel: (604) 270-2277
Telex: 610-922-5059
A,C,CM,E*,M,P*
Hewlett-Packard (Canada) Ltd.
121 - 3350 Douglas Street
VICTORIA, British Columbia V8Z 3L1
Tel: (604) 381-6616
C

Manitoba

Hewlett-Packard (Canada) Ltd.
1825 Inkster Blvd.
WINNIPEG, Manitoba R2X 1R3
Tel: (204) 694-2777
A,C,CM,E,M,P*
New Brunswick
Hewlett-Packard (Canada) Ltd.
814 Main Street
MONCTON, New Brunswick E1C 1E6
Tel: (506) 855-2841
C

Nova Scotia

Hewlett-Packard (Canada) Ltd.
Suite 111
900 Windmill Road
DARTMOUTH, Nova Scotia B3B 1P7
Tel: (902) 469-7820
C,CM,E*,M,P*
Ontario
Hewlett-Packard (Canada) Ltd.
3325 N. Service Rd., Unit W03
BURLINGTON, Ontario L7N 3G2
Tel: (416) 335-8644
C,M*

Ontario

Hewlett-Packard (Canada) Ltd.
552 Newbold Street
LONDON, Ontario N6E 2S5
Tel: (519) 686-9181
A,C,CM,E*,M,P*

Hewlett-Packard (Canada) Ltd.
552 Newbold Street
LONDON, Ontario N6E 2S5
Tel: (519) 686-9181
A,C,CM,E*,M,P*

Hewlett-Packard (Canada) Ltd.
6877 Goreway Drive
MISSISSAUGA, Ontario L4V 1M8
Tel: (416) 678-9430
Telex: 069-83644
A,C,CM,E,M,P

Hewlett-Packard (Canada) Ltd.
2670 Queensview Dr.
OTTAWA, Ontario K2B 8K1
Tel: (613) 820-6483
A,C,CM,E*,M,P*
Hewlett-Packard (Canada) Ltd.
3790 Victoria Park Ave.
WILLOWDALE, Ontario M2H 3H7
Tel: (416) 499-2550
C,E

Quebec

Hewlett-Packard (Canada) Ltd.
17500 Trans Canada Highway
South Service Road
KIRKLAND, Quebec H9J 2X8
Tel: (514) 697-4232
Telex: 058-21521
A,C,CM,E,M,P*
Hewlett-Packard (Canada) Ltd.
1150 rue Claire Fontaine
QUEBEC CITY, Quebec G1R 5G4
Tel: (418) 648-0726
C

Hewlett-Packard (Canada) Ltd.
130 Robin Crescent
SASKATOON, Saskatchewan S7L 6M7
Tel: (306) 242-3702
C

CHILE

ASC Ltda.
Austria 2041
SANTIAGO
Tel: 223-5946, 223-6148
Telex: 392-340192 ASC CK
C,P

Jorge Calcagni y Cia
Av. Italia 634 Santiago
Casilla 16475
SANTIAGO 9
Tel: 9-011-562-222-0222
Telex: 392440283 JCYCL CZ
CM,E,M

Metrolab S.A.
Monjitas 454 of. 206
SANTIAGO
Tel: 395752, 398296
Telex: 340866 METLAB CK
A

Olympia (Chile) Ltda.
Av. Rodrigo de Araya 1045
Casilla 256-V
SANTIAGO 21
Tel: 225-5044
Telex: 340892 OLYMP
Cable: Olympiachile Santiagochile
C,P

CHINA, People's Republic of

China Hewlett-Packard Co., Ltd.
47/F China Resources Bldg.
26 Harbour Road
HONG KONG
Tel: 5-8330833
Telex: 76793 HPA HX
Cable: HP ASIA LTD
A*,M*

China Hewlett-Packard Co., Ltd.
P.O. Box 9610, Beijing
4th Floor, 2nd Watch Factory Main
Shuang Yu Shou, Bei San Huan Road
Hai Dian District
BEIJING
Tel: 33-1947 33-7426
Telex: 22601 CTSHP CN
Cable: 1920 Beijing
A,C,CM,E,M,P

China Hewlett-Packard Co., Ltd.
CHP Shanghai Branch
23/F Shanghai Union Building
100 Yan An Rd. East
SHANG-HAI
Tel: 265550
Telex: 33571 CHPSB CN
Cable: 3416 Shanghai
A,C,CM,E,M,P

COLOMBIA
Instrumentación
H. A. Langebaek & Kler S.A.
Carrera 4A No. 52A-26
Apartado Aereo 6287
BOGOTA 1, D.E.
Tel: 212-1466
Telex: 44400 INST CO
Cable: AARIS Bogota
CM,E,M

Nefromedicas Ltda.
Calle 123 No. 9B-31
Apartado Aereo 100-958
BOGOTA D.E., 10
Tel: 213-5267, 213-1615
Telex: 43415 HEGAS CO
A

Compumundo
Avenida 15 # 107-80
BOGOTA D.E.
Tel: 57-214-4458
Telex: 39645466 MARCO
P

Carvajal, S.A.
Calle 29 Norte No. 6A-40
Apartado Aereo 46
CALI
Tel: 9-011-57-3-621888
Telex: 39655650 CUJCL CO
C,E,P

CONGO
Seric-Congo
B. P. 2105
BRAZZAVILLE
Tel: 815034
Telex: 5262

COSTA RICA
Científica Costarricense S.A.
Avenida 2, Calle 5
San Pedro de Montes de Oca
Apartado 10159
SAN JOSE
Tel: 9-011-506-243-820
Telex: 3032367 GALGUR CR
CM,E,M

O. Fischel R. Y. Cia. S.A.
Apartados 434-10174
SAN JOSE
Tel: 23-72-44
Telex: 2379
Cable: OFIR
A

CYPRUS
Telereza Ltd.
P.O. Box 1152
Valentine House
8 Stassandrou St.
NICOSIA
Tel: 45 628, 62 698
Telex: 5845 tlrx cy
E,M,P

DENMARK
Hewlett-Packard A/S
Kongevejen 25
DK-3460 BIRKEROD
Tel: 45-02-81-6640
Telex: 37409 hpas dk
A,C,CM,E,M,P

Hewlett-Packard A/S
Røllghedsvej 32
DK-8240 RISSKOV, Aarhus
Tel: 45-06-17-6000
Telex: 37409 hpas dk
C,E

DENMARK

Hewlett-Packard A/S
Kongevejen 25
DK-3460 BIRKEROD
Tel: 45-02-81-6640
Telex: 37409 hpas dk
A,C,CM,E,M,P

Hewlett-Packard A/S
Røllghedsvej 32
DK-8240 RISSKOV, Aarhus
Tel: 45-06-17-6000
Telex: 37409 hpas dk
C,E

DOMINICAN REPUBLIC

Microprog S.A.
Juan Tomás Mejía y Cotes No. 60
Arroyo Hondo
SANTO DOMINGO
Tel: 565-6268
Telex: 4510 ARENTA DR (RCA)
P

ECUADOR

CYEDE Cia. Ltda.
Avenida Eloy Alfaro 1749
y Belgica
Casilla 6423 CCI
QUITO
Tel: 9-011-593-2-450975
Telex: 39322548 CYEDE ED
E,P

Medtronics
Valladolid 524 Madrid
P.O. 9171, QUITO
Tel: 2-238-951
Telex: 2298 ECUAME ED
A

Hospitalar S.A.
Robles 625
Casilla 3590
QUITO
Tel: 545-250, 545-122
Telex: 2485 HOSPTEL ED
Cable: HOSPITALAR-Quito
M

Ecuador Overseas Agencies C.A.
Calle 9 de Octubre #818
P.O. Box 1296, Guayaquil
QUITO
Tel: 306022
Telex: 3361 PBCGYE ED
M

EGYPT

Sakrcro Enterprises
P.O. Box 259
ALEXANDRIA
Tel: 802908, 808020, 805302
Telex: 54333
C

International Engineering Associates
6 El Gamea Street
Agoza
CAIRO
Tel: 71-21-68134-80-940
Telex: 93830 IEA UN
Cable: INTEGASSO
E

Sakrcro Enterprises
70 Mossadak Street
Dokki, Giza
CAIRO
Tel: 706 440, 701 087
Telex: 9337
C

S.S.C. Medical
40 Gezerat El Arab Street
Mohandessin
CAIRO
Tel: 803844, 805998, 810263
Telex: 20503 SSC UN
M*

EL SALVADOR

IPESA de El Salvador S.A.
29 Avenida Norte 1223
SAN SALVADOR
Tel: 9-011-503-266-858
Telex: 301 20539 IPESA SAL
A,C,CM,E,P

ETHIOPIA

Seric-Ethiopia
P.O. Box 2764
ADDIS ABABA
Tel: 185114
Telex: 21150
C,P

FINLAND

Hewlett-Packard Finland
Field Oy
Nittilytanpolku 10
00620 HELSINKI
Tel: (90) 757-1011
Telex: 122022 Field SF
CM
Hewlett-Packard Oy
Pispankalliontie 17
02200 ESPOO
Tel: (90) 887-21
Telex: 121563 HEWPA SF
A, C, E, M, P

FRANCE

Hewlett-Packard France
Z.I. Mercure B
Rue Berthelot
13763 Les Milles Cedex
AIX-EN-PROVENCE
Tel: 33-42-59-4102
Telex: 410770F
A,C,E,M
Hewlett-Packard France
64, Rue Marchand Saillant
F-61000 ALENCON
Tel: (33) 29 04 42
C**

Hewlett-Packard France
Batiment Levitan
2585, route de Grasse
Bretelle Autoroute
06600 ANTIBES
Tel: (93) 74-59-19
C

FRANCE (Cont'd)

Hewlett-Packard France
28 Rue de la République
Boite Postale 503
25026 **BESANÇON CEDEX, FRANCE**
Tel: (81) 83-16-22
Telex: 361157
C,E*

