NS 3000/iX NMMGR Screens Reference Manual

HP 3000 MPE/iX Computer Systems

Edition 8

HEWLETT® PACKARD

36922-90038

E1098

Printed in: U.S.A. October 1998

Notice

Restricted Rights Legend

Acknowledgments

UNIX is a registered trademark of The Open Group.

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304 U.S.A.

Contents

Contents

Figures

Figures

Tables

Preface

This manual documents functionality for the MPE/iX 6.0 release, as well as later releases for HP 3000 Series 900 systems.

This reference manual assumes that you are familiar with your network topology.

NMMGR is an interface used to configure Local Area Networks (LANs), point-to-point (router) networks, token ring networks, FDDI, 100VG-AnyLAN, 100Base-T, and X.25 networks. The NMMGR screens described in this manual are accompanied by parameter descriptions that give you ideas on which values are appropriate for your network. Ultimately it is up to you to decide which values to supply depending on how the network is used and maintained.

Special Note

MPE/iX, Multiprogramming Executive with Integrated POSIX, is the latest in a series of forward-compatible operating systems for the HP 3000 line of computers.

In HP documentation and in talking with HP 3000 users, you will encounter references to MPE XL, the direct predecessor of MPE/iX. MPE/iX is a superset of MPE XL. All programs written for MPE XL will run without change under MPE/iX. You can continue to use MPE XL system documentation, although it may not refer to features added to the operating system to support POSIX (for example, hierarchical directories).

Finally, you may encounter references to MPE V, which is the operating system for HP 3000s, not based on the PA-RISC architecture. MPE V software can be run on the PA-RISC HP 3000s (Series 900) in what is known as *compatibility mode*.

Helpful Manuals

This manual is intended as a reference for those who need detailed information about NS 3000/iX configuration screens and their fields. Not all parts of the NMMGR screens set are described in this manual. The following paragraphs describe where to find information about other aspects of NMMGR and network configuration.

The planning you should do before attempting to configure a network is discussed in the *HP 3000/iX Network Planning and Configuration Guide*.

An introduction to the generic use of the NMMGR utility, including discussions of the first levels of selection menus and of the utility screen branch, can be found in *Using the Node Management Services (NMS) Utilities*.

The NMMGR screens that are associated with configuring the terminal, printer, and other serial device connections made through the Datacommunications and Terminal Controller (DTC) are described in *Configuring Systems for Terminals, Printers, and Other Serial Devices*.

Related Publications

- *HP 3000/iX Network Planning and Configuration Guide* provides information for planning your network and also provides step-by-step instructions for using guided configuration to configure network links.

Additional manuals that may be of interest when working with the NS 3000/iX network services and link products are listed here:

- *Using the Node Management Services (NMS) Utilities*
- *NS 3000/iX Operations and Maintenance Reference Manual*
- *NS 3000/iX Error Messages Reference Manual*
- *Using NS 3000/iX Network Services*
- *NetIPC 3000/XL Programmer's Reference Manual*

1 Overview

NS 3000/iX network subsystems on HP 3000 Series 900 computers are configured using a utility called the node management configuration manager (NMMGR). NMMGR uses a series of VPLUS screens to display and accept configuration data. Configuration data is stored in a hierarchically structured file, of file type NCONF, called `NMCONFIG.PUB.SYS`. The network services, network transport, data communications configurator, and logging services use `NMCONFIG.PUB.SYS` to get the information they need to operate.

NMMGR may be used to configure the network in two ways.

- **Guided Configuration** directs you through an established sequence of configuration screens for the type of network you are configuring. In general, you should always use Guided Configuration to establish your initial network configuration and in most cases for network maintenance and updating.
- **Unguided Configuration** (manual configuration) allows a more random type of access to NMMGR screens. Unguided configuration is more appropriate when examining or modifying the fields of a single screen or of a few specific screens.

These two methods are not mutually exclusive; they may, with some restrictions, be used in conjunction with one another during configuration. Refer to Chapter 2, “Introductory Screens,” (Figure 2-1) for the screen flow of the introductory screens for guided and unguided configurations.

Using The Command Window

The command window at the top of each NMMGR screen is used to enter NMMGR or MPE commands. The command window is the third line from the top of an NMMGR screen and has **`Command:`** on the left-hand side.

You type a command in the command window and execute it by pressing the **[Enter]** key. The **[Enter]** key is the block mode enter key, different from the carriage return key. The **[Enter]** key is usually marked **ENTER** and the carriage return key is usually marked **RETURN**.

For more information about the command window, refer to *Using the Node Management Services (NMS) Utilities*.

Using The Path Name

The **path name** is used to go directly to a given screen. A path name may include one or more of the following variables:

- *NIname* is the name of the network interface you want to modify.
- *linkname* is the name of the link you want to modify.
- *gatewayn* is the name of the gateway you want to modify.
- *mapentry* is the name of the entry you want to modify in the router mapping table.
- *fsetname* is the name of the X.25 facility set you want to modify.

The path name is specified with each screen in this manual. To use a path name to go directly to a screen, type the path name preceded by an "@" in the command window and press the **[Enter]** key. For example, to go directly to the screen that contains the parameters for the X.25 facility set called "MySet" for the NI called "MyX25NI," you would type the following: `@NETXPORT.NI.MyX25NI.PROTOCOL.X25.FACSET.MySet`

Getting Help

Help is available for all the NMMGR screens described in this manual. It is also available for the screens used to configure the distributed terminal subsystem and those used for guided configuration.

There are two ways to access NMMGR help:

- The simplest way to use the help facility is to press the **[Help]** function key while at the screen for which you need information. You will immediately be presented with text that describes the screen, each parameter configured using the screen, and the operation associated with each of the screen's function keys.
- You can also access the NMMGR help system by entering a **?** at the command line. You are presented with a list of available help topics. One of these topics, Index, provides a list of parameters and the screens on which they are configured. Path branching information is included where appropriate.

Help messages are provided as an aid to configuration and are not intended to be a complete reference. They provide only the information that is immediately needed to understand how to use a screen. If you need more detailed information than is provided by a help message, refer to this manual or, if you are using guided configuration, to the *HP 3000/iX Network Planning and Configuration Guide*.

Using This Manual

This manual is organized so that you can find information on specific screens in any of the following ways:

- If you know the name of the screen you need information about, you can refer to the index for an alphabetical listing of screens by name.
- Screens are arranged in this manual by screen type. If you know both the screen's name and its type you can locate screens easily using the Table of Contents.
- You may refer to configuration path maximums at the end of this Chapter to locate information on individual software maximums when configuring a supported link.
- In many cases, you can use the index to locate information on individual configuration parameters. This can be especially helpful if you need to identify the specific screen that contains a value that you want to modify.

Screen Numbers

Each NMMGR configuration screen has a screen number associated with it. These numbers are located immediately to the left of each screen's title.

Screen numbers are strictly for convenience in referencing information about each screen.

You can also use screen numbers to locate information about other NMMGR configuration screens in the relevant manuals.

NOTE There is no significance to the order of the numbers assigned to the various configuration screens. The numbers are provided strictly as a reference aid for individual screens and have no relationship to each other.

Software Configuration Maximums (MPE/iX 6.0)

The following are the software maximums in Table 1-1 that must be adhered to when configuring a supported link. These maximums may be further limited by the system hardware (number of available slots). Maximums are also documented throughout the manual for the appropriate screen.

Table 1-1 Configuration Maximums

Screen Number/Description	Path	Maximum Limit
#9 Network Directory Select Node Name	None	File Size Limit[a]
#85 Link Selection	LINK	256/system
#112 Network Interface Configuration	NETXPORT.NI	12 NI/system[b]
#115 Point-to-Point Mapping Configuration	NETXPORT.NI.*NIname*.MAPPING	1024 Mappings/Router
#117 Gateway Half NI Links	NETXPORT.NI.*NIname*.LINK	1 link/Gateway Half NI
#119 Point-to-Point NI Links	NETXPORT.NI.*NIname*.	40 links/Router NI
#151 X.25 Network Interface Links	NETXPORT.NI.*NIname*.LINK	12 links/X.25 NI
#152 Neighbor Gateways	NETXPORT.NI.*NIname*.INTERNET	14 gateways/NI
#158 Neighbor Gateway Reachable Networks	NETXPORT.NI.*NIname*.INTERNET.gatewayn	2550 nets/NI[c]
#162 X.25 SVC Address Key Paths	NETXPORT.*NIname*.PROTOCOL.X25.SVCPATH	2048/X.25 NI
#163 X.25 PVC Address Key Paths	NETXPORT.*NIname*.PROTOCOL.X.25.PVCPATH	128/X.25NI
#164 X.25 User Facility Sets	NETXPORT.NI.*NIname*.POROTOCOL.X25.FACSET	128/X.25 NI

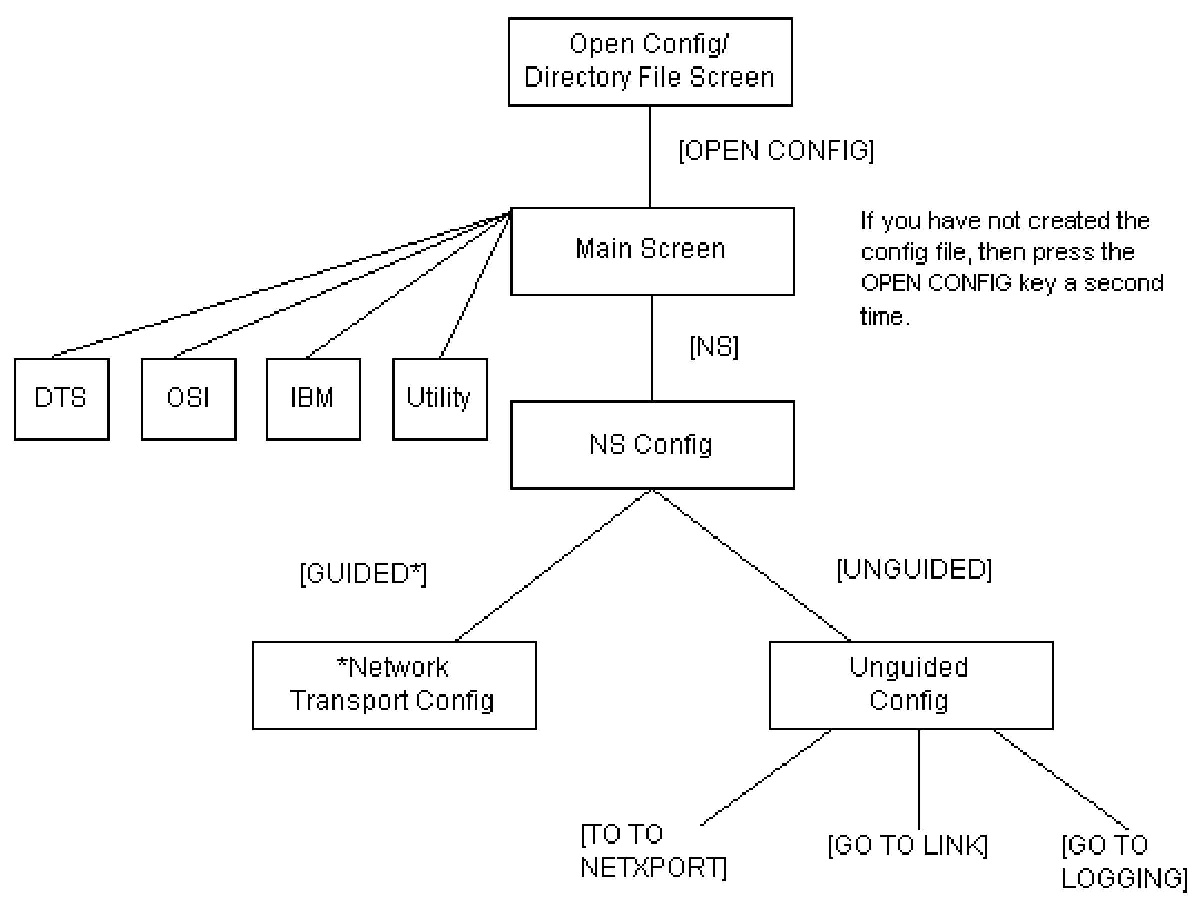
a. Maintenance Node command **EXPANDDIR** may be used to expand the directory file. Refer to *Using the Node Management Services (NMS) Utilities* manual for information regarding this command.
b. One NI must be used for loopback.
c. 2,550 reachable networks (255 pages and 10 reachable nets per page).