Hewlett-Packard France
ZA Kergaradec
Rue Fernand Forest
F-29239 **GOUEESNOU**
Tel: (98) 41-87-90
E

Hewlett-Packard France
Chemin des Mouilles
Boite Postale 162
69131 **ECULLY Cedex (Lyon)**
Tel: 33-78-33-8125
Telex: 310617F
A,C,E,M,P*

Hewlett-Packard France
Parc d'activités du Bois Briard
2 Avenue du Lac
F-91040 **EVRY Cedex**
Tel: 33 11/6077 9660
Telex: 692315F
C

Hewlett-Packard France
Application Center
5, avenue Raymond Chanas
38320 **EYBENS (Grenoble)**
Tel: (76) 62-57-98
Telex: 980124 HP GRENOB EYBE
C

Hewlett-Packard France
Rue Fernand. Forest
Z.A. Kergaradec
29239 **GOUESNOU**
Tel: (98) 41-87-90

Hewlett-Packard France
Parc Club des Tanneries
Batiment B4
4, Rue de la Faisanderie
67381 **LINCOLSHEIM**
(Strasbourg)
Tel: (88) 76-15-00
Telex: 890141F
C,E*,M*,P*

Hewlett-Packard France
Centre d'affaires Paris-Nord
Bâtiment Ampère
Rue de la Commune de Paris
Boite Postale 300
93153 **LE BLANC-MESNIL**
Tel: (1) 865-44-52
Telex: 211032F
C,E,M

Hewlett-Packard France
Parc d'activités Cadéra
Quartier Jean-Mermoz
Avenue du Président JF Kennedy
33700 **MÉRIGNAC (Bordeaux)**
Tel: 33-56-34-0084
Telex: 550105F
C,E,M

Hewlett-Packard France
3, Rue Graham Bell
BP 5149
57074 **METZ Cedex**
Tel: (87) 36-13-31
Telex: 860602F
C,E

Hewlett-Packard France
Miniparc-ZIRST
Chemin du Vieux Chêne
38240 **MEYLAN (Grenoble)**
Tel: (76) 90-38-40
980124 HP Grenoble
C

Hewlett-Packard France
Bureau vert du Bois Briard
Cheman de la Garde
- CP 212 212
44085 **NANTES Cedex**
Tel: (40) 50-32-22
Telex: 711085F
A,C,E,CM*,P

Hewlett-Packard France
125, Rue du Faubourg Bannier
45000 **ORLÉANS**
Tel: 33-38-62-2031
E,P*

Hewlett-Packard France
Zone Industrielle de Courtaboëuf
Avenue des Tropiques
91947 **LES ULIS Cedex (Orsay)**
Tel: 33-6-907 7825
Telex: 600048F
A,C,CM,E,M,P**

Hewlett-Packard France
15, Avenue de L'Amiral-Bruix
75782 **PARIS Cedex 16**
Tel: 33-15-02-1220
Telex: 613663F
C,P*

Hewlett-Packard France
242 Ter. Ave J Mermoz
64000 **PAU**
Tel: 33-59-80-3802
Telex: 550365F
C,E*

Hewlett-Packard France
6, Place Sainte Croix
86000 **POITIERS**
Tel: 33-49-41-2707
Telex: 792335F
C, E*

Hewlett-Packard France
47, Rue de Chatisvle
51100 **REIMS**
Tel: 33-26-88-6919
C, P*

Hewlett-Packard France
Parc d'activités de la Poterie
Rue Louis Kerautel-Botmel
35000 **RENNES**
Tel: 33-99-51-4244
Telex: 740912F
A*, C,E,M,P*

Hewlett-Packard France
98 Avenue de Bretagne
76100 **ROUEN**
Tel: 33-35-63-5766
Telex: 770035F
C,E

Hewlett-Packard France
4, Rue Thomas-Mann
Boite Postale 56
67033 **STRASBOURG Cedex**
Tel: (88) 28-56-46
Telex: 890141F
C,E,M,P*

Hewlett-Packard France
Le Pérípole III
3, Chemin du Pigeonnier de la Céprière
31081 **TOULOUSE Cedex**
Tel: 33-61-40-1112
Telex: 531639F
A,C,E,M,P*

Hewlett-Packard France
Les Cardoulines
Batiment B2
Route des Dolines
Parc d'activité de Valbonne
Sophia Antipolis
06560 **VALBONNE (Nice)**
Tel: (93) 65-39-40
C

Hewlett-Packard France
9, Rue Baudin
26000 **VALENCE**
Tel: 33-75-42-7616
C**

Hewlett-Packard France
Carolor
ZAC de Bois Briard
57640 **VIGY (Metz)**
Tel: (87) 711 20 22
C

Hewlett-Packard France
Parc d'activité des Prés
1, Rue Papin Cedex
59658 **VILLENEUVE D'ASCO**
Tel: 33-20-91-4125
Telex: 160124F
C,E,M,P

Hewlett-Packard France
Parc d'activités Paris-Nord 11
Boite Postale 60020
95971 Roissy Charles de Gaulle
VILLEPINTE
Tel: (1) 48 63 80 80
Telex: 211032F
C,E,M,P*

GABON

Sho Gabon
P.O. Box 89
LIBREVILLE
Tel: 721 484
Telex: 5230

GERMAN FEDERAL REPUBLIC

Hewlett-Packard GmbH
Vertriebszentrum Mitte
Hewlett-Packard-Strasse
D-6380 **BAD HOMBURG**
Tel: (06172) 400-0
Telex: 410 844 hpbhg
A,C,E,M,P

Hewlett-Packard GmbH
Geschäftsstelle
Keithstrasse 2-4
D-1000 **BERLIN 30**
Tel: (030) 21 99 04-0
Telex: 018 3405 hpbln d
A,C,E,M,P

Hewlett-Packard GmbH
Verbindungsstelle Bonn
Friedrich-Ebert-Allee 26
5300 **BONN**
Tel: (88) 234001
Telex: 8869421

Hewlett-Packard GmbH
Vertriebszentrum Südwest
Schickardstrasse 2
D-7030 **BÖBLINGEN**
Postfach 1427
Tel: (07031) 645-0
Telex: 7265 743 hep
A,C,CM,E,M,P

Hewlett-Packard GmbH
Zentralbereich Mktg
Herrenberger Strasse 130
D-7030 **BÖBLINGEN**
Tel: (07031) 14-0
Telex: 7265739 hep
Hewlett-Packard GmbH
Geschäftsstelle
Schleefstr. 28a
D-4600 **DORTMUND-41**
Tel: (0231) 45001
Telex: 822858 hep d od
A,C,E

Hewlett-Packard GmbH
Reparaturzentrum Frankfurt
Berner Strasse 117
6000 **FRANKFURT/MAIN 60**
Tel: (069) 500001-0
Telex: 413249 hpffm

Hewlett-Packard GmbH
Vertriebszentrum Nord
Kapstadtring 5
D-2000 **HAMBURG 60**
Tel: 49-40-63-804-0
Telex: 021 63 032 hph d
A,C,E,M,P

Hewlett-Packard GmbH
Geschäftsstelle
Heidering 37-39
D-3000 **HANNOVER 61**
Tel: (0511) 5706-0
Telex: 092 3259 hphan
A,C,CM,E,M,P

Hewlett-Packard GmbH
Geschäftsstelle
Rosslauer Weg 2-4
D-6800 **MANNHEIM**
Tel: 49-0621-70-05-0
Telex: 0462105 hpmhm
A,C,E

Hewlett-Packard GmbH
Geschäftsstelle
Messerschmittstrasse 7
D-7910 **NEU ULM**
Tel: 49-0731-70-73-0
Telex: 0712816 HP ULM-D
A,C,E*

Hewlett-Packard GmbH
Geschäftsstelle
Emmericher Strasse 13
D-8500 **NÜRNBERG 10**
Tel: (0911) 5205-0
Telex: 0623 860 hpnbg
C,CM,E,M,P

Hewlett-Packard GmbH
Vertriebszentrum Ratingen
Berliner Strasse 111
D-4030 **RATINGEN 4**
Postfach 31 12
Tel: (02102) 494-0
Telex: 589 070 hprad
A,C,E,M,P

Hewlett-Packard GmbH
Vertriebszentrum Muchen
Eschenstrasse 5
D-8028 **TAUFKIRCHEN**
Tel: 49-89-61-2070
Telex: 0524985 hpmch
A,C,CM,E,M,P
Hewlett-Packard GmbH
Geschäftsstelle
Ermisallee
7517 **WALDBRONN 2**
Postfach 1251
Tel: (07243) 602-0
Telex: 782 838 hep k
A,C,E

GREAT BRITAIN See United Kingdom

GREECE

Hewlett-Packard A.E.
178, Kifissias Avenue
6th Floor
HALANDRI-ATHENS
Greece
Tel: 301116473 360, 301116726 090
Telex: 221 286 HPHLGR
A,C,CM**,E,M,P

Kostas Karayannis S.A.
8, Omirou Street
ATHENS 133
Tel: 32 30 303, 32 37 371
Telex: 215962 RKAR GR
A,C*,CM,E

Impexin
Intelect Div.
209 Mesogion
11525 **ATHENS**
Tel: 6474481/2
Telex: 216286
P

Hariri Company
38, Mihalakopoulou
ATHENS 612
Tel: 7236071
Telex: 218767
M*

Hellamco
P.O. Box 87528
18507 **PIRAEUS**
Tel: 4827049
Telex: 241441
A

GUATEMALA

IPESA DE GUATEMALA
Avenida Reforma 3-48, Zona 9
GUATEMALA CITY
Tel: 316627, 317853, 66471/5
9-011-502-2-316627
Telex: 3055765 IPESA GU
A,C,CM,E,M,P

HONG KONG

Hewlett-Packard Hong Kong, Ltd.
G.P.O. Box 795

5th Floor, Sun Hung Kai Centre
30 Harbour Road, Wan Chai

HONG KONG

Tel: 852-5-832-3211

Telex: 66678 HEWPA HX

Cable: HEWPACK HONG KONG
E,C,P

CET Ltd.

10th Floor, Hua Asia Bldg.

64-66 Gloucester Road

HONG KONG

Tel: (5) 200922

Telex: 85148 CET HX

CM

Schmidt & Co. (Hong Kong) Ltd.

18th Floor, Great Eagle Centre

23 Harbour Road, Wanchai

HONG KONG

Tel: 5-8330222

Telex: 74766 SCHMC HX

A,M

ICELAND

Hewlett-Packard Iceland

Hoefdabakka 9

112 REYKJAVIK

Tel: 354-1-67-1000

Telex: 37409

A,C,CM,E,M,P

INDIA

Computer products are sold through
Blue Star Ltd. All computer repairs
and maintenance service is done
through Computer Maintenance Corp.

Blue Star Ltd.

B. D. Patel House

Near Sardar Patel Colony

AHMEDABAD 380 014

Tel: 403531, 403532

Telex: 0121-234

Cable: BLUE FROST

A,C,CM,E

Blue Star Ltd.

40/4 Lavelle Road

BANGALORE 560 001

Tel: 57881, 867780

Telex: 0845-430 BSLBIN

Cable: BLUESTAR

A,C*,CM,E

Blue Star Ltd.

Band Box House

Prabhadevi

BOMBAY 400 025

Tel: 4933101, 4933222

Telex: 011-71051

Cable: BLUESTAR

A,M

Blue Star Ltd.

Sahas

414/2 Vir Savarkar Marg

Prabhadevi

BOMBAY 400 025

Tel: 422-6155

Telex: 011-71193 BSSS IN

Cable: FROSTBLUE

A,CM,E,M

Blue Star Ltd.

Ke:yan, 19 Vishwas Colony

Alkapuri, BORDA, 390 005

Tel: 65235, 65236

Cable: BLUE STAR

A

Blue Star Ltd.

7 Hare Street

P.O. Box 506

CALCUTTA 700 001

Tel: 230131, 230132

Telex: 031-61120 BSNF IN

Cable: BLUESTAR

A,M,C,E

Blue Star Ltd.

133 Kodambakkam High Road

MADRAS 600 034

Tel: 472056, 470238

Telex: 041-379

Cable: BLUESTAR

A,M

Blue Star Ltd.

13 Community Center

New Friends Colony

NEW DELHI 110 065

Tel: 682547

Telex: 031-2463

Cable: BLUEFROST

A,C*,CM,E,M

Blue Star Ltd.

15/16 C Wellesley Rd.

PUNE 411 011

Tel: 22775

Cable: BLUE STAR

A

Blue Star Ltd.

2-2-47/1108 Bolarum Rd.

SECUNDERABAD 500 003

Tel: 72057, 72058

Telex: 0155-459

Cable: BLUEFROST

A,C,E

Blue Star Ltd.

T.C. 7/603 Poornima

Maruthunkuzhi

TRIVANDRUM 695 013

Tel: 65799, 65820

Telex: 0884-259

Cable: BLUESTAR

E

Computer Maintenance Corporation
Ltd.

115, Sarojini Devi Road

SECUNDERABAD 500 003

Tel: 310-184, 345-774

Telex: 031-2960

C**

INDONESIA

BERCA Indonesia P.T.

P.O. Box 496/Jkt.

Jl. Abdul Muis 62

JAKARTA

Tel: 21-373009

Telex: 46748 BERSAL IA

Cable: BERSAL JAKARTA

P

BERCA Indonesia P.T.

P.O. Box 2497/Jkt

Antara Bldg., 12th Floor

Jl. Medan Merdeka Selatan 17

JAKARTA-PUSAT

Tel: 21-340417

Telex: 46748 BERSAL IA

A,C,E,M,P

BERCA Indonesia P.T.

Jalan Kutai 24

SURABAYA

Tel: 67118

Telex: 31146 BERSAL SB

Cable: BERSAL-SURABAYA

A*,E,M,P

IRAQ

Hewlett-Packard Trading S.A.

Service Operation

Al Mansoor City 9B/3/7

BAGHDAD

Tel: 551-49-73

Telex: 212-455 HEPAIRAQ IK

C

IRELAND

Hewlett-Packard Ireland Ltd.

Temple House, Temple Road

Blackrock, Co. DUBLIN

Tel: 88/333/99

Telex: 30439

C,E,P

Hewlett-Packard Ltd.

75 Belfast Rd, Carrickfergus

Belfast BT38 8PH

NORTHERN IRELAND

Tel: 09603-67333

Telex: 747626

M

ISRAEL

Eidan Electronic Instrument Ltd.

P.O. Box 1270

JERUSALEM 91000

16, Ohaliav St.

JERUSALEM 94467

Tel: 533 221, 553 242

Telex: 25231 AB/PAKRD IL

A,M

Computation and Measurement

Systems (CMS) Ltd.

11 Masad Street

67060

TEL-AVIV

Tel: 388 388

Telex: 33569 Motil IL

C,CM,E,P

ITALY

Hewlett-Packard Italiana S.p.A.

Traversa 99C

Via Giulio Petroni, 19

I-70124 BARI

Tel: (080) 41-07-44

C,M

Hewlett-Packard Italiana S.p.A.

Via Emilia, 51/C

I-40011 BOLOGNA Anzola Dell'Emilia

Tel: 39-051-731061

Telex: 511630

C,E,M

Hewlett-Packard Italiana S.p.A.

Via Principe Nicola 43G/C

I-95126 CATANIA

Tel: (095) 37-10-87

Telex: 970291

C

Hewlett-Packard Italiana S.p.A.

Via G. di Vittorio 10

20094 CORSICO (Milano)

Tel: 39-02-4408351

Hewlett-Packard Italiana S.p.A.

Viale Brigata Bisagno 2

16129 GENOVA

Tel: 39-10-541141

Telex: 215238

Hewlett-Packard Italiana S.p.A.

Viale G. Modugno 33

I-16156 GENOVA PEGLI

Tel: (010) 68-37-07

Telex: 215238

C,E

Hewlett-Packard Italiana S.p.A.

Via G. di Vittorio 9

I-20063 CERNUSCO SUL

NAVIGLIO

(Milano)

Tel: (02) 923691

Telex: 334632

A,C,CM,E,M,P

Hewlett-Packard Italiana S.p.A.

Via Nuova Rivoltana 95

20090 LIMITO (Milano)

Tel: 02-92761

Hewlett-Packard Italiana S.p.A.

Via Nuova San Rocco a

Capodimonte, 62/A

I-80131 NAPOLI

Tel: (081) 7413544

Telex: 710698

A**,C,E,M

Hewlett-Packard Italiana S.p.A.

Via Orazio 16

80122 NAPOLI

Tel: (081) 7611444

Telex: 710698

Hewlett-Packard Italiana S.p.A.

Via Pellizzo 15

35128 PADOVA

Tel: 39-49-664-888

Telex: 430315

A,C,E,M

Hewlett-Packard Italiana S.p.A.

Viale C. Pavese 340

I-00144 ROMA EUR

Tel: 39-65-48-31

Telex: 610514

A,C,E,M,P*

Hewlett-Packard Italiana S.p.A.

Via di Casellina 57/C

500518 SCANDICCI-FRENZE

Tel: 39-55-753863

C,E,M

Hewlett-Packard Italiana S.p.A.

Corso Svizzera, 185

I-10144 TORINO

Tel: 39-11-74-4044

Telex: 221079

A*,C,E

IVORY COAST

S.I.T.E.L.

Societe Ivoirienne de

Telecommunications

Bd. Giscard d'Estaing

Carrefour Marcory

Zone 4.A.

Boite postale 2580

ABIDJAN 01

Tel: 353600

Telex: 43175

E

S.I.T.I.

Immeuble "Le General"

SALES & SUPPORT OFFICES

Arranged alphabetically by country

5

JAPAN (Cont'd)

Yokogawa-Hewlett-Packard Ltd.
Chuo Bldg., 5-4-20 Nishi-Nakajima
4-20 Nishinakajima, 5 Chome,
Yodogawa-ku

OSAKA, 532
Tel: (06) 304-6021
Telex: YHPOSA 523-3624
C,CM,E,M,P*

Yokogawa-Hewlett-Packard Ltd.
1-27-15, Yabe
SAGAMIHARA Kanagawa, 229
Tel: 0427 59-1311

Yokogawa-Hewlett-Packard Ltd.
Hamamtsu Motoshiro-Cho Daichi
Seimei Bldg 219-21, Motoshiro-Cho
Hamamatsu-shi
SHIZUOKA, 430
Tel: (0534) 56 1771
C,E

Yokogawa-Hewlett-Packard Ltd.
Shinjuku Daiichi Seimei Bldg.
2-7-1, Nishi Shinjuku
Shinjuku-ku, **TOKYO 163**
Tel: 03-348-4611
C,E,M

Yokogawa Hewlett-Packard Ltd.
9-1, Takakura-cho
Hachioji-shi, **TOKYO, 192**
Tel: 81-426-42-1231
C,E

Yokogawa-Hewlett-Packard Ltd.
3-29-21 Takaido-Higashi, 3 Chome
Suginami-ku **TOKYO 168**
Tel: (03) 331-6111
Telex: 232-2024 YHPTOK
C,CM,E,P*

Yokogawa Hokushin Electric
Corporation
Shinjuku-NS Bldg. 10F
4-1 Nishi-Shinjuku 2-Chome
Shinjuku-ku
TOKYO, 163
Tel: (03) 349-1859
Telex: J27584
A

Yokogawa Hokushin Electric Corp.
9-32 Nokacho 2 Chome
Musashino-shi
TOKYO, 180
Tel: (0422) 54-1111
Telex: 02822-421 YEW MTK J
A

Yokogawa-Hewlett-Packard Ltd.
Meiji-Seimei
Utsunomiya Odori Building
1-5 Odori, 2 Chome
UTSUNOMIYA, Tochigi 320
Tel: (0286) 33-1153
C,E