2 Introductory Screens

The introductory screens are the first few screens that are displayed when you configure a node using NMMGR.

Figure 2-1 shows the screen flow of the introductory screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow. This Chapter describes the introductory screens relevant to configuring NS using unguided configurations.

Figure 2-1 NMMGR Screen Flow

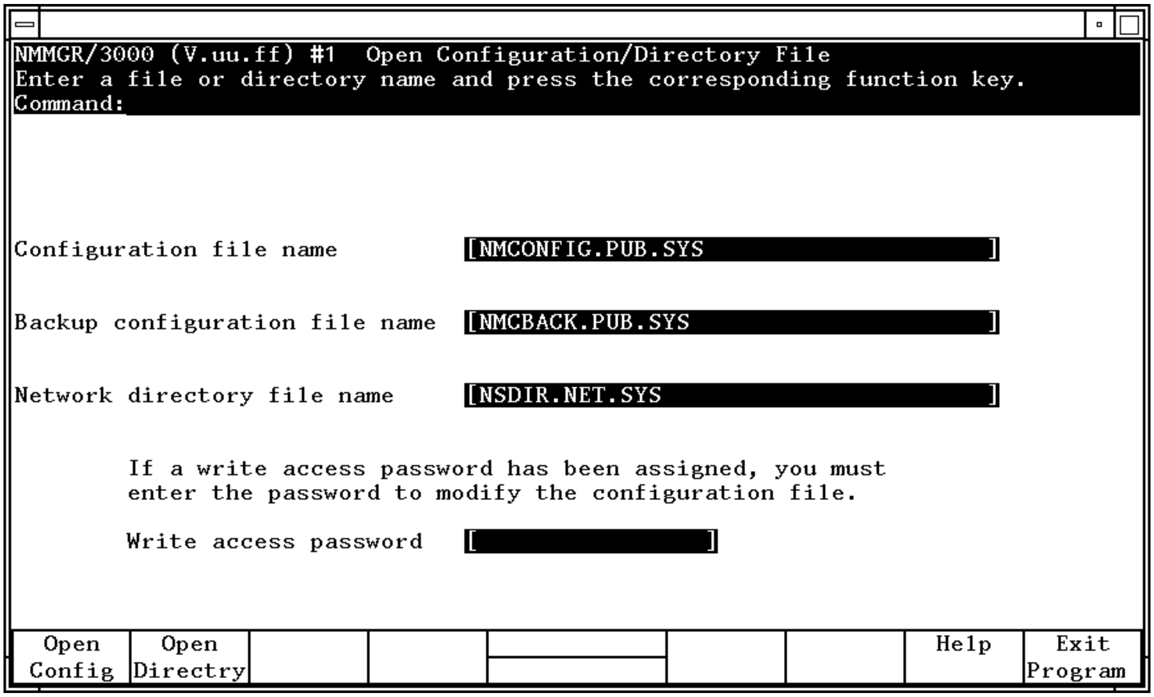


*For information specific to the Guided Configuration screens, refer to the *HP 3000/iX Network Planning and Configuration Guide.*

Open Configuration Directory File

The Open Configuration/Directory File screen (#1) shown in Figure 2-2 is the first screen displayed when you run NMMGR.

Figure 2-2 Open Configuration/Directory Screen



To create or modify a configuration, enter the configuration file name and press the **[Open Config]** key. If the configuration file does not already exist, NMMGR will ask you to press the **[Open Config]** key again to confirm creation. Upon pressing the **[Open Config]** key the Main screen (#2) will appear as shown in Figure 2-3.

To change the default backup file name, enter a new name in the backup configuration file name field before you open the configuration file.

To create or modify a network directory, enter the network directory file name and press the **[Open Directry]** key. If the directory file does not already exist, NMMGR will ask you to press the **[Open Directry]** key again to confirm creation. Upon pressing the **[Open Directory]** key, the Network Directory Main screen (#8) will appear as shown in Chapter 15, “Network Directory,” (Figure 15-3).

If a write access password has been assigned, you must enter the password in the write access password field before you will be able to open a configuration or directory file for write access or to create a new configuration or directory file. To open a file in read only mode if a write access password has been assigned, leave this field blank.

NOTE The write access password is optional. If you do not choose to assign a password, you will be able to update the configuration file at any time it is opened. For information on how to assign a write access password, refer to the information about the **password** maintenance mode command in *Using the Node Management Services (NMS) Utilities*.

Fields

`configuration file name` The only valid configuration file name the system recognizes for use by the network subsystems is `NMCONFIG.PUB.SYS`. You can, however, create or modify a configuration file using a different name and save it as an **offline configuration file**. You can use offline configuration files as a means of creating and storing configurations that you want to use in the future. When you are ready to use an offline configuration file, simply rename it as `NMCONFIG.PUB.SYS` and reboot the system. (Keep in mind that any file you use as a configuration file must be successfully validated before you try to use it.)

`Backup configuration file` A backup file name must be specified whenever a configuration file is opened or created. The default backup configuration file name is `NMCBACK.group.account`. The backup file will be automatically updated with the contents of the configuration file each time the configuration is successfully validated.

`Network directory file name` The name of the network directory file you want to create or update. The network directory uses a KSAM file pair, therefore two files are actually created for each network directory. The only file name the system recognizes as a network directory data file is `NSDIR.NET.SYS`. The only file name the system recognizes as a network directory key file is `NSDIRK.NET.SYS`. (`NSDIRK.NET.SYS` is generated automatically when `NSDIR.NET.SYS` is created.)

You can create **offline directories** in the same way that you can create offline configuration files, by using a different file name when you create and save network directory information. When you are ready to use the offline directory, you must be sure to rename both the data file and the key file to the system-recognized names.

Network directory screens are discussed in Chapter 15, “Network Directory,” of this manual.

`Write access password` The password is an optional feature. If a password has been assigned, you must enter the password in the write access password field in order to update the configuration file. It is still possible to open the file without using an assigned password, but the file will be in read only mode and NMMGR will accept no changes to the file.

If no password has been assigned, you should ignore the write access password field.

If you want to assign a password for the system you are configuring, refer to *Using the Node Management Services (NMS) Utilities*.

Main

If you create or modify a configuration file and press the **[Open Config]** key from the Open Configuration/Directory File, the Main screen (#2) shown in Figure 2-3 appears.

Figure 2-3 Main Screen

```
NMMGR/3000 (V.uu.ff) #2  Main                                    Data: Y
Type in the node name and press Save Data; then press the desired function key.
 Command:

Local HP 3000 node name [ALPHA.DOMAIN.ORG                                    ]

                             (node.domaNn.organization)
Are you using OpenView DTC Manager?  [ ] (Y/N)
                                                           Y
Do you have X.25 system-to-system or PAD connections?  [ ] (Y/N)

DTS        - Configuration of DTC device connections, links, & profiles.

NS         - Configuration of ARPA Network:  Logging, LAN (802.3/Ethernet),
             NS/Token Ring (802.5), X.25 (WAN), Point-to-Point, NS/SNA, FDDI
             100VGLAN, 100BT.

OSI        - Configuration of OSI network:
             OSI Transport & Session (OTS) and OSI FTAM services.

IBM        - Configuration of the IBM network:
             Logging, SNA node, NRJE, RJE, IMF, DHCF, APPC, & SNADS.

  DTS    |   NS    |  OSI    |  IBM    |         |Utility |  Save   |  Help   | Prior
         |         |         |         |         |        |  Data   |         | Screen
```

At the Main screen you configure the local node name of the HP 3000 host system. Before you can proceed beyond the Main configuration screen you will need to enter a valid local node name, answer the questions asked on the screen, and press the **[Save Data]** key.

NOTE

NS/SNA is no longer offered as a product and has been removed from the Corporate Price List. The product is obsolete with no plans for support.

Fields

`local node name`

The local node name is the name by which the HP 3000 Series 900 machine is known in the network. The format of a node name is `name.domain.organization` where the total number of characters is 50 or fewer, and each field contains 16 or fewer 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. The *name.domain* portion of each node name must be unique within the internetwork. HP recommends that all nodes on the same network be assigned the same domain and organization.

Assign meaningful node names. For example, `MKTG.IND.HP` and `LAB.IND.HP` are meaningful names for two nodes on the same Local Area Network within Hewlett-Packard. One node (`MKTG.IND.HP`) is used by the marketing department. The other node (`LAB.IND.HP`) is used by the lab. The *domain* field is the same because the nodes belong to the same network. The *organization* field is the same because the nodes belong to the same internetwork. Refer to the *HP 3000/iX Network Planning and Configuration Guide* for more information about node names.

NOTE Even if you are planning to use only domain names for network access, you will still need to configure the local node name on this screen. The datacommmunications and terminal subsystem (DTS) requires the local node name for communications between the host and its Datacommunications and Terminal Controllers (DTCs).

The Main screen also requires you to specify whether or not you are using OpenView DTC Manager and whether or not you will be configuring X.25 system-to-system or PAD connections. The answers you provide to these questions determine the set of screens that you will be taken through when you configure terminal, printer, and other serial device connections through DTS. If you are configuring an ARPA network connection, you will already have answered these questions. Refer to *Configuring Systems for Terminals, Printers, and Other Serial Devices* for more information on how to answer these questions.

Once you have entered the local node name and answered the two questions on this screen, press the **[Save Data]** key to save the node name information in the configuration file. You can then proceed to one of the various NMMGR configuration subbranches referenced on the next page.

NMMGR Configuration Subbranches

To select one of the NMMGR configuration subbranches (DTS, NS, OSI, IBM and Utility), press the appropriate function key.

To configure Datacommunications and Terminal Controllers (DTCs) and the devices attached to them, press the **[DTS]** function key and refer to *Configuring Systems for Terminals, Printers, and Other Serial Devices*.

To configure an ARPA network using guided configuration screens (recommended), press the **[NS]** key and refer to the *HP 3000/iX Network Planning and Configuration Guide*.

To configure an ARPA network using unguided configuration screens, press the **[NS]** key and continue on in this manual.

To configure OSI, press the **[OSI]** function key and refer to *Installing, Configuring, and Starting OSI/iX*.

To configure an HP-to-IBM link, press the **[IBM]** function key and refer to the *SNA LINK/iX Node Manager's Guide*.

To use NMMGR utilities to copy, compress, validate, or print a configuration, press the **[Utility]** function key and refer to *Using the Network Management Services (NMS) Utilities*.

NS Configuration

If you press the **[NS]** function key from the Main screen, the NS Configuration screen (#166) shown in Figure 2-4 appears. You have a choice of selecting guided or unguided configurations.

Figure 2-4 NS Configuration Screen

```
NMMGR/3000 (V.uu.ff) #166  NS Configuration                      Data: Y
Select the next screen and press the corresponding function key.
 Command:

Guided     - Use this function to define or modify your network, network
Config       directory, or logging configuration.

Unguided   - You only need to use unguided (manual) configuration if you
Config       need to modify default network performance parameters not
             accessible through guided configuration.

Local domain name:  If your network uses domain names, enter the domain name
in the field below and press the Save Data key before selecting the guided
or unguided option.  Otherwise, leave the local node name in this field.

[ALPHA.ARPA.DOM.COM                                                 ]
[                                                                   ]
[                                                                   ]
[                                                                   ]


File:  NMCONFIG.PUB.SYS
 Guided  Unguided                               Save    Help   Prior
 Config   Config                                Data           Screen
```

Guided/Unguided Configuration

Use the function keys on this screen to select the guided or the unguided configuration branch for NS configuration. If you are using domain names for network access, enter the domain name for the system you are configuring in the local domain name field in place of the local node name. (If you are not using domain names, leave the local node name as is.)