Yokogawa-Hewlett-Packard Ltd.
Yasuda Seimei Nishiguchi Bldg.
30-4 Tsuruya-cho, 3 Chome
Kanagawa-ku, **YOKOHAMA 221**
Tel: (045) 312-1252
C,CM,E

JORDAN

Scientific and Medical Supplies Co.
P.O. Box 1387

AMMAN
Tel: 24907, 39907
Telex: 21456 SABCO JO
C,E,M,P

KENYA

ADCOM Ltd., Inc., Kenya
P.O.Box 30070

NAIROBI
Tel: 331955
Telex: 22639
E,M

KOREA

Samsung Hewlett-Packard Co. Ltd.
Dongbang Yeoeuido Building
12-16th Floors
36-1 Yeoeuido-Dong
Youngdeungpo-Ku

SEOUL
Tel: 784-4666, 784-2666
Telex: 25166 SAMSAN K
C,CM,E,M,P

Young In Scientific Co., Ltd.
Youngwha Building
547 Shinsa Dong, Kangnam-Ku
SEOUL 135
Tel: 546-7771
Telex: K23457 GINSCO
A

Dongbang Healthcare
Products Co. Ltd.
Suite 301 Medical Supply Center
Bldg. 1-31 Dongsungdong
Jong Ro-gu, **SEOUL**
Tel: 764-1171, 741-1641
Telex: K25706 TKBKO
Cable: TKBEEPKO
M

KUWAIT

Al-Khaldiya Trading & Contracting
P.O. Box 830
SAFAT
Tel: 424910, 411726
Telex: 22481 AREEG KT
Cable: VISCOUNT
E,M,A

Gulf Computing Systems
P.O. Box 25125
SAFAT
Tel: 435969
Telex: 23648
P

Photo & Cine Equipment
P.O. Box 270
SAFAT
Tel: 2445111
Telex: 22247 MATIN KT
Cable: MATIN KUWAIT
P

W.J. Towell Computer Services
P.O. Box 5897
SAFAT
Tel: 2462640/1
Telex: 30336 TOWELL KT
C

LEBANON

Computer Information Systems S.A.L.
Chammass Building
P.O. Box 11-6274 Dora

BEIRUT
Tel: 89 40 73
Telex: 42309 chacies le
C,E,M,P

LIBERIA

Unichemicals Inc.
P.O. Box 4509

MONROVIA
Tel: 224282
Telex: 4509
E

LUXEMBOURG

Hewlett-Packard Belgium S.A./N.V.
Blvd de la Woluwe, 100
Woluwedal
B-1200 **BRUSSELS**

Tel: (02) 762-32-00
Telex: 23-494 paloben br
A,C,CM,E,M,P

MADAGASCAR

Technique et Precision
12, rue de Nice
P.O. Box 1227
101 **ANTANANARIVO**
Tel: 22090
Telex: 22255
P

MALAYSIA

Hewlett-Packard Sales (Malaysia)
Sdn. Bhd.
9th Floor
Chung Khiaw Bank Building
46, Jalan Raja Laut
50736 **KUALA LUMPUR, MALAYSIA**
Tel: 03-2986555
Telex: 31011 HPSM MA
A,C,E,M,P*

Protel Engineering
P.O. Box 1917
Lot 6624, Section 64
23/4 Pending Road
Kuching, **SARAWAK**
Tel: 36299
Telex: 70904 PROMAL MA
Cable: PROTELENG
A,E,M

MALTA

Philip Toledo Ltd.
Kirkirkara P.O. Box 11
Notabile Rd.
MRIEHEL
Tel: 447 47, 455 66, 4915 25
Telex: Media MW 649
E,M,P

MAURITIUS

Blanche Birger Co. Ltd.
18, Jules Koenig Street
PORT LOUIS
Tel: 20828
Telex: 4296
P

MEXICO

Hewlett-Packard de Mexico,
S.A. de C.V.
Rio Nio No. 4049 Desp. 12
Fracc. Cordoba
JUAREZ
Tel: 161-3-15-62
P

Hewlett-Packard de Mexico,
S.A. de C.V.
Condominio Kadereyta
Circuito del Mezon No. 186 Desp. 6
COL. DEL PRADO - 76030 Qro.
Tel: 463-6-02-71
P

Hewlett-Packard de Mexico,
S.A. de C.V.
Monti Morelos No. 299
Fraccionamiento Loma Bonita 45060
GUADALAJARA, Jalisco
Tel: 36-31-48-00
Telex: 0684 186 ECOMÉ
P

Microcomputadoras
Hewlett-Packard, S.A.
Monti Peivoux 115
LOS LOMAS, Mexico, D.F.
Tel: 520-9127
P

Microcomputadoras Hewlett-Packard,
S.A. de C.V.
Monte Peivoux No. 115
Lomas de Chapultepec, 11000
MEXICO, D.F.
Tel: 520-9127
P

Hewlett-Packard de Mexico,
S.A. de C.V.
Monte Peivoux No. 111
Lomas de Chapultepec
11000 **MEXICO, D.F.**
Tel: 5-40-62-28, 72-66, 50-25
Telex: 17-74-507 HEWPACK MEX
A,C,CM,E,M,P

Hewlett-Packard De Mexico (Polanco)
Avenida Ejercito Nacional #579
2do y 3er piso
Colonia Granada 11560
MEXICO D.F.
Tel: 254-4433
P

Hewlett-Packard de Mexico,
S.A. de C.V.
Czda. del Valle
409 Ote. 4th Piso
Colonia del Valle
Municipio de Garza
Garcia Nuevo Leon
66220 **MONTERREY, Nuevo León**
Tel: 83-78-42-40
Telex: 382410 HPMY
C

Infograficas y Sistemas
del Noreste, S.A.
Rio Orinoco #171 Oriente
Despacho 2001
Colonia Del Valle
MONTERREY
Tel: 559-4415, 575-3837
Telex: 483164
A,E

Hewlett-Packard de Mexico,
S.A. de C.V.
Blvd. Independencia No. 2000 Ote.
Col. Estrella
TORREON, COAH.
Tel: 171-18-21-99
P

MOROCCO

Etablissement Hubert Dolbeau & Fils
81 rue Karatchi
B.P. 11133
CASABLANCA
Tel: 3041-82, 3068-38
Telex: 23051, 22822
E

Gerep
2, rue Agadir
Boite Postale 156
CASABLANCA 01
Tel: 272093, 272095
Telex: 23 739
P

Sama-Maroc
Dept. Seric
6, rue Lapebie
CASABLANCA
Tel: 260980
Telex: 21641
C,P

NETHERLANDS

Hewlett-Packard Nederland B.V.
Startbaan 16
NL-1187 XR **AMSTELVEEN**
P.O. Box 667
NL-1180 AR **AMSTELVEEN**
Tel: (020) 547-6911
Telex: 13 216 HEPAN NL
A,C,CM,E,M,P

Hewlett-Packard Nederland B.V.
Bongerd 2
P.O. Box 41
NL 2900AA **CAPELLE A/D IJSSEL**
Tel: 31-20-51-6444
Telex: 21261 HEPAC NL
C,E

Hewlett-Packard Nederland B.V.
Pastoor Petersstraat 134-136
P.O. Box 2342
NL 5600 CH **EINDHOVEN**
Tel: 31-40-32-6911
Telex: 51484 hepae nl
C,E,P

NEW ZEALAND

Hewlett-Packard (N.Z.) Ltd.
5 Owens Road
P.O. Box 26-189
Epsom, **AUCKLAND**
Tel: 64-9-687-159
Cable: HEWPAK Auckland
C,CM,E,P*

Hewlett-Packard (N.Z.) Ltd.
184-190 Willis Street
WELLINGTON
P.O. Box 9443
Courtenay Place, **WELLINGTON 3**
Tel: 64-4-887-199
Cable: HEWPAK Wellington
C,CM,E,P

Northrop Instruments & Systems Ltd.
369 Khyber Pass Road
P.O. Box 8602
AUCKLAND
Tel: 794-091
Telex: 60605
A,M

Northrop Instruments & Systems Ltd.
110 Mandeville St.
P.O. Box 8388
CHRISTCHURCH
Tel: 488-873
Telex: 4203
A,M

Northrop Instruments & Systems Ltd.
Sturdee House
85-87 Ghuznee Street
P.O. Box 2406
WELLINGTON
Tel: 850-091
Telex: NZ 3380
A,M

NIGERIA

Elmecc Nigeria Ltd.
45 Saka Tirubu St.
Victoria Island
LAGOS
Tel: 61-98-94
Telex: 20-117
E

NORTHERN IRELAND See United Kingdom

NORWAY

Hewlett-Packard Norge A/S
Folke Bernadottes vei 50
P.O. Box 3558
N-5033 **FYLLINGSDALEN** (Bergen)
Tel: 0047/5/16 55 40
Telex: 78621 hpnas n
C,E,M

Hewlett-Packard Norge A/S
Osterdalen 16-18
P.O. Box 34
N-1345 **OEËTERAAS**
Tel: 47-2-17-1180
Telex: 78621 hpnas n
A,C,CM,E,M,P

Hewlett-Packard Norge A/S
Boehmergt. 42
Box 2470
N-5037 **BOLHEIMSVIK**
Tel: 0047/5/29 00 90

OMAN

Khimjil Ramdas
P.O. Box 19
MUSCAT/SULTANATE OF OMAN
Tel: 795 901
Telex: 3489 BROKER MB MUSCAT
P

Suhail & Saud Bahwan
P.O. Box 169
MUSCAT/SULTANATE OF OMAN
Tel: 734 201-3
Telex: 5274 BAHWAN MB
E

Imtac LLC
P.O. Box 9196
MINA AL FAHAL/SULTANATE OF OMAN
Tel: 70-77-27, 70-77-23
Telex: 3865 Tawoos On
A,C,M

PAKISTAN

Mushko & Company Ltd.
House No. 16, Street No. 16
Sector F-6/3
ISLAMABAD
Tel: 824545
Telex: 54001 Muski Pk
Cable: FEMUS Islamabad
A,E,P*

Mushko & Company Ltd.
Oosman Chambers
Abdullah Haroon Road
KARACHI 0302
Tel: 524131, 524132
Telex: 2894 MUSKO PK
Cable: COOPERATOR Karachi
A,E,P*

PANAMA

Electronico Balboa, S.A.
Calle Samuel Lewis, Ed. Alfa
Apartado 4929
PANAMA CITY
Tel: 9-011-507-636613
Telex: 368 3483 ELECTRON PG
CM,E,M,P

PERU

Cía Electro Médica S.A.
Los Flamencos 145, Ofc. 301/2
San Isidro
Casilla 1030
LIMA 1
Tel: 9-011-511-4-414325, 41-3705
Telex: 39425257 PE PB SIS
CM,E,M,P
SAMS S.A.
Arenida Republica de Panama 3534
San Isidro, **LIMA**
Tel: 9-011-511-4-229332/413984/
413226
Telex: 39420450 PE LIBERTAD
A,C,P

PHILIPPINES

The Online Advanced Systems Corp.
2nd Floor, Electra House
115-117 Esteban Street
P.O. Box 1510
Legaspi Village, Makati
Metro **MANILA**
Tel: 815-38-10 (up to 16)
Telex: 63274 ONLINE PN
A,C,E,M,P

PORTUGAL

Mundinter Intercambio
Mundial de Comércio S.A.R.L.
Av. Antonio Augusto Aguiar 138
Apartado 2761
LISBON
Tel: (19) 53-21-31, 53-21-37
Telex: 16691 munter p
M

Soquimica
Av. da Liberdade, 220-2
1298 **LISBOA** Codex
Tel: 56-21-82
Telex: 13316 SABASA
A

Telectra-Empresa Técnica de
Equipamentos Eléctricos S.A.R.L.
Rua Rodrigo da Fonseca 103
P.O. Box 2531
LISBON 1
Tel: (19) 68-60-72
Telex: 12598
C,M,E
C.P.C.S.I.
Rua de Costa Cabral 575
4200 **PORTO**
Tel: 499174/495173
Telex: 28054
C,P

PUERTO RICO

Hewlett-Packard Puerto Rico
101 Muñoz Rivera Av
Esu. Calle Ochoa
HATO REY, Puerto Rico 00918
Tel: (809) 754-7800
A,C,CM,M,E,P

QATAR

Computer Arabia
P.O. Box 2750
DOHA
Tel: 428555
Telex: 4806 CHPARB
P
Nasser Trading & Contracting
P.O. Box 1563
DOHA
Tel: 422170
Telex: 4439 NASSER DH
M

SAUDI ARABIA

Modern Electronics Establishment
Hewlett-Packard Division
P.O. Box 281
Thuobah
AL-KHOBAR 31952
Tel: 895-1760, 895-1764
Telex: 671 106 HPMEEK SJ
Cable: ELECTA AL-KHOBAR
C,E,M

Modern Electronics Establishment
Hewlett-Packard Division
P.O. Box 1228
Redec Plaza, 6th Floor
JEDDAH
Tel: 644 96 28
Telex: 4027 12 FARNAS SJ
Cable: ELECTA JEDDAH
A,C,CM,E,M,P

Modern Electronics Establishment
Hewlett-Packard Division
P.O. Box 22015
RIYADH 11495
Tel: 491-97 15, 491-63 87
Telex: 202049 MEERYD SJ
C,E,M

Abdul Ghani El Ajou Corp.
P.O. Box 78
RIYADH
Tel: 40 41 717
Telex: 200 932 EL AJOU
P

SCOTLAND See United Kingdom

SENEGAL

Societe Hussein Ayad & Cie.
76, Avenue Georges Pompidou
B.P. 305
DAKAR
Tel: 32339
Cable: AYAD-Dakar
E
Monager Distribution S.A.
1, Rue Parent
B.P. 148
DAKAR
Tel: 215 671
Telex: 587
P

Systeme Service Conseil (SSC)
14, Avenue du Parachois
DAKAR ETOLE
Tel: 219976
Telex: 577
C,P

SINGAPORE

Hewlett-Packard Singapore (Sales)
Pte. Ltd.
1150 Depot Road
SINGAPORE, 0410
Tel: 4731788
Telex: 34209 HPSGSO RS
Cable: HEWPACK, Singapore
A,C,E,M,P
Dynamar International Ltd.
Unit 05-11 Block 6
Kolam Ayer Industrial Estate
SINGAPORE 1334
Tel: 747-6188
Telex: 26283 RS
CM

SOUTH AFRICA

Hewlett-Packard So Africa (Pty.) Ltd.
P.O. Box 120
Howard Place, **CAPE PROVINCE**
7450 South Africa
Tel: 27 121153-7954
Telex: 57-20006
A,C,CM,E,M,P
Hewlett-Packard So Africa (Pty.) Ltd.
2nd Floor Juniper House
92 Overport Drive
DURBAN 4067
Tel: 27-31-28-4178
Telex: 6-22954
C

Hewlett-Packard So Africa (Pty.) Ltd.
Shop 6 Linton Arcade
511 Cape Road
Linton Grange
PORT ELIZABETH 6001
Tel: 27141130 1201
Telex: 24-2916
C

Hewlett-Packard So Africa (Pty.) Ltd.
Fountain Center
Kalkoen Str.
Monument Park Ext 2
PRETORIA 0105
Tel: (012) 45 5725
Telex: 32163
C,E

Hewlett-Packard So Africa (Pty.) Ltd.
Private Bag Wendywood
SANDTON 2144
Tel: 27-11-802-5111, 27-11-802-5125
Telex: 4-20877 SA
Cable: HEWPACK Johannesburg
A,C,CM,E,M,P

SPAIN

Hewlett-Packard Española, S.A.
Calle Entenza, 321
E-BARCELONA 29
Tel: 3/322 24 51, 321 73 54
Telex: 52603 hpbee
A,C,E,M,P

Hewlett-Packard Española, S.A.
Calle San Vicente S/N
Edificio Albia II-7B
48001 BILBAO
Tel: 4/423 83 06
A,C,E,M
Hewlett-Packard Española, S.A.
Crta. N-VI, Km. 16, 400
Las Rozas
E-MADRID
Tel: (1) 637.00.11
Telex: 23515 HPE
C,M

Hewlett-Packard Española, S.A.
Avda. S. Francisco Javier, S/N
Planta 10. Edificio Sevilla 2
E-SEVILLA 5, SPAIN
Tel: 54/64 44 54
Telex: 72933
A,C,M,P

Hewlett-Packard Española, S.A.
Isabel La Católica, 8
E-46004 VALENCIA
Tel: 34-6-361 1354
Telex: 63435
C,P

Hewlett-Packard Española, S.A.
Av. de Zugazarte, 8
Las Arenas-Guecho
E-48930 VIZCAYA
VIZCAYA
Tel: 34-423-83 06
Telex: 33032

SWEDEN

Hewlett-Packard Sverige AB
Östra Tullgatan 3
S-20011 **MALMÖ**
Box 6132
Tel: 46-40-702-70
Telex: (854) 17886 (via Spånga office)
C,P
Hewlett-Packard Sverige AB
Elementvagen 16
S-7022 7 **ÖREBRO**
Tel: 49-019-10-4820
Telex: (854) 17886 (via Spånga office)
C

Hewlett-Packard Sverige AB
Skalhottsgatan 9, Kista
P.O. Box 19
S-16393 **SPÅNGA**
Tel: (08) 750-2000
Telex: (854) 17886
Telefax: (08) 7527781
A,C,CM,E,M,P

Hewlett-Packard Sverige AB
Box 266
Topasgatan 1A
S-42123 **VÄSTRA-FRÖLUNDA**
(Gothenburg)
Tel: 46-031-89-1000
Telex: (854) 17886 (via Spånga office)
A,C,CM,E,M,P

SUDAN

Mediterranean Engineering
& Trading Co. Ltd.
P.O. Box 1025
KHARTOUM
Tel: 41184
Telex: 24052
C,P

SWITZERLAND

Hewlett-Packard (Schweiz) AG
Clarastrasse 12
CH-4058 BASEL
Tel: 41-61-33-5920
A,C,E,P
Hewlett-Packard (Schweiz) AG
7, rue du Bois-du-Lan
Case postale 365-1366
CH-1217 MEYRIN 1
Tel: (0041) 22-83-11-11
Telex: 27333 HPAG CH
A,C,CM,E,M,P

SALES & SUPPORT OFFICES

Arranged alphabetically by country

7

SWITZERLAND (Cont'd) TOGO

Hewlett-Packard (Schweiz) AG
Allmend 2
CH-8967 WIDEN
Tel: 41-57-31-2111
Telex: 53933 hpag ch
Cable: HPAG CH
A,C,CM,E,M,P

Hewlett-Packard (Schweiz) AG
Schwamendingenstrasse 10
CH-8050 ZURICH
Tel: 41-1-315-8181
Telex: 823 537 HPAG CH
C,P

SYRIA

General Electronic Inc.
Nuri Basha Ahnaf Ebn Kays Street
P.O. Box 5781

DAMASCUS

Tel: 33-24-87
Telex: 44-19-88
Cable: ELECTROBOR DAMASCUS
E

Middle East Electronics
P.O.Box 2308

Abu Rumaneh

DAMASCUS

Tel: 33 45 92
Telex: 411 771 Meesy
M

TAIWAN

Hewlett-Packard Taiwan Ltd.
THM Office

2, Huan Nan Road
CHUNG LI, Taoyuan
Tel: (034) 929-666

C

Hewlett-Packard Taiwan Ltd.

Kaohsiung Office
11/F, 456, Chung Hsiao 1st Road
KAOSHIUNG

Tel: (07) 2412318
C,E

Hewlett-Packard Taiwan Ltd.