If you are entering a domain name, press the **[Save Data]** key to save the domain name in the configuration file before continuing.

Hewlett-Packard recommends that you press the **[Guided Config]** key to select the guided configuration branch whenever you need to initially configure a network interface. Guided configuration supplies many default values for your configuration and requires that you visit a minimal number of screens. To use the guided configuration screens, refer to the *HP 3000/iX Network Planning and Configuration Guide*.

If you need to modify configuration values that are not available on the guided screens, press the **[Unguided Config]** key to select the unguided configuration branch. This manual provides information on every screen available to you through unguided NS configuration.

Fields

`Local domain name`

If you are not using domain names for network access, leave the local node name in this field.

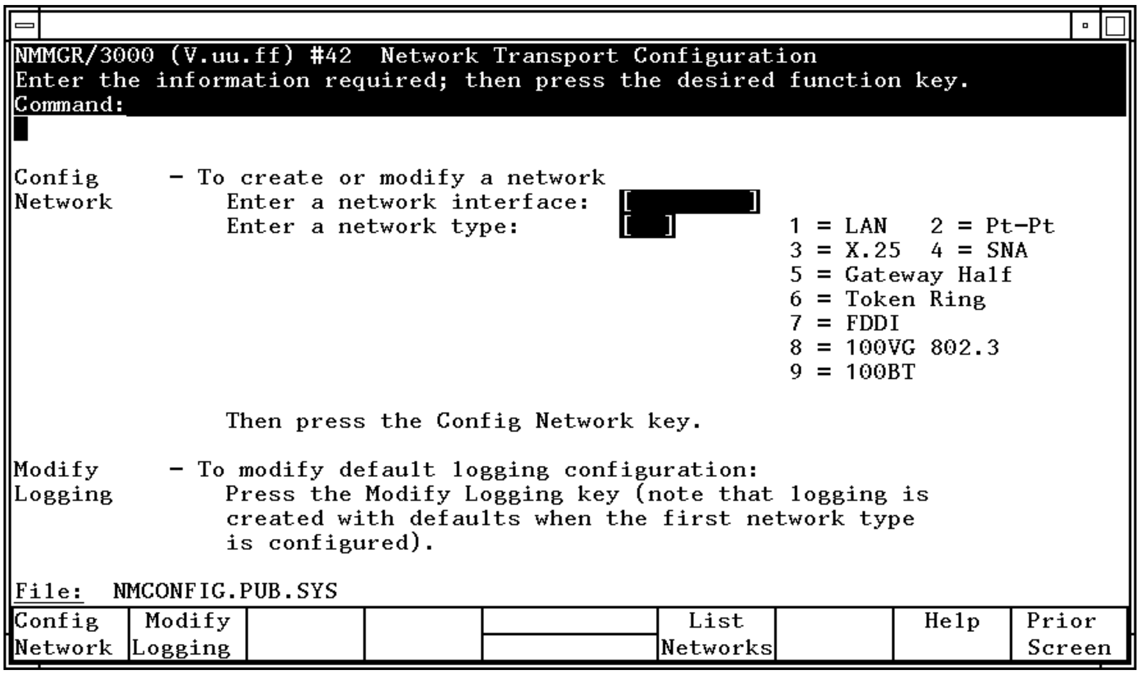
If you are using domain names, enter the name of this system in the ARPANET standard format. This name can be used by other nodes on the network to access this host.

The domain name is composed of labels, with each label separated by a period. Each label must start with a letter or digit and have as interior characters only letters, digits, hyphens (-) or underbars (_). A domain name may have any number of labels but its total length, including periods, is limited to 255 characters. Domain names are not case sensitive.

Network Transport Configuration

If you press the **[Guided Config]** function key from the NS Configuration screen, the Network Transport Configuration screen (#42) shown in Figure 2-5 appears. This is the first guided configuration screen. For information specific to the guided configuration screens (including the screen shown here), refer to the *HP 3000/iX Network Planning and Configuration Guide*.

Figure 2-5 Network Transport Configuration Screen



Guided configuration is an NMMGR procedure that automates configuration. It assumes and supplies default values wherever possible to furnish most of the configuration file's data.

When you run guided configuration, you visit only a minimal number of configuration screens. A number of these screens are different from those you would see during unguided configuration.

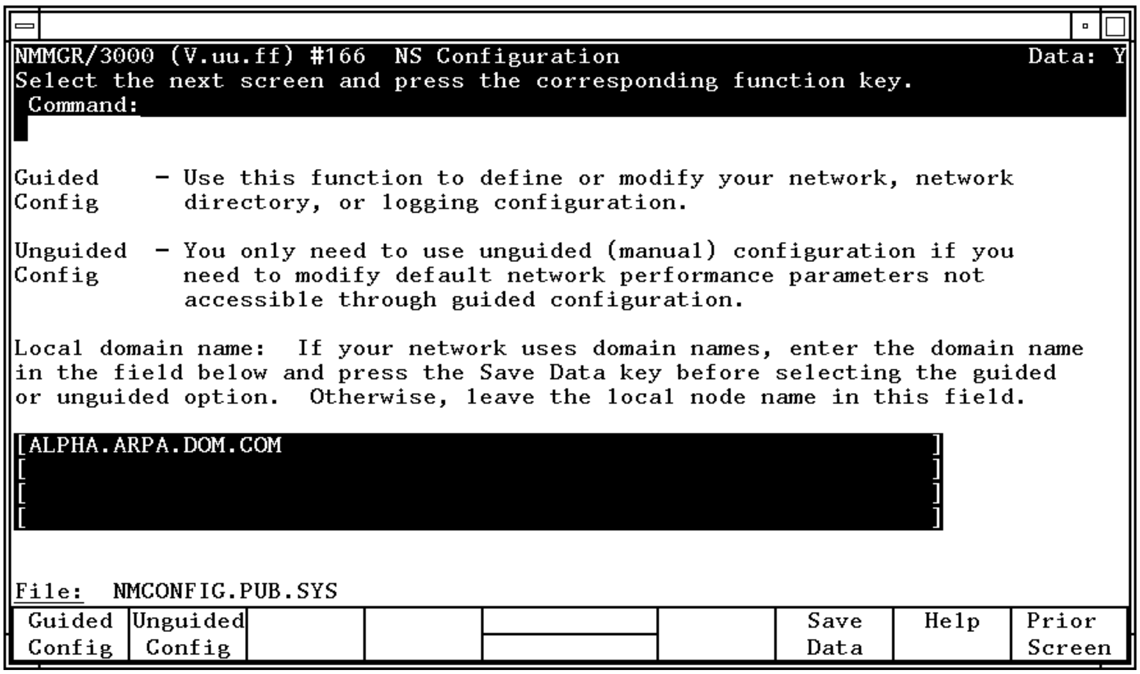
NOTE

HP strongly recommends that you use guided configuration to configure each node initially. You can also take advantage of its convenience later 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.

Unguided Configuration

If you press the **[Unguided Configuration]** function key from NS Configuration screen (#166), the Unguided Configuration screen (#80) shown in Figure 2-6 appears.

Figure 2-6 Unguided Configuration



To configure or update a link, press the **[Go To LINK]** function key and refer to Chapter 3, “Link Configuration Screens,” in this manual.

To configure or update screens that are common to all network interfaces, press the **[Go To NETXPORT]** function key and refer to Chapter 4, “Network Transport Configuration Screens,” in this manual.

To configure or update logging, press the **[Go To LOGGING]** function key and refer to Chapter 14, “Logging Configuration Screens,” in this manual.

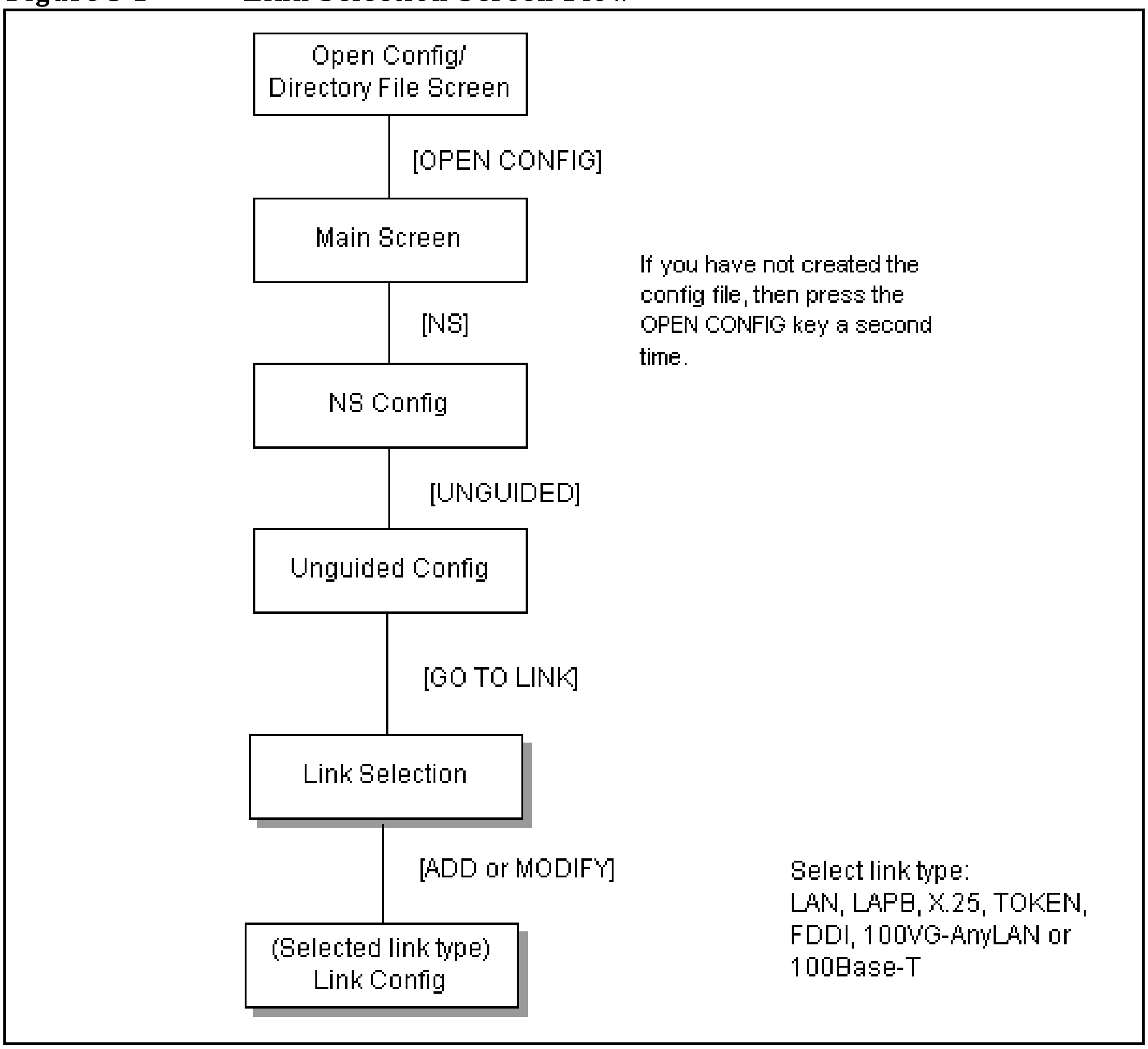
3 Link Configuration Screens

Link configuration screens are used to define a link from the HP 3000 to a network. The first screen, Link Selection, allows you to define a link of type LAN, LAP-B (point-to-point), X.25, TOKEN, FDDI, 100VG-AnyLAN, or 100Base-T. A screen is then displayed that allows you to configure operating parameters for the link type that you select.

The links defined and configured in these screens must match the links defined later when configuring the network interface (path name `NETXPORT.NI.`*`NIname`*`.LINK`) in the following chapters.