8th Floor, Hewlett-Packard Building
337 Fu Hsing North Road
TAIPEI

Tel: (02) 712-0404
Telex: 24439 HEWPACK
Cable: HEWPACK Taipei
A,C,CM,E,M,P

Ing Lih Trading Co.

3rd Floor, No. 7, Sect. 2
Jen Ai Road
TAIPEI 100

Tel: (02) 394-8191
Telex: 22894 SANKWANG
A

THAILAND

Unimesa Co. Ltd.
30 Patpong Ave., Suriwong
BANGKOK 5,
Tel: 235-5727, 234-0991/3
Telex: 84439 Simonco TH
Cable: UNIMESA Bangkok
A,C,E,M

Bangkok Business Equipment Ltd.
5/C-6 Dejo Road
BANGKOK

Tel: 234-8670, 234-8671
Telex: 87699-BEQUIPT TH
Cable: BUSIQUIPT Bangkok
P

Societe Africaine De Promotion
Immeuble Sageb
Rue d'Atakpame
P.O. Box 4150
LOME
Tel: 21-62-88
Telex: 5357
P

TRINIDAD & TOBAGO

Caribbean Telecoms Ltd.
Corner McAllister Street &
Eastern Main Road, Laventille
P.O. Box 732

PORT-OF-SPAIN

Tel: 624-4213
Telex: 22561 CARTEL WG
Cable: CARTEL, PORT OF SPAIN
CM,E,M,P

Computer and Controls Ltd.

P.O. Box 51
1 Taylor Street
PORT-OF-SPAIN
Tel: (809) 622-7719/622-7985
Telex: 38722798 COMCON WG
LOGO AGENCY 1264
A,P

Feral Assoc.

8 Fitzgerald Lane

PORT-OF-SPAIN

Tel: 62-36864, 62-39255
Telex: 22432 FERALCO
Cable: FERALCO
M

TUNISIA

Tunisie Electronique S.A.R.L.
31 Avenue de la Liberte

TUNIS

Tel: 280-144
C,E,P

Tunisie Electronique S.A.R.L.
94, Av. Jugurtha, Mutuelleville
1002 TUNIS-BELVEDERE

Tel: 280144

Telex: 13238

C,E,P

Corema S.A.
1 ter. Av. de Carthage

TUNIS

Tel: 253-821
Telex: 12319 CABAM TN
M

TURKEY

E.M.A
Mediha Eldem Sokak No. 41/6
Yenisehir

ANKARA

Tel: 319175
Telex: 42321 KTX TR
Cable: EMATRADE ANKARA
M

Teknim Company Ltd.

Iran Caddesi No. 7

Karaklidere

ANKARA

Tel: 275800
Telex: 42155 TKNM TR
C,E

Kurt & Kurt A.S.

Mithatpasa Caddesi No. 75
Kat 4 Kizilay

ANKARA

Tel: 318875/6/7/8
Telex: 42490 MESR TR
A

Saniva Bilgisayar Sistemleri A.S.

Buyukdere Caddesi 103/6
Gayrettepe

ISTANBUL

Tel: 1673180
Telex: 26345 SANI TR
C,P

Best Inc.

Esentepe, Gazeteciler Sitesi

Keskin Kalem

Sokak 6/3, Gayrettepe

ISTANBUL

Tel: 172 1328, 173 3344
Telex: 42490

A

UNITED ARAB EMIRATES

Emitac Ltd.

P.O. Box 1641

SHARJAH

Tel: 591181

Telex: 68136 EMITAC EM

Cable: EMITAC SHARJAH

E,C,M,P,A

Emitac Ltd.

P.O. Box 2711

ABU DHABI

Tel: 820419-20

Cable: EMITACH ABUDHABI

Emitac Ltd.

P.O. Box 8391

DUBAI,

Tel: 377591

Emitac Ltd.

P.O. Box 473

RAS AL KHAIMAH

Tel: 28133, 21270

UNITED KINGDOM ENGLAND

Hewlett-Packard Ltd.

Miller House

The Ring, BRACKNELL

Berks RG12 1XN

Tel: 44/344/424-898

Telex: 848733

E

Hewlett-Packard Ltd.

Elstree House, Elstree Way

BOREHAMWOOD, Herts WD6 1SG

Tel: 01 207 5000

Telex: 8952716

C,E

Hewlett-Packard Ltd.

Oakfield House, Oakfield Grove

Clifton BRISTOL, Avon BS8 2BN

Tel: 44-272-736 806

Telex: 444302

C,E,P

Hewlett-Packard Ltd.

9 Bridewell Place

LONDON EC4V 6BS

Tel: 44-01-583-6565

Telex: 298163

C,P

Hewlett-Packard Ltd.

Pontefract Road

NORMANTON, West Yorkshire WF6 1RN

Tel: 44/924/895 566

Telex: 557355

C,P

Hewlett-Packard Ltd.

The Quadrangle

106-118 Station Road

REDHILL, Surrey RH1 1PS

Tel: 44-737-686-55

Telex: 947234

C,E,P

Hewlett-Packard Ltd.

Avon House

435 Stratford Road

Shirley, SOLIHULL, West Midlands

B90 4BL

Tel: 44-21-745-8800

Telex: 339105

C,E,P

Hewlett-Packard Ltd.

Heathside Park Road

Cheadle Heath, Stockport

SK3 ORB, United Kingdom

Tel: 44-061-428-0828

Telex: 668068

A,C,E,M,P

Hewlett-Packard Ltd.

Harmon House

No. 1 George Street

UXBRIDGE, Middlesex UX8 1YH

Tel: 895 720 20

Telex: 893134/5

C,CM,E,M,P

Hewlett-Packard Ltd.

King Street Lane

Winnersh, WOKINGHAM

Berkshire RG11 5AR

Tel: 44/734/784774

Telex: 8471789

A,C,E,M,P

NORTHERN IRELAND

Hewlett-Packard (Ireland) Ltd.

Carrickfergus Industrial Centre

75 Belfast Road, Carrickfergus

CO. ANTRIM BT38 8PM

Tel: 09603 67333

C,E

Cardiac Services Company

95A Finaghy Road South

BELFAST, BT10 0BY

Tel: 0232-625566

Telex: 747626

M

SCOTLAND

Hewlett-Packard Ltd.

1/3 Springburn Place

College Milton North

EAST KILBRIDE, G74 5NU

Tel: 041-332-6232

Telex: 779615

C,E

Hewlett-Packard Ltd.

SOUTH QUEENSFERRY

West Lothian, EH30 9TG

Tel: 031 331 1188

Telex: 72682 HPSQFYG

C,CM,E,M,P

UNITED STATES

Hewlett-Packard Co.
Customer Information Center
Tel: (800) 752-0900
Hours: 6:00 AM to 5:00 PM
Pacific Time

Alabama

Hewlett-Packard Co.
2100 Riverchase Center
Building 100 - Suite 118
BIRMINGHAM, AL 35244
Tel: (205) 988-0547
A,C,M,P*

Hewlett-Packard Co.

420 Wynn Drive
HUNTSVILLE, AL 35805
Tel: (205) 830-2000
C,CM,E,M*

Alaska

Hewlett-Packard Co.
4000 Old Seward Highway
Suite 101
ANCHORAGE, AK 99503
Tel: (907) 563-8855
C,E

Arizona

Hewlett-Packard Co.
8080 Pointe Parkway West
PHOENIX, AZ 85044
Tel: (602) 273-8000
A,C,CM,E,M,P

Hewlett-Packard Co.
3400 East Britannia Dr.
Bldg. C, Suite 124

TUCSON, AZ 85706

Tel: (602) 573-7400

C,E,M**

California

Hewlett-Packard Co.
99 South Hill Dr.
BRISBANE, CA 94005
Tel: (415) 330-2500

C

Hewlett-Packard Co.
1907 North Gateway Blvd.
FRESNO, CA 93727
Tel: (209) 252-9652
C,M

Hewlett-Packard Co.
1421 S. Manhattan Av.
FULLERTON, CA 92631
Tel: (714) 999-6700
C,CM,E,M

Hewlett-Packard Co.
7408 Hollister Ave. #A
GOLETA, CA 93117
Tel: (805) 685-6100
C,E

Hewlett-Packard Co.
2525 Grand Avenue
LONG BEACH, CA 90815
Tel: (213) 498-1111
C

Hewlett-Packard Co.
5651 West Manchester Ave.
LOS ANGELES, CA 90045
Tel: (213) 337-8000
Hewlett-Packard Co.
3155 Porter Drive
PALO ALTO, CA 94304
Tel: (415) 857-8000
C,E

Hewlett-Packard Co.
5725 W. Las Positas Blvd.
PLEASANTON, CA 94566
Tel: (415) 460-0282
C

Hewlett-Packard Co.
4244 So. Market Court, Suite A
SACRAMENTO, CA 95834
Tel: (916) 929-7222
A*,C,E,M

Hewlett-Packard Co.
9606 Aero Drive
SAN DIEGO, CA 92123
Tel: (619) 279-3200
C,CM,E,M

Hewlett-Packard Co.
3003 Scott Boulevard
SANTA CLARA, CA 95054
Tel: (408) 988-7000
Telex: 910-338-0586
A,C,CM,E

Hewlett-Packard Co.
2150 W. Hillcrest Dr.
THOUSAND OAKS, CA 91320
(805) 373-7000
C,CM,E

Colorado
Hewlett-Packard Co.
2945 Center Green Court South
Suite A
BOULDER, CO 80301
Tel: (303) 499-6655
A,C,E

Hewlett-Packard Co.
24 Inverness Place, East
ENGLEWOOD, CO 80112
Tel: (303) 649-5000
A,C,CM,E,M

Connecticut
Hewlett-Packard Co.
500 Sylvan Av.
BRIDGEPORT, CT 06606
Tel: (203) 371-6454
C,E

Hewlett-Packard Co.
47 Barnes Industrial Road South
WALLINGFORD, CT 06492
Tel: (203) 265-7801
A,C,CM,E,M