Figure 3-1 shows the screen flow of the link selection screens. Screens unique to the link selection are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 3-1 Link Selection Screen Flow



Link Selection

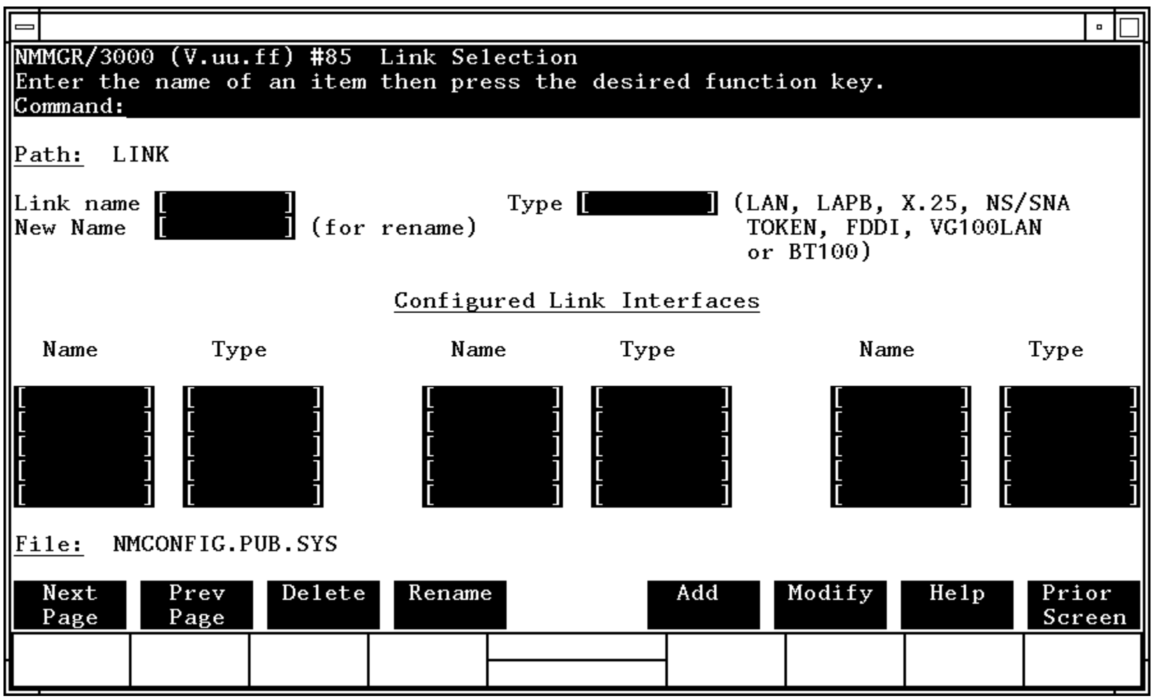
The Link Selection screen (#85) in Figure 3-2 is displayed when you press the **[Go To LINK]** function key at the Unguided Configuration screen (#80). It is also displayed when you type the path name:

```
@LINK
```

in the command window of any screen and press the **[Enter]** key.

NOTE Fields described as **"HP modifiable"** should be changed only upon the recommendation of your HP representative.

Figure 3-2 Link Selection Screen



NOTE NS/SNA is no longer offered as a product and has been removed from the Corporate Price List. The product is obsolete with no plans for support.

Use the fields and the function keys of the select screen to perform the desired action as follows:

- To define a new link configuration, specify the link name and the type; then press the **[Add]** function key. 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 *linkname*; then press the **[Modify]** function key. The data screen that contains information 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 the **[Rename]** function key. The previously configured link name is replaced and the screen displays the new name in the display fields labeled Configured Link Interfaces.
- To delete an existing link configuration, specify the link name, then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured link name and associated data is deleted and is no longer displayed in the display fields labeled Configured Link Interfaces.

Fields

`Link name` Enter the link name for either a LAN, LAP-B, X.25, NS/SNA, Token Ring, FDDI, 100VG-AnyLAN, or 100Base-T.

The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic. This name must match the link name configured in the corresponding `NETXPORT.NI.`*`NIname`*`.LINK screen`.

`Types` **(Required only when adding a link.)** Enter the type shown on the screen that corresponds to your link.

- Choose `LAN` if you are using a ThinLAN, ThickLAN, or Ethertwist link. Refer to LAN Link Configuration.
- Choose `LAPB` if you are using a point-to-point (router) Link. Refer to Link Configuration: LAP-B Link Data.
- Choose `X.25` if you are using an X.25 link. Refer to X.25 Link Configuration.
- Choose `TOKEN` if you are using a token ring link. Refer to Token Ring Link Configuration.
- Choose `FDDI` if you are using an FDDI link. Refer to FDDI Link Configuration.
- Choose `100VG-AnyLAN` if you are using an 100VG-AnyLAN link. Refer to 100VG-AnyLAN Link Configuration.
- Choose `100Base-T` if you are using an 100Base-T link. Refer to 100Base-T Link Configuration.

NS/SNA is no longer offered as a product.

`New name` **(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. The link name must match the link name configured in the corresponding `NETXPORT.NI.`*`NIname`*`.LINK` screen.

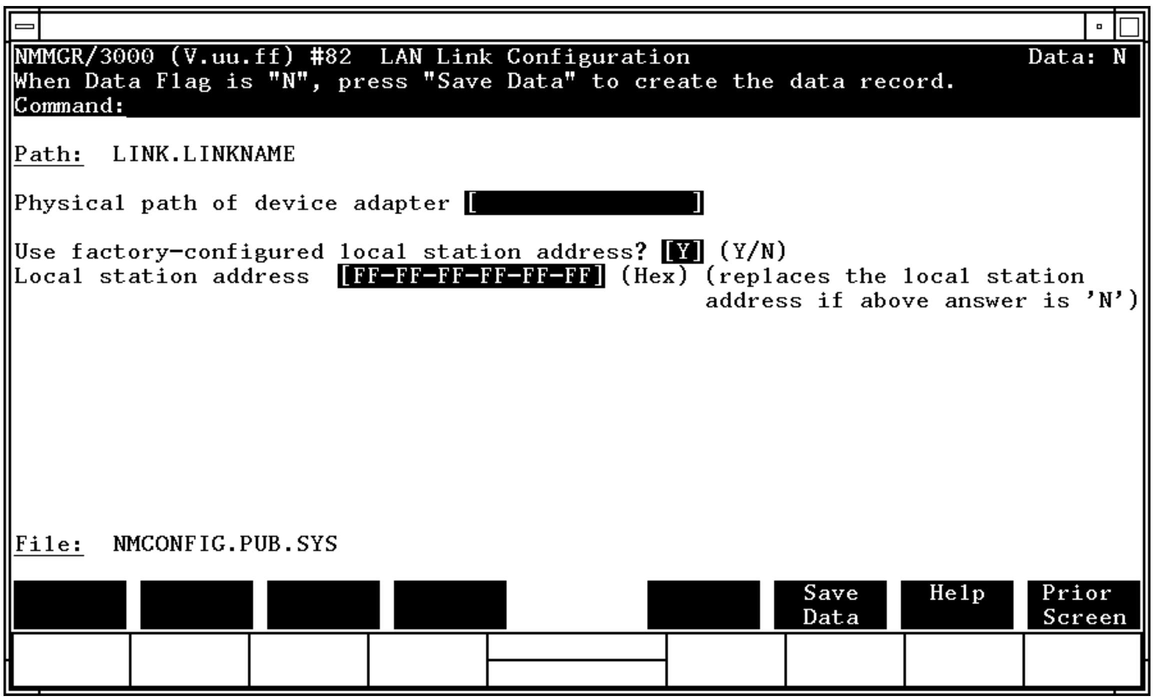
LAN Link Configuration

The LAN Link Configuration screen (#82) in Figure 3-3 is displayed when you select a link name of type LAN at the Link Selection screen (Figure 3-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@LINK.`*`linkname`*

in the command window of any screen and press the **[Enter]** key, where *linkname* is the name of a configured LAN link.

Figure 3-3 LAN Link Configuration Screen



Press the [**Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Physical path of device adapter` The physical path number corresponds to the slot location of the node's local area network interface controller (LANIC) card. For HP 3000 systems, the path is derived by a basic formula of *4 x slot number*. (Example: 4 x 10 = 40, where the LANIC card is installed in slot number 10 and the physical path of the card is 40.)

For some HP systems, you must specify a channel number (`ccc`) and subchannel number (`sss`) in the form ccc.sss while others require a bus converter number followed by a slash (/) and then a channel number (`ccc`) and subchannel number (`sss`) in the form `b/ccc.sss`.

If you are unsure of the slot location or of the physical path number to configure for your system, see your system documentation or consult your Hewlett-Packard service representative.

`Use factory-configured local station 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 Hewlett-Packard representative.

Default value: `Y`

`Local station address`

(modifiable.) This field is to be used only with specific instructions from your Hewlett-Packard representative. It allows you to enter a station address to replace the factory configured address. The format must be compatible with HP software requirements. Your Hewlett-Packard representative will supply instructions in the unlikely event that you need to enter an address to replace the default.

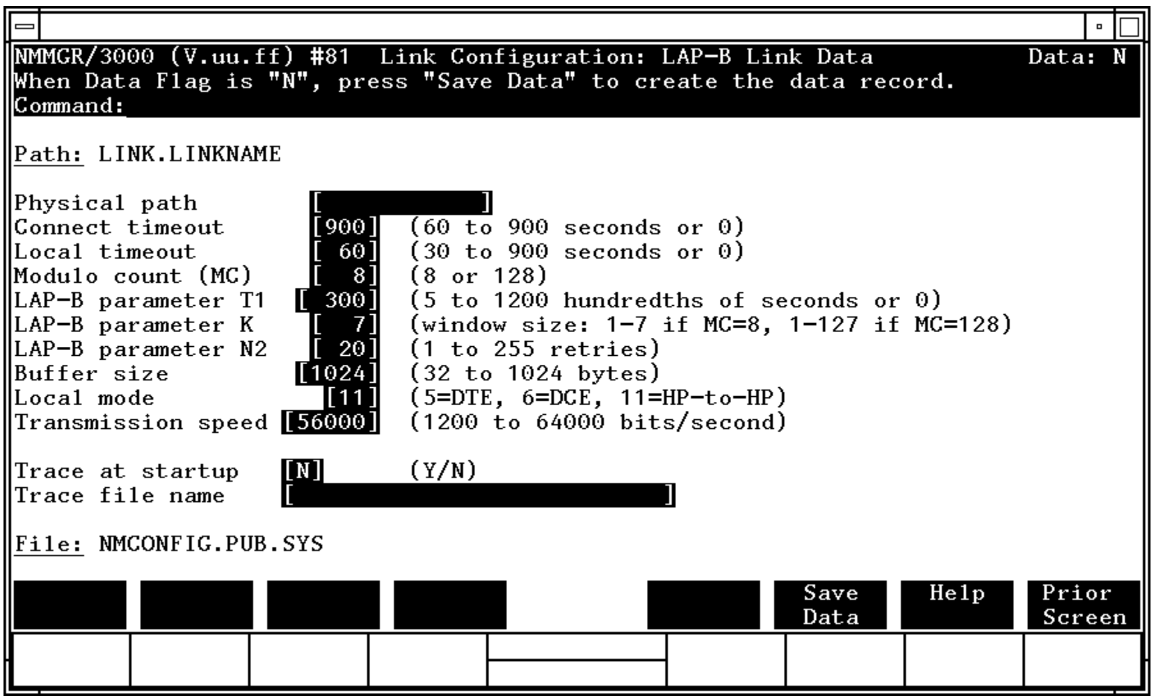
Link Configuration: LAP-B Link Data

The Link Configuration: LAP-B Link Data screen (#81) in Figure 3-4 is displayed when you select a link name of type LAP-B at the Link Selection screen (Figure 3-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@LINK.`*`linkname`*

in the command window of any screen and press the **[Enter]** key, where *linkname* is a configured LAP-B link.

Figure 3-4 Link Configuration: LAP-B Link Data Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Physical path`

The physical path of the Programmable Serial Interface (PSI) card.