Florida
Hewlett-Packard Co.
2901 N.W. 62nd Street
FORT LAUDERDALE, FL 33309
Tel: (305) 973-2600
C,E,M,P*

Hewlett-Packard Co.
6800 South Point Parkway
Suite 301
JACKSONVILLE, FL 32216
Tel: (904) 636-9955
C*,M**

Hewlett-Packard Co.
255 East Drive, Suite B
MELBOURNE, FL 32901
Tel: (305) 729-0704
CM,E

Hewlett-Packard Co.
6177 Lake Ellenor Drive
ORLANDO, FL 32809
Tel: (305) 859-2900
A,C,CM,E,P*

Hewlett-Packard Co.
4700 Bayou Blvd.
Building 5
PENSACOLA, FL 32503
Tel: (904) 476-8422
A,C,M

Hewlett-Packard Co.
5550 W. Idlewild, #150
TAMPA, FL 33614
Tel: (813) 884-3282
C,E,M,P

Georgia
Hewlett-Packard Co.
2015 South Park Place
ATLANTA, GA 30339
Tel: (404) 955-1500
Telex: 810-766-4890
A,C,CM,E,M,P*

Hewlett-Packard Co.
3607 Parkway Lane
Suite 300
NORCROSS, GA 30092
Tel: (404) 448-1894
C,E,P

Hawaii
Hewlett-Packard Co.
Pacific Tower
1001 Bishop St.
Suite 2400
HONOLULU, HI 96813
Tel: (808) 526-1555
A,C,E,M

Idaho
Hewlett-Packard Co.
11309 Chinden Blvd.
BOISE, ID 83714
Tel: (208) 323-2700
C

Illinois
Hewlett-Packard Co.
2205 E. Empire St.
P.O. Box 1607
BLOOMINGTON, IL 61702-1607
Tel: (309) 662-9411
A,C,E,M**

Hewlett-Packard Co.
525 W. Monroe, #1308
CHICAGO, IL 60606
Tel: (312) 930-0010
C

Hewlett-Packard Co.
1200 East Diehl Road
NAPERVILLE, IL 60566
Tel: (312) 357-8800
C

Hewlett-Packard Co.
5201 Tollview Drive
ROLLING MEADOWS, IL 60008
Tel: (312) 255-9800
Telex: 910-687-1066
A,C,CM,E,M

Indiana
Hewlett-Packard Co.
11911 N. Meridian St.
CARMEL, IN 46032
Tel: (317) 844-4100
A,C,CM,E,M

Hewlett-Packard Co.
111 E. Ludwig Road
Suite 108
FT. WAYNE, IN 46825
Tel: (219) 482-4283
C,E

Iowa
Hewlett-Packard Co.
4070 22nd Av. SW
CEDAR RAPIDS, IA 52404
Tel: (319) 390-4250
C,E,M

Hewlett-Packard Co.
4201 Corporate Dr.
WEST DES MOINES, IA 50265
Tel: (515) 224-1435
A**,C,M**

Kansas
Hewlett-Packard Co.
North Rock Business Park
3450 N. Rock Rd.
Suite 300
WICHITA, KS 67226
Tel: (316) 684-8491
C,E

Kentucky
Hewlett-Packard Co.
305 N. Hurstbourne Lane,
Suite 100
LOUISVILLE, KY 40223
Tel: (502) 426-0100
A,C,M

Louisiana
Hewlett-Packard Co.
160 James Drive East
ST. ROSE, LA 70087
P.O. Box 1449
KENNER, LA 70063
Tel: (504) 467-4100
A,C,E,M,P

Maryland
Hewlett-Packard Co.
3701 Koppers Street
BALTIMORE, MD 21227
Tel: (301) 644-5800
Telex: 710-862-1943
A,C,CM,E,M

Hewlett-Packard Co.
2 Choke Cherry Road
ROCKVILLE, MD 20850
Tel: (301) 948-6370
A,C,CM,E,M

Massachusetts
Hewlett-Packard Co.
1775 Minuteman Road
ANDOVER, MA 01810
Tel: (617) 682-1500
A,C,CM,E,M,P*

Hewlett-Packard Co.
29 Burlington Mall Rd
BURLINGTON, MA 01803-4514
Tel: (617) 270-7000
C,E

Michigan
Hewlett-Packard Co.
4326 Cascade Road S.E.
GRAND RAPIDS, MI 49506
Tel: (616) 957-1970
C,M

Hewlett-Packard Co.
39550 Orchard Hill Place Drive
NOVI, MI 48050
Tel: (313) 349-9200
A,C,E,M

Hewlett-Packard Co.
560 Kirts Rd.
Suite 101
TROY, MI 48064
Tel: (313) 362-5180
C

Minnesota
Hewlett-Packard Co.
2025 W. Larpenteur Ave.
ST. PAUL, MN 55113
Tel: (612) 644-1100
A,C,CM,E,M

Missouri
Hewlett-Packard Co.
1001 E. 101st Terrace Suite 120
KANSAS CITY, MO 64131-3368
Tel: (816) 941-0411
A,C,CM,E,M

Hewlett-Packard Co.
13001 Hollenberg Drive
BRIDGETON, MO 63044
Tel: (314) 344-5100
A,C,E,M

Nebraska
Hewlett-Packard
11626 Nicholas St.
OMAHA, NE 68154
Tel: (402) 493-0300
C,E,M

New Jersey
Hewlett-Packard Co.
120 W. Century Road
PARAMUS, NJ 07652
Tel: (201) 265-5000
A,C,CM,E,M

Hewlett-Packard Co.
20 New England Av. West
PISCATAWAY, NJ 08854
Tel: (201) 562-6100
A,C,CM,E

New Mexico
Hewlett-Packard Co.
7801 Jefferson N.E.
ALBUQUERQUE, NM 87109
Tel: (505) 823-6100
C,E,M

Hewlett-Packard Co.
1362-C Trinity Dr.
LOS ALAMOS, NM 87544
Tel: (505) 662-6700
C,E

New York
Hewlett-Packard Co.
5 Computer Drive South
ALBANY, NY 12205
Tel: (518) 458-1550
A,C,E,M

Hewlett-Packard Co.
9600 Main Street
CLARENCE, NY 14031
Tel: (716) 759-8621
C,E,M

Hewlett-Packard Co.
200 Cross Keys Office Park
FAIRPORT, NY 14450
Tel: (716) 223-9950
A,C,CM,E,M

Hewlett-Packard Co.
7641 Henry Clay Blvd.
LIVERPOOL, NY 13088
Tel: (315) 451-1820
A,C,CM,E,M

Hewlett-Packard Co.
No. 1 Pennsylvania Plaza
55th Floor
34th Street & 7th Avenue
MANHATTAN NY 10119
Tel: (212) 971-0800
C,M*

Hewlett-Packard Co.
15 Myers Corner Rd.
Hollowbrook Park, Suite 2D
WAPPINGERS FALLS, NY 12590
Tel: (914) 298-9125
CM,E

Hewlett-Packard Co.
2975 Westchester Ave
PURCHASE, NY 10577
Tel: (914) 935-6300
C,CM,E

Hewlett-Packard Co.
3 Crossways Park West
WOODBURY, NY 11797
Tel: (516) 682-7800
A,C,CM,E,M

North Carolina
Hewlett-Packard Co.
305 Gregson Dr.
CARY, NC 27511
Tel: (919) 467-6600
C,CM,E,M,P*

Hewlett-Packard Co.
9401 Arrow Point Blvd
Suite 100
CHARLOTTE, NC 28217
Tel: (704) 527-8780
C*

Hewlett-Packard Co.
5605 Roanne Way
GREENSBORO, NC 27420
Tel: (919) 852-1800
A,C,CM,E,M,P*

Ohio
Hewlett-Packard Co.
2717 S. Arlington Road
AKRON, OH 44312
Tel: (216) 644-2270
C,E

Hewlett-Packard Co.
4501 Erskine Road
CINCINNATI, OH 45242
Tel: (513) 891-9870
C,M

Hewlett-Packard Co.
15885 Sprague Road
CLEVELAND, OH 44136
Tel: (216) 243-7300
A,C,CM,E,M

Hewlett-Packard Co.
9080 Springboro Pike
MIAMISBURG, OH 45342
Tel: (513) 433-2223
A,C,CM,E*,M

Hewlett-Packard Co.
One Maritime Plaza, 5th Floor
720 Water Street
TOLEDO, OH 43604
Tel: (419) 242-2200
C

Hewlett-Packard Co.
675 Brooksedge Blvd.
WESTERVILLE, OH 43081
Tel: (614) 891-3344
C,CM,E*

Oklahoma
Hewlett-Packard Co.
3525 N.W. 56th St.
Suite C-100
OKLAHOMA CITY, OK 73112
Tel: (405) 946-9499
C,E*,M

SALES & SUPPORT OFFICES

Arranged alphabetically by country

9

UNITED STATES (Cont'd)

Hewlett-Packard Co.
6655 South Lewis,
Suite 105
TULSA, OK 74136
Tel: (918) 481-6700
A**,C,E,M*,P*

Oregon

Hewlett-Packard Co.
9255 S. W. Pioneer Court
WILSONVILLE, OR 97070
Tel: (503) 682-8000
A,C,E*,M

Pennsylvania

Hewlett-Packard Co.
Heatherwood Industrial Park
50 Dorchester Rd.
Route 22
HARRISBURG, PA 17112-2799
Tel: (717) 657-5900
C

Hewlett-Packard Co.
111 Zeta Drive
PITTSBURGH, PA 15238
Tel: (412) 782-0400
A,C,E,M

Hewlett-Packard Co.
2750 Monroe Boulevard
VALLEY FORGE, PA 19482
Tel: (215) 666-9000
A,C,CM,E,M

South Carolina

Hewlett-Packard Co.
Brookside Park, Suite 122
1 Harbison Way
COLUMBIA, SC 29212
Tel: (803) 732-0400
C,M