The basic formula for deriving the physical path is *4 x slot number*. (Example: 4 x 10 = 40.) For systems with dual card cages, you must also specify a path number for the card cage, as follows:

PathNumber/(4 X SlotNumber)

where (a) *PathNumber* is a number corresponding to the card cage the PSI is in:

Card cage 0: *PathNumber* = 2

Card cage 1: *PathNumber* = 6

(b) / is the slash character (not the division sign), (c) the parentheses are used to set off an arithmetic formula (they are not entered as part of the Physical Path value), (d) X is the multiplication sign (not the character X), and (e) SlotNumber is the number of the slot, within the card cage, the PSI is in.

Examples:

If the PSI is in card cage 0, slot number 4, the Physical Path is 2/16

(*PathNumber*, slash character, 4 multiplied by 4).

If the PSI is in card cage 1, slot number 3, the Physical Path is 6/12

(*PathNumber*, slash character, 4 multiplied by 3).

If you are unsure of the slot location or of the physical path number to configure for your system, see your system documentation or consult your Hewlett-Packard service representative.

`Connect timeout` **(HP modifiable.)** During link initialization, this value specifies the amount of time the PSI 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 (0 means disabled)

`Local timeout` This is a handshake sequence between the host and its PSI card. It is useful to prevent the PSI card from keeping a line up when the system goes down.

Default value: 60

Range: 30–900 seconds or 0 (0 means disabled)

`Modulo count` This parameter specifies a window representing the number of frames that can be outstanding.

Default value: 8

Range: 8 or 128

`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 acknowledgment before initiating a recovery procedure. This delay must account for three frame transmissions and two frame-processing delays. An approximation of this value is three seconds for line speeds greater than or equal to 9600 bits per second and four seconds for line speeds less than 9600 bits per second.

The formula for the approximation in hundredths of a second is the following:

```
400 x [(buffer size x 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 to 1200 hundredths of seconds or 0 (0 means disabled)

`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 if modulo count=8; 1–127 if modulo count=128

`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 retries

`Buffer size` Layer 3 through 7 frame size. This is the amount of data that a user of OSI Levels 3 through 7 can put in that frame. It does not include Level 2 header or trailer information. This parameter is used to configure memory buffers.

Default value: 1024

Range: 32–1024 Bytes

`Local mode` If the node you are configuring is a Hewlett-Packard computer operating across a point-to-point link, enter 11 (the default). HP computers at both ends of a point-to-point link must both be configured as HP point-to-point. If the remote node is a non-HP node and the local station is acting as DTE, enter 5. If the remote node is a non-HP node and the local station is acting as DCE, enter 6. If the node you are configuring is DCE, then the node at the other side must be DTE. If the node you are configuring is DTE, then the node at the other side must be DCE.

Default value: 11

Range: 5 = DTE, 6 = DCE, 11 = HP Point-to-Point

`Transmission speed` This is the line-transmission speed in bits per second. It may be overridden by whichever device is providing clocking. The PSI simply transmits using the provided clock source, whether it is the HP 3000's CPU clock or a modem.

Default value: 56000

Range: 1200, 2400, 4800, 9600, 19200, 38400, 56000, or 64000 bits/second

`Trace at startup` **(HP modifiable.)** Enter `Y` (YES) to enable link tracing at link startup, `N` (NO) otherwise. This value 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 file name`

(HP modifiable.) Required if link trace is enabled. Name of the disk file where you want to record tracing. Must be a valid file name. Enter the file name 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.

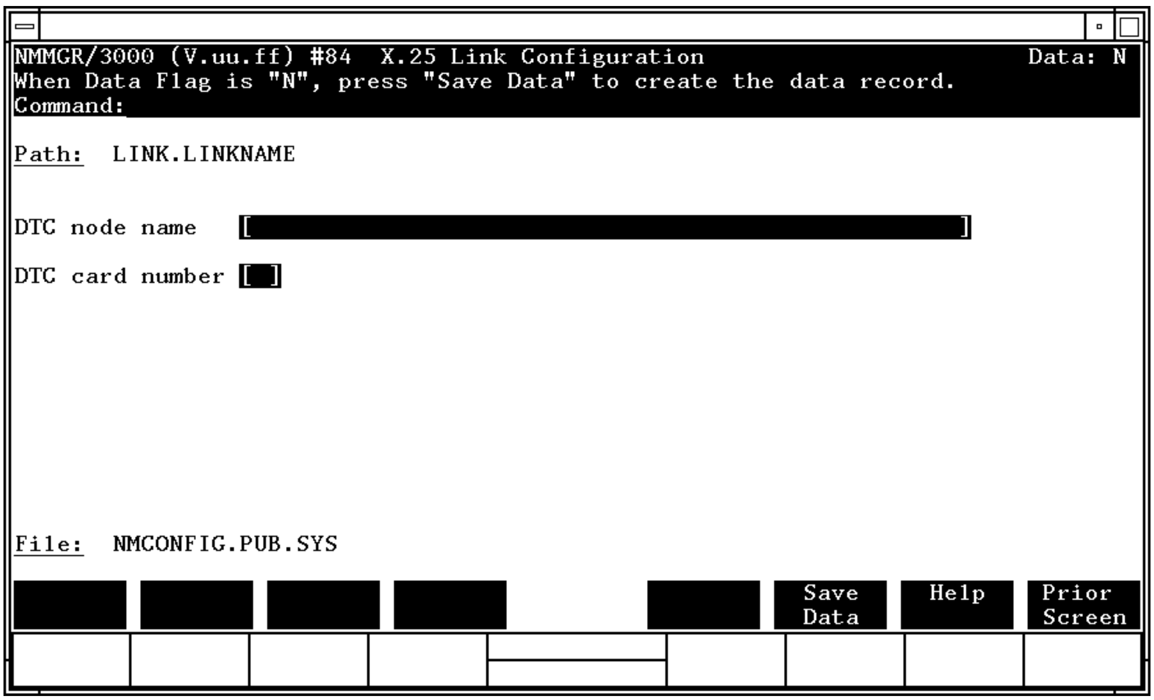
X.25 Link Configuration

The X.25 Link Configuration Screen (#84) in Figure 3-5 is displayed when you add a link of type X.25 at the Link Selection Screen (Figure 3-2) and press the **[Add]** or **[Modify]** function key. This screen is also displayed when you type the path name:

`@LINK.`*`linkname`*

in the command window of any screen and press the **[Enter]** key, where *linkname* is a configured X.25 link.

Figure 3-5 X.25 Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`DTC node name`
: This is the name of the DTC node where the DTC/X.25 Network Access card is installed. The format for the name is `name.domain.organization`. The entire DTC name can have a maximum number of 50 characters, and each field can have a maximum of 16 characters (alphanumeric, underscore or hyphens) and is separated from the other fields by periods. The first character of each field must be alphabetic.

Each DTC must have a unique *name* within the local network, and the `name.domain` portion of the DTC name must be *unique* for each DTC within the internetwork. HP recommends that all nodes on the same network be assigned the same domain and organization.

The DTC node name must match the name configured at the DTC Node Name screen under DTS configuration. Refer to *Configuring Systems for Terminals, Printers, and Other Serial Devices* for more information about configuring the DTC.

`DTC card number`

(Required.) Enter the DTC card number. The DTC card number is the number of the slot in the DTC where the DTC/X.25 Network Access card for this node resides. Slot 0 of the DTC is reserved and cannot be used by a DTC/X.25 Network Access card. A DTC can be configured with a maximum of 3 DTC/X.25 Network Access cards.

Make sure that the DTC is already configured before you configure an X.25 link on the HP 3000. Refer to *Configuring Systems for Terminals, Printers, and Other Serial Devices* and *Using the OpenView DTC Manager* for complete information on configuring the DTC.

Default: None.

Range: 1–5

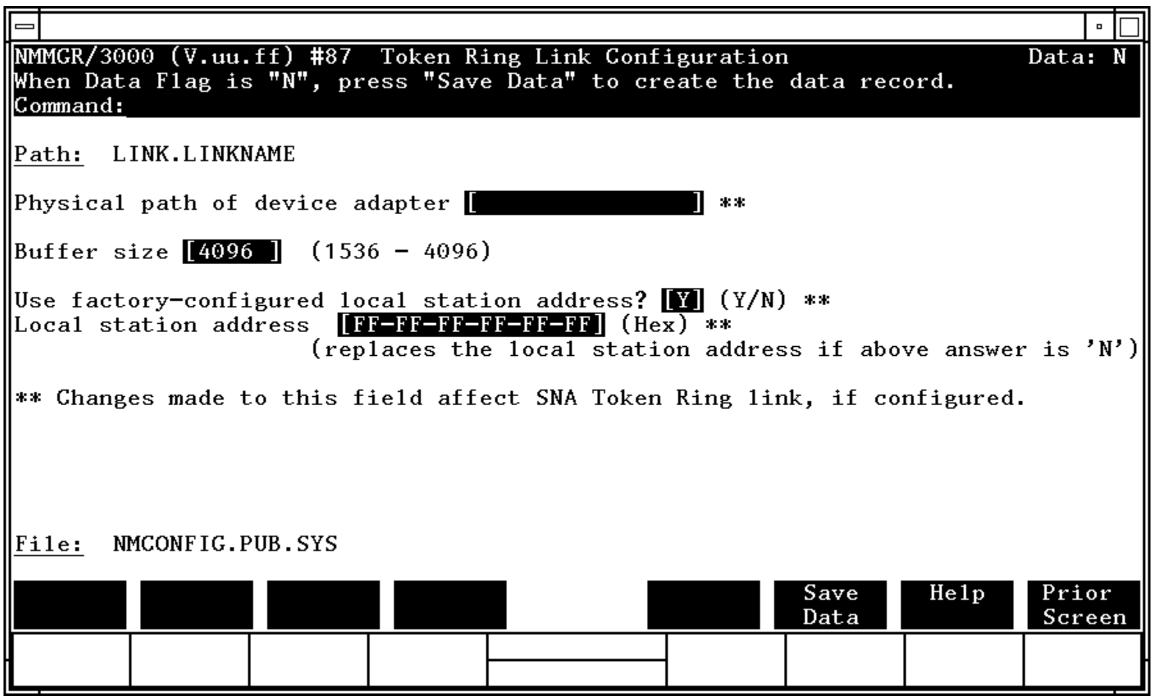
Token Ring Link Configuration

The Token Ring Link Configuration screen (#87) in Figure 3-6 is displayed when you select a link name of type TOKEN at the Link Selection screen (Figure 3-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@LINK.`*`linkname`*

in the command window of any screen and press the **[Enter]** key, where *linkname* is the name of a configured token ring link.

Figure 3-6 Token Ring Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

CAUTION

If the SNA token ring link product is already configured for the IBM subsystem, the values that initially appear in the Token Ring Link Configuration screen fields reflect the SNA configuration. If the same token ring card is being used for both NS and SNA communications, certain fields in the Token Ring Link Configuration screen must match the values of the SNA token ring link configuration. (See the following field descriptions.)

If the *Link Name* configured for a NS token ring link is the same as the name of a SNA token ring link, make sure that the values of these fields in the NS token ring link configuration match the SNA token ring link configuration; otherwise, the NS token ring link configuration will change the SNA token ring link configuration.

Fields

`Physical path of device adapter` The physical path number corresponds to the slot location of a node's token ring device adapter. For HP 3000 systems, the path is derived by a basic formula of *4 x slot number*. (Example: 4 x 10 = 40, where the token ring device adapter is installed in slot number 10 and the physical path of the device adapter is 40.)

NOTE

If the same token ring card is being used for both NS and SNA communications, you must use the same value for this field as is configured for the SNA link.

If you are unsure of the slot location or of the physical path number to configure for your system, see your system documentation or consult your Hewlett-Packard service representative.

`Buffer size` The size, in bytes, of the buffer that holds data transferred from the token ring card to the upper layers (inbound data only).

Default value: 4096

Range: 1536–4096

`Use factory-configured local station address?`

The token ring adapter is supplied with a 48-bit station address. These are guaranteed to be unique. Do not override the factory configured local node address except on the specific instructions of your network administrator or your Hewlett-Packard representative.

Default value: Y

NOTE If the same token ring card is being used for both NS and SNA communications, you must specify the local station address that is configured for the SNA token ring link.

`Local station address` This field is to be used only with specific instructions from your network administrator or your Hewlett-Packard representative. It allows you to enter a station address to replace the factory configured address. The format must be compatible with HP software requirements.

NOTE If the same token ring card is being used for both NS and SNA communications, you must specify the local station address that is configured for the SNA Link.

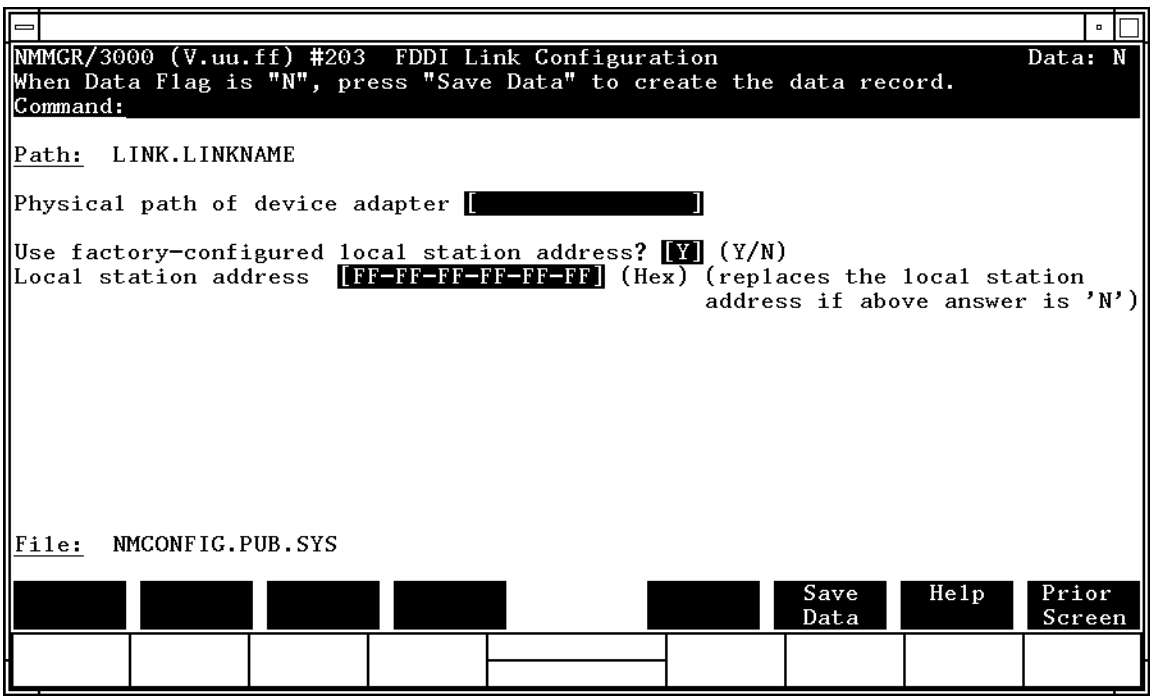
FDDI Link Configuration

The FDDI Link Configuration screen (#203) in Figure 3-7 is displayed when you select a link name of type FDDI at the Link Selection screen (Figure 3-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@LINK.`*`linkname`*