Hewlett-Packard Co.
545 N. Pleasantburg Dr.
Suite 100
GREENVILLE, SC 29607
Tel: (803) 232-8002
C

Tennessee

Hewlett-Packard Co.
One Energy Centr. Suite 200
Pellissippi Pkwy.
KNOXVILLE, TN 37932
Tel: (615) 966-4747
A,C,E,M,P

Hewlett-Packard Co.
3070 Directors Row
Directors Square
MEMPHIS, TN 38131
Tel: (901) 346-8370
A,C,E,M

Hewlett-Packard Co.
44 Vantage Way,
Suite 160
NASHVILLE, TN 37228
Tel: (615) 255-1271
A,C,E,M,P

Texas

Hewlett-Packard Co.
1826-P Kramer Lane
AUSTIN, TX 78758
Tel: (512) 835-6771
C,E,P*

Hewlett-Packard Co.
5700 Cromo Dr
EL PASO, TX 79912
Tel: (915) 833-4400
C,E*,M**

Hewlett-Packard Co.
3952 Sandshell Drive
FORT WORTH, TX 76137
Tel: (817) 232-9500
C

Hewlett-Packard Co.
10535 Harwin Drive
HOUSTON, TX 77036
Tel: (713) 776-6400
A,C,E,M,P*

Hewlett-Packard Co.
3301 West Royal Lane
IRVING, TX 75063
Tel: (214) 869-3377
C,E

Hewlett-Packard Co.
109 E. Toronto, Suite 100
McALLEN, TX 78501
Tel: (512) 630-3030
C

Hewlett-Packard Co.
930 E. Campbell Rd.
RICHARDSON, TX 75081
Tel: (214) 231-6101
A,C,CM,E,M,P*

Hewlett-Packard Co.
1020 Central Parkway South
SAN ANTONIO, TX 78232
Tel: (512) 494-9336
A,C,E,M,P*

Utah

Hewlett-Packard Co.
3530 W. 2100 South St.
SALT LAKE CITY, UT 84119
Tel: (801) 974-1700
A,C,E,M

Virginia

Hewlett-Packard Co.
840 Greenbrier Circle
Suite 101
CHESAPEAKE, VA 23320
Tel: (804) 424-7105
C,E,M

Hewlett-Packard Co.
4305 Cox Road
GLEN ALLEN, VA 23060
Tel: (804) 747-7750
A,C,E,M,P*

Hewlett-Packard Co.
Tanglewood West Bldg.
Suite 240
3959 Electric Road
ROANOKE, VA 24018
Tel: (703) 774-3444
C,E,P

Washington

Hewlett-Packard Co.
15815 S.E. 37th Street
BELLEVUE, WA 98006
Tel: (206) 643-4004
A,C,CM,E,M

Hewlett-Packard Co.
1225 Argonne Rd
SPOKANE, WA 99212
Tel: (509) 922-7000
C

West Virginia

Hewlett-Packard Co.
501 56th Street
CHARLESTON, WV 25304
Tel: (304) 925-0492
A,C,M

Wisconsin

Hewlett-Packard Co.
275 N. Corporate Dr.
BROOKFIELD, WI 53005
Tel: (414) 784-8800
A,C,E*,M

URUGUAY

Pablo Ferrando S.A.C. e. l.
Avenida Italia 2877
Casilla de Correo 370
MONTEVIDEO
Tel: 59-82-802-586
Telex: 398802586
A,CM,E,M

Olympia de Uruguay S.A.
Maquinas de Oficina
Avda. del Libertador 1997
Casilla de Correos 6644
MONTEVIDEO
Tel: 91-1809, 98-3807
Telex: 6342 OROU UY
P

VENEZUELA

Hewlett-Packard de Venezuela C.A.
3A Transversal Los Ruices Norte
Edificio Segre 2 & 3
Apartado 50933
CARACAS 1050
Tel: (582) 239-4133
Telex: 251046 HEWPACK
A,C,CM,E,M,P

Hewlett-Packard de Venezuela, C.A.
Centro Ciudad Comercial Tamanaco
Nivel C-2 (Nueva Etapa)
Local 53H05
Chuo, **CARACAS**
Tel: 928291
P

Albis Venezolana S.R.L.
Av. Las Marias, Ota. Alix,
El Pedregal
Apartado 81025
CARACAS 1080A
Tel: 747984, 742146
Telex: 24009 ALBIS VC
A

Tecnologica Medica del Caribe, C.A.
Multicentro Empresarial del Este
Ave. Libertador
Edif. Libertador
Nucleo "C" - Oficina 51-52
CARACAS
Tel: 339867/333780
M

Hewlett-Packard de Venezuela C.A.
Residencias Tia Betty Local 1
Avenida 3 y con Calle 75
MARACAIBO, Estado Zulia
Apartado 2646
Tel: 58-2-617-5669
Telex: 62464 HPMAR
C,E*

Hewlett-Packard de Venezuela C.A.
Urb. Lomas de Este
Torre Trebol - Piso 11
VALENCIA, Estado Carabobo
Apartado 3347
Tel: (5841) 222992
C,P

YUGOSLAVIA

Do Hermes
General Zdanova 4
YU-11000 BEOGRAD
Tel: (011) 342 641
Telex: 11433
A,C,E,M,P

Do Hermes
Celovska 73
YU-61000 LJUBLJANA
Tel: (061) 553 170
Telex: 31583
A,C,E,M,P

Elektrotehna
Titova 51
YU-61000 LJUBLJANA
CM

Do Hermes
Kralja Tomislava 1
YU-71000 SARAJEVO
Tel: (071) 35 859
Telex: 41634
C**,P

ZAIRE

Computer & Industrial Engineering
25, Avenue de la Justice
B.P. 12797
KINSHASA, Gombe
Tel: 32063
Telex: 21552
C,P

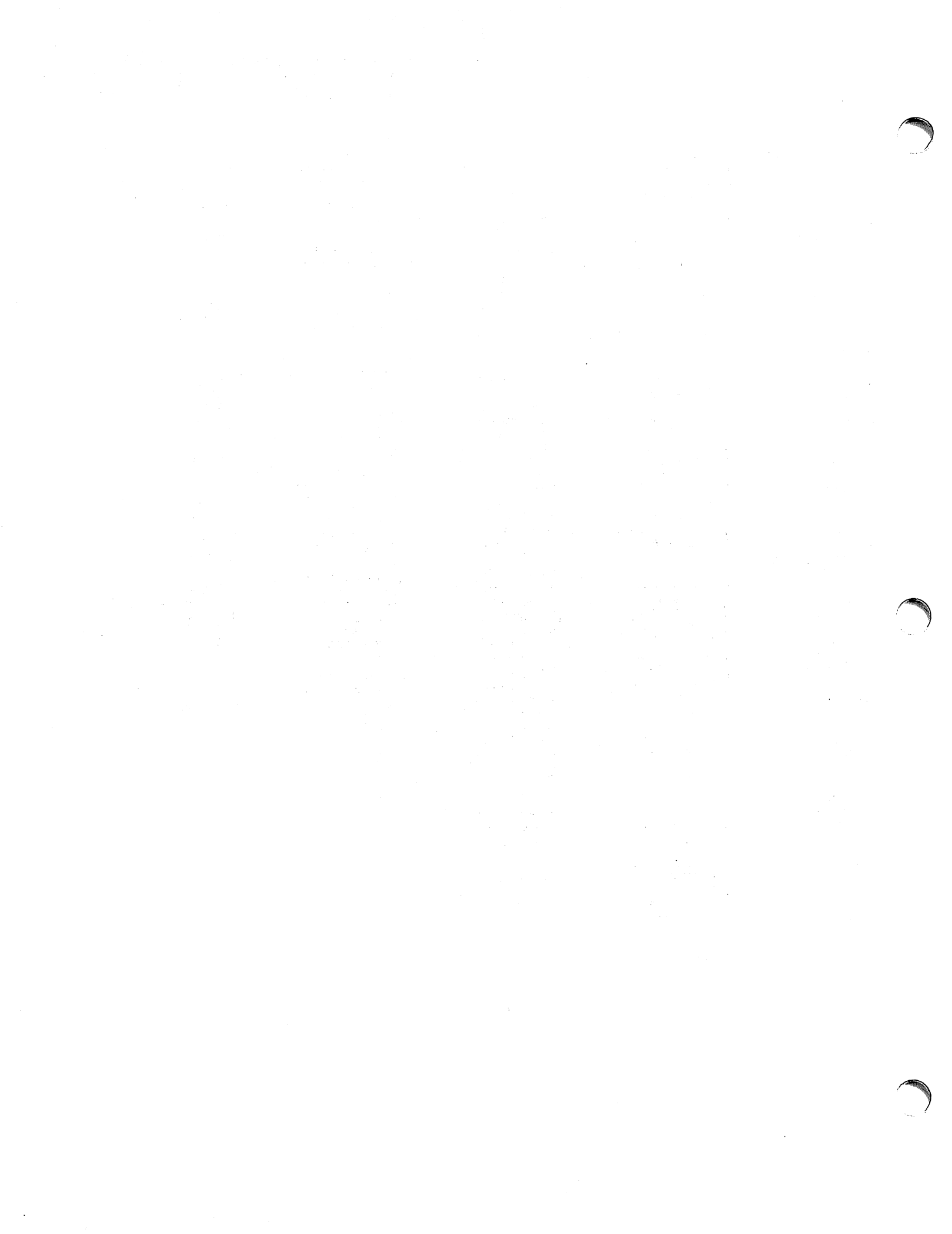
ZAMBIA

R.J. Tilbury (Zambia) Ltd.
P.O. Box 32792
LUSAKA
Tel: 215590
Telex: 40128
E

ZIMBABWE

Field Technical Sales (Private) Limited
45, Kelvin Road North
P.O. Box 3458
SALISBURY
Tel: 705 231
Telex: 4-122 RH
E,P

September 1987



Part No. 32344-90002
Printed in U.S.A. 05/87
E0587