in the command window of any screen and press the **[Enter]** key, where *linkname* is the name of a configured FDDI link.

Figure 3-7 FDDI Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Physical path of device adapter` The physical path number corresponds to the slot location of a node's FDDI device adapter. For HP 3000 systems, the path is derived by a basic formula of *4 x slot number*. (Example: 4 x 10 = 40, where the FDDI device adapter is installed in slot number 10 and the physical path of the device adapter is 40.)

If you are unsure of the slot location or of the physical path number to configure for your system, see your system documentation or consult your Hewlett-Packard service representative.

`Use factory-configured local station address?`

The FDDI adapter is supplied with a 48-bit station address. These are guaranteed to be unique. Do not override the factory configured local node address except on the specific instructions of your network administrator or your Hewlett-Packard representative.

Default value: Y

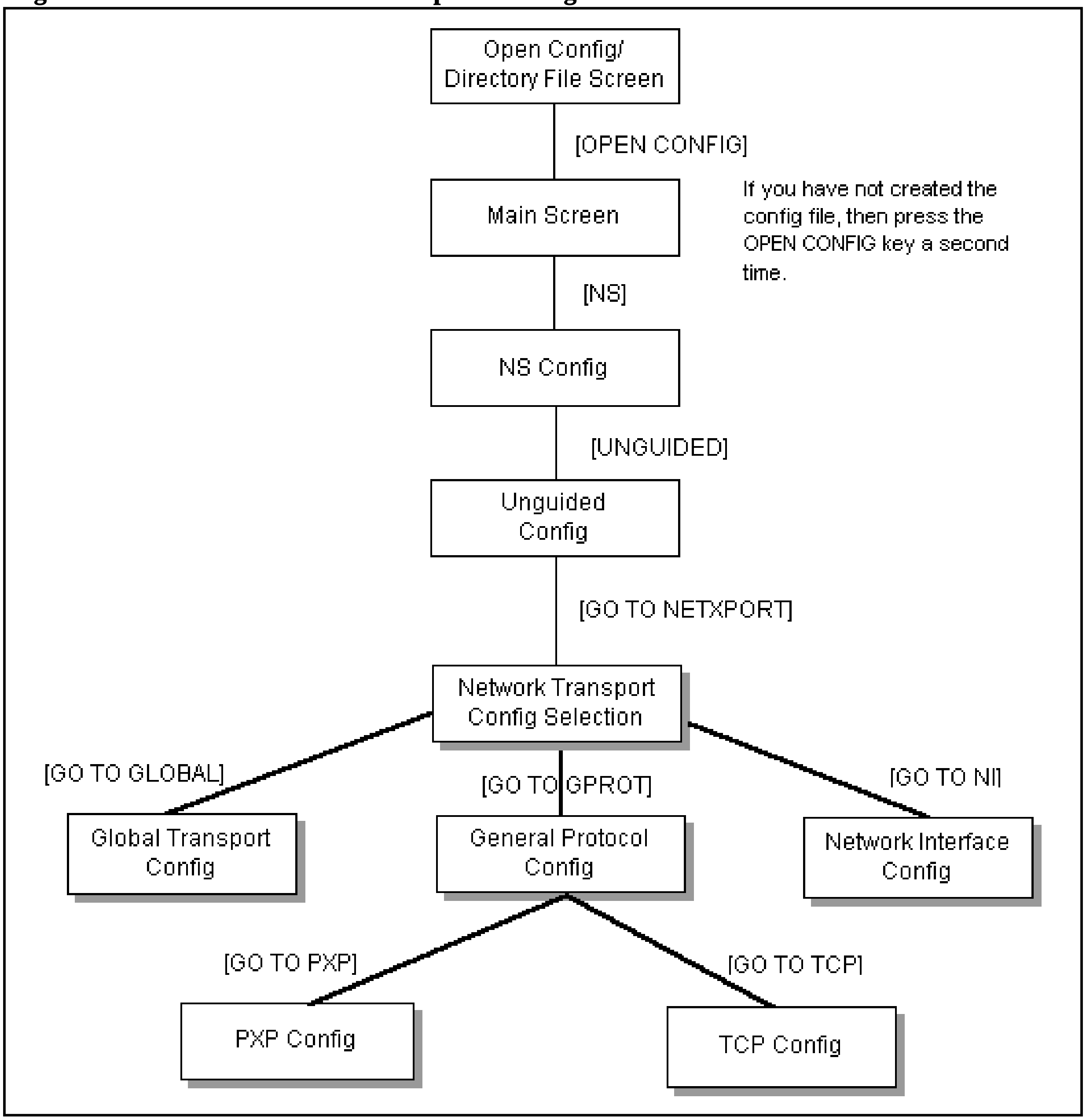
`Local station address`

This field is to be used only with specific instructions from your network administrator or your Hewlett-Packard representative. It allows you to enter a station address to replace the factory configured address. The format must be compatible with HP software requirements.

4 Network Transport Configuration Screens

This section contains information about the NMMGR configuration screens that are common to all network interfaces. The network transport configuration branch of NMMGR begins with a screen called the Network Transport Configuration Selection screen. Figure 4-1 shows the screen flow for configuring the Network Transport Configuration screens. Screens unique to the Network Transport Configuration are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow

Figure 4-1 Network Transport configuration Screen Flow



The Network Transport Configuration Selection screen allows you to define global parameters for the node as well as network interfaces of type LAN, ROUTER (point-to-point), X.25, SNA, TOKEN (token ring), FDDI, 100VG-AnyLAN, 100Base-T, Gateway Half, or Loopback.

To reach the network transport configuration screens, run NMMGR, and refer to the following pages of this section for a step-by-step process.

Step-by-Step Process:

Step 1. Run NMMGR. The Open Configuration/Directry File screen is displayed.

Step 2. Enter the configuration file name (`NMCONFIG.PUB.SYS`) and password, if a password is required, and press the **[Open Config]** function key. If you have not yet created the configuration file you will need to press the key a second time. The Main screen is displayed.

Step 3. Press the **[NS]** function key. The NS Configuration screen is displayed.

Step 4. Press the **[Unguided Config]** function key. The Unguided Configuration screen is displayed.

Step 5. Press the **[Go To NETXPORT]** function key and the Network Transport Configuration Selection screen is displayed.

For more general information on NMMGR, refer to *Using the Node Management Services (NMS) Utilities*.

NOTE Fields described as **“HP modifiable”** should be changed only upon the recommendation of your Hewlett-Packard representative.

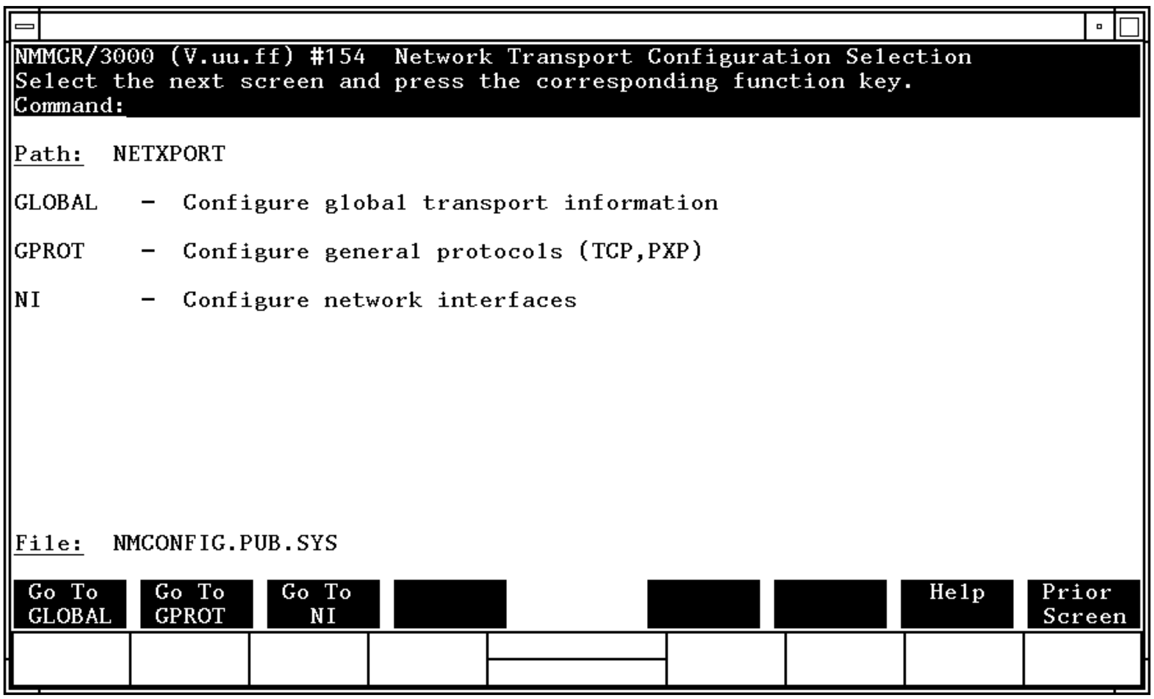
Network Transport Configuration Selection

The Network Transport Configuration Selection screen (#154) shown in Figure 4-2 is displayed when you press the function key for **[Go To NETXPORT]** at the Unguided Configuration screen (#80). It is also displayed when you type the path name:

`@NETXPORT`

in the command window of any screen and press the **[Enter]** key.

Figure 4-2 Network Transport Configuration Selection Screen



From this screen you proceed to the screens used to configure the network transport.

Choose the item you wish to configure and press the corresponding function key. Global transport information and general protocol information should be configured for all network interfaces.

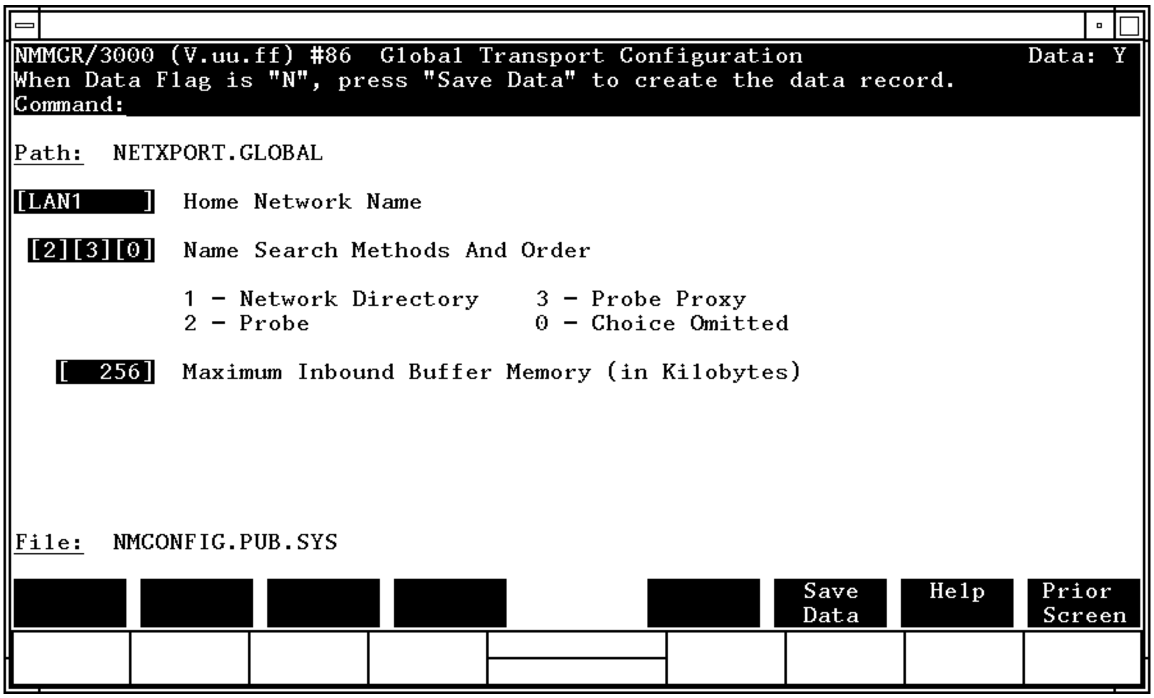
Global Transport Configuration

The Global Transport Configuration screen (#86) in Figure 4-3 is displayed when you press the **[Go To GLOBAL]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

`@NETXPORT.GLOBAL`

in the command window of any screen and press the **[Enter]** key.

Figure 4-3 Global Transport Configuration Screen



This screen lets you enter information that is used for transferring information between nodes. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Home network name`

Leave this field blank if there are no gateway half network interfaces configured and this node will be on only a single network. Otherwise, enter the network interface (NI) name of the network that this node will usually be on.

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.

Related screen:

- `NETXPORT.NI`

  NI names are 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 `IPCDest` or `IPCLookup` intrinsics) will be resolved into network addressing information. This addressing information is contained in a structure called a path report.

The search order will be checked against the capabilities of the node and search methods will be ignored if they are not appropriate for the node. If all choices fail (or are omitted), the network will attempt to resolve the address using the domain name resolver.

The available search methods are as follows:

0 =	**Choice Omitted**. Enter a 0 if you want to omit one or more of the name search methods. If you enter 0s in all three fields, all three choices are omitted. In this case, the network will try to resolve the address using the domain name resolver.
1 =	**Network directory**. Enter a 1 to specify that the network should attempt to resolve the address via a search of the network directory.
2 =	**Probe**. Enter a 2 to indicate that the network should attempt to resolve the address using the probe protocol.
3 =	**Probe proxy**. Enter a 3 to indicate that the network should attempt to resolve the address via the network directory configured on the proxy node, if a proxy node exists.

Default value: 2, 3, 1 (Probe, Probe Proxy, Network Directory)

Range: 0–3

NOTE If you are using domain names, the domain name can be resolved via either the domain name resolver or host tables. See the *HP 3000/iX Network Planning and Configuration Guide* for more information on domain names.

`Maximum inbound buffer memory (in kilobytes)` This configures the amount of memory used to store incoming data. NS divides this number by the inbound buffer size configured for the link to calculate the number of inbound buffers to allocate. HP recommends you use the default.

Default value: 256

Range: 128–512

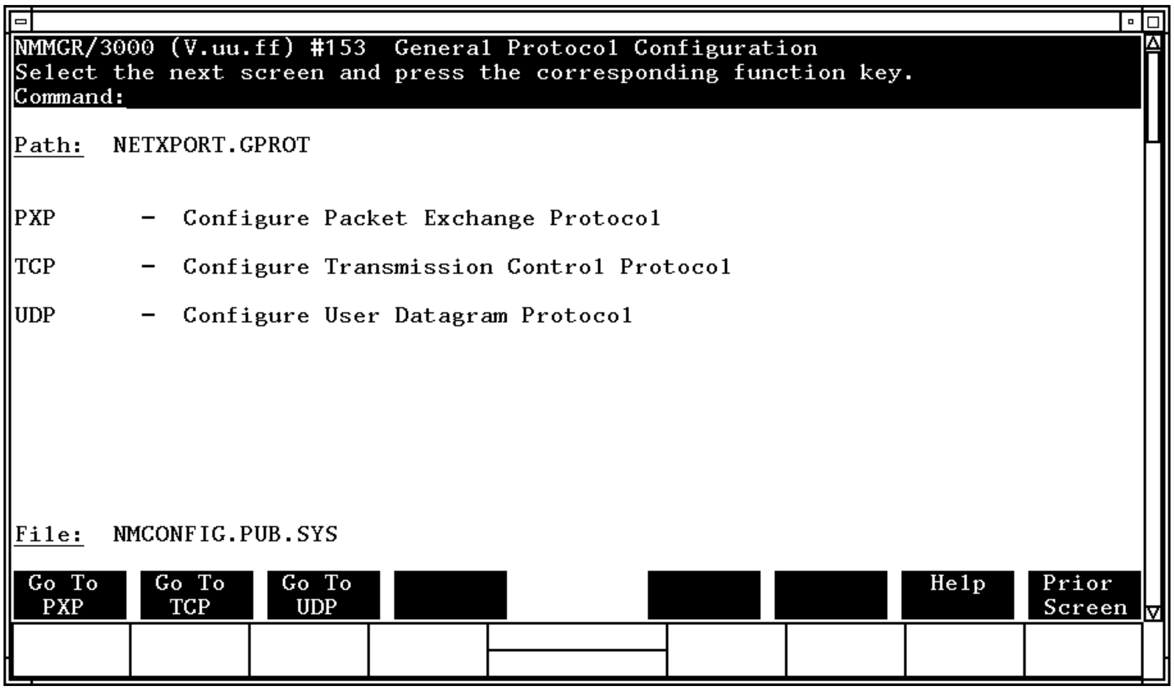
General Protocol Configuration

The General Protocol Configuration screen (#153) in Figure 4-4 is displayed when you press the **[Go To GPROT]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

`@NETXPORT.GPROT`

in the command window of any screen and press the **[Enter]** key.

Figure 4-4 General Protocol Configuration Screen



From this screen you proceed to the screens used to configure the general protocols of the network transport. The UDP, TCP, and PXP protocols must be configured for each node.

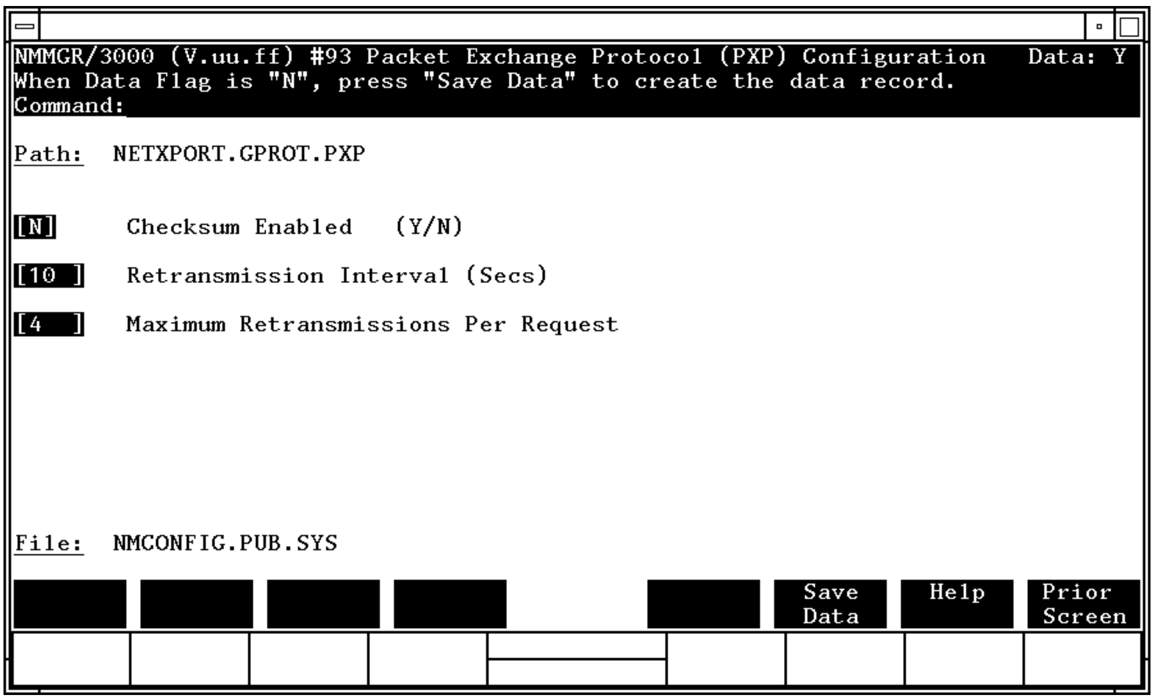
Packet Exchange Protocol (PXP) Configuration

The Packet Exchange Protocol (PXP) Configuration screen (#93) in Figure 4-5 is displayed when you press the **[Go To PXP]** function key at the General Protocol Configuration screen (Figure 4-4). It is also displayed when you type the path name:

```
@NETXPORT.GPROT.PXP
```

in the command window of any screen and press the **[Enter]** key.

Figure 4-5 Packet Exchange Protocol (PXP) Configuration Screen



This screen contains the information necessary to configure packet exchange protocol (PXP) for the node. The information configured falls into two categories:

- Reliability (checksum field).
- Performance parameters (retransmission fields).

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Checksum enabled (Y/N)`

Checksumming is a method of error checking. Enter a `Y` (yes) to enable checksumming for all sockets for this protocol. Enter an `N` (no) to allow individual sockets to choose checksumming for themselves.

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 unless communication to a non-HP machine is desired.

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 will be necessary. Frequent log messages indicating that retransmissions are taking place or that requests are failing indicate 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:

```
RTXinterval + (RTXinterval * MAXRTX)
```

where `RTXinterval` is the configured retransmission interval and `MAXRTX` is the configured maximum retransmissions per packet. Note that excessive values would cause unacceptably long delays before `IPCLookup` would fail under normal conditions such as the remote node failing.

Default value: 4

Range: 1–100

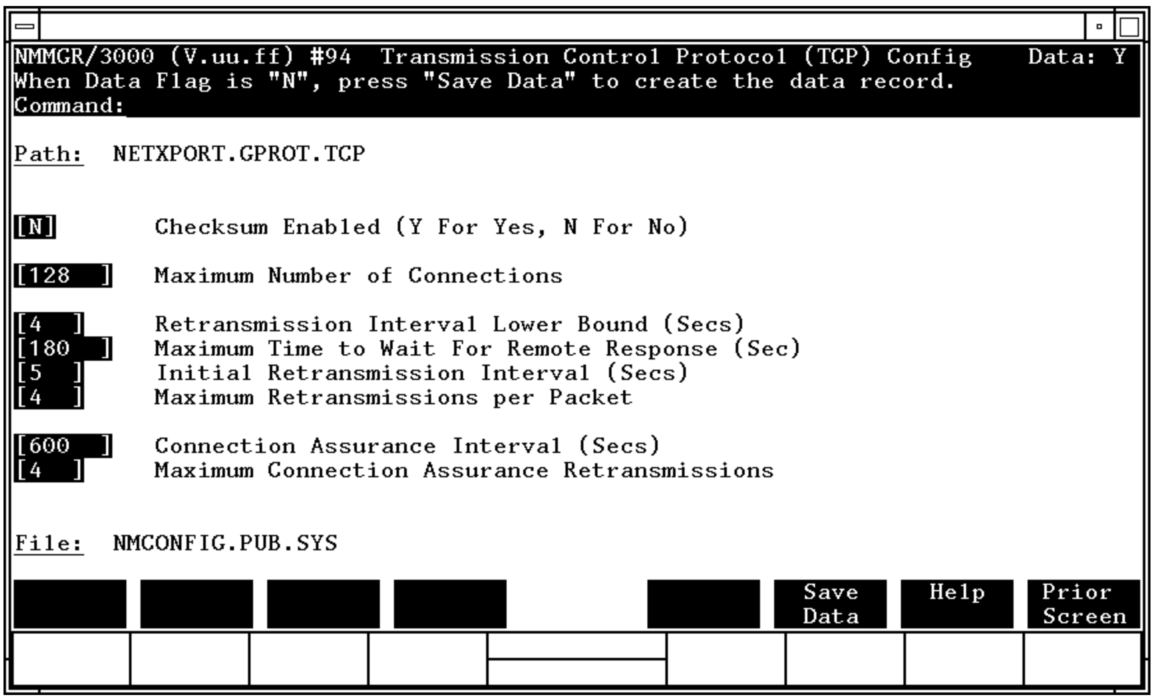
Transmission Control Protocol (TCP) Configuration

The Transmission Control Protocol (TCP) Configuration screen (#94) in Figure 4-6 is displayed when you press the **[Go To TCP]** function key at the General Protocol Configuration screen (Figure 4-4). It is also displayed when you type the path name:

```
@NETXPORT.GPROT.TCP
```

in the command window of any screen and press the **[Enter]** key.

Figure 4-6 Transmission Control Protocol (TCP) Configuration Sxreen



This screen lets you enter the information necessary to configure transmission control protocol (TCP) for the node. TCP is required in order for the network transport to function. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. 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 algorithm used for congestion and flow control is based on the **Van Jacobson algorithm** which uses the **initial retransmission timeout** for most calculations. The initial retransmission timeout is the greater of the following two values:

- The value you configure in the Retransmission interval lower bound field

  or

- The calculated smooth round trip (SRT) time which is automatically calculated based on the average round trip time from the last few send and acknowledgement packet timestamps.

The TCP retransmission algorithm works as follows:

- Once a packet is sent, the local node waits for a response from the remote node. If a response is not received before the initial retransmission timeout, the packet is transmitted again.
- The algorithm uses a multiplier of 2. For each time that a packet is retransmitted, the multiplier is doubled, thus exponentially increasing the wait time. Given an initial retransmission timeout of X seconds, the sequence of timeout values would be X, 2X, 4X, 8X seconds and so on.
- Retransmission is stopped when either one of the following happens:
  - The time configured in maximum time to wait for remote response is reached. This happens when the total time of all retransmission intervals would exceed the maximum time to wait for remote response.
  - The number of retransmissions configured in maximum retransmissions per packet is reached.

Let us take an example using the default values. Assume that the calculated smooth round trip is 1 second. Since the retransmission interval lower bound (4 secs) is the greater of the two, its value is used as the initial retransmission timeout. If the node does not get an acknowledgement after 4 seconds, the packet is retransmitted. If there is still no acknowledgement, the retransmission of the outstanding packet would be at intervals of 4, 8, 16, and 30 seconds. The connection would be broken after 30 seconds because a maximum of 4 retries is allowed.

Needless retransmissions may occur if you set retransmission interval lower bound low and you set maximum time to wait for remote response and maximum retransmissions per packet high. If the retransmission interval lower bound is set too high, an unnecessarily long delay occurs when a packet is lost, and a retransmission will be necessary.

Connections may be prematurely aborted if you set retransmission interval lower bound low and you set maximum time to wait for remote response or maximum retransmissions per packet low. 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.

Fields

`Checksum enabled`

Checksumming is a method of error checking used for reliability. TCP checksumming causes a very slight overhead. It is not normally needed over most reliable link types. 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:

- The destination path report in the network directory or probe.
- The local configuration (as specified in this screen).
- The values specified in the NetIPC intrinsics, `IPCCONNECT` and `IPCRECVCN`.

Should any of these sources indicate checksumming enabled, the connection will be checksummed.

The effect of disabling checksum in the configuration is not to prohibit checksumming, but simply to allow each connection to choose for itself. The Network Services specify checksumming disabled in their NetIPC calls thereby allowing control to be taken through the configuration and network directory. Therefore, TCP checksumming for Network 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`

This is a sizing parameter that allows you to configure the number of connections based on the size of your network (how many users there are). Each connection functions as a separate entity in regard to destination, flow control and retransmissions. TCP connections and NetIPC have a one-to-one correspondence for calls to `IPCCONNECT`, and therefore between each Network Service invoked by each user. There is no multiplexing of user or Network Services data over TCP connections.

The number of connections configured should reflect an estimation of the number of Network Services and NetIPC users that will be active simultaneously. This includes both outbound and inbound connections. The value configured should be relatively large to accommodate expansion. Note that the allocation of buffers is related to the number of TCP connections. If this field is modified, the NI screens controlling buffer allocation (`NETXPORT.NI.`*`NIname`* for outbound buffers, and `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` for store and forward buffers) must be updated.

Default value: 128

Range: 1–4096

`Retransmission interval lower bound (Secs)` The retransmission interval is the smallest interval (in seconds) that a TCP connection waits for a reply from a remote node before retransmitting a packet. If the calculated SRT time is greater than this value, then the SRT time is used for retransmission. Increase the value if connections are being dropped prematurely or if there is too much traffic due to packet retransmission.

Default value: 4

Range: 1–999

`Maximum time to wait for remote response (sec)` This is the total time allowed for retransmissions. Increase this value if connections are being dropped prematurely. Decrease this value if there is too much traffic due to packet retransmission.

Default value: 180

Range: 10–32767

`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 should be greater than the retransmission interval lower bound.

Default value: 5

Range: 2–999

`Maximum retransmissions per packet`

This is the maximum number of times that TCP will retransmit a packet before aborting the connection. Increase the value if connections are being dropped prematurely. Decrease the value if there is too much traffic due to packet retransmission.

Default value: 4

Range: 1–100

`Connection assurance interval (secs)`

This timer allows you to adjust the time you wait for resources to be released after an idle disconnect. If the remote connection is abruptly interrupted, TCP waits for the amount of time calculated by the following algorithm:

```
CAinterval + (CAinterval * MAXCARTX)
```

where `CAinterval` is the connection assurance interval and `MAXCARTX` is the maximum connection assurance retransmissions.

TCP drops the connection thus freeing all resources held by that connection. Increase this value if you are experiencing too much overhead for retries due to idle disconnects. Decrease this value if you are waiting too long for resources to be freed due to idle disconnects.

Default value: 600

Range: 10–32767

`Maximum connection assurance retransmissions`

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 value 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)
```

where `CAinterval` is the connection assurance interval and `MAXCARTX` is the maximum connection assurance retransmissions.

Default value: 4

Range: 0–999

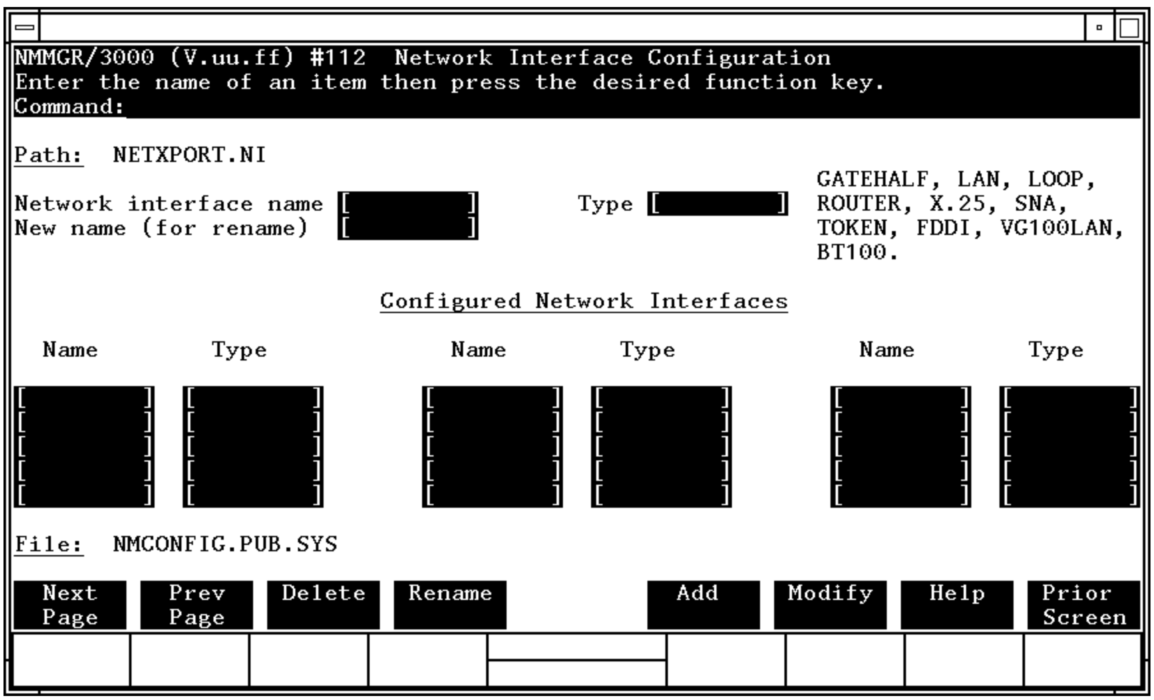
Network Interface Configuration

Network Interface Configuration The Network Interface Configuration screen (#112) in Figure 4-7 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

`@NETXPORT.NI`

in the command window of any screen and press the **[Enter]** key.

Figure 4-7 Network Interface Configuration Screen



For information on selecting a specific network interface, refer to the following Chapters:

LAN	Chapter 5, "LAN Network Interface Configuration Screens."
ROUTER	Chapter 6, "Point-to-Point (Router) Network Interface Configuration Screens."
X.25	Chapter 7, "X.25 Network Interface Configuration Screens."
TOKEN	Chapter 8, "Token Ring Network Interface Configuration Screens."
FDDI	Chapter 9, "FDDI Network Interface Configuration Screens."

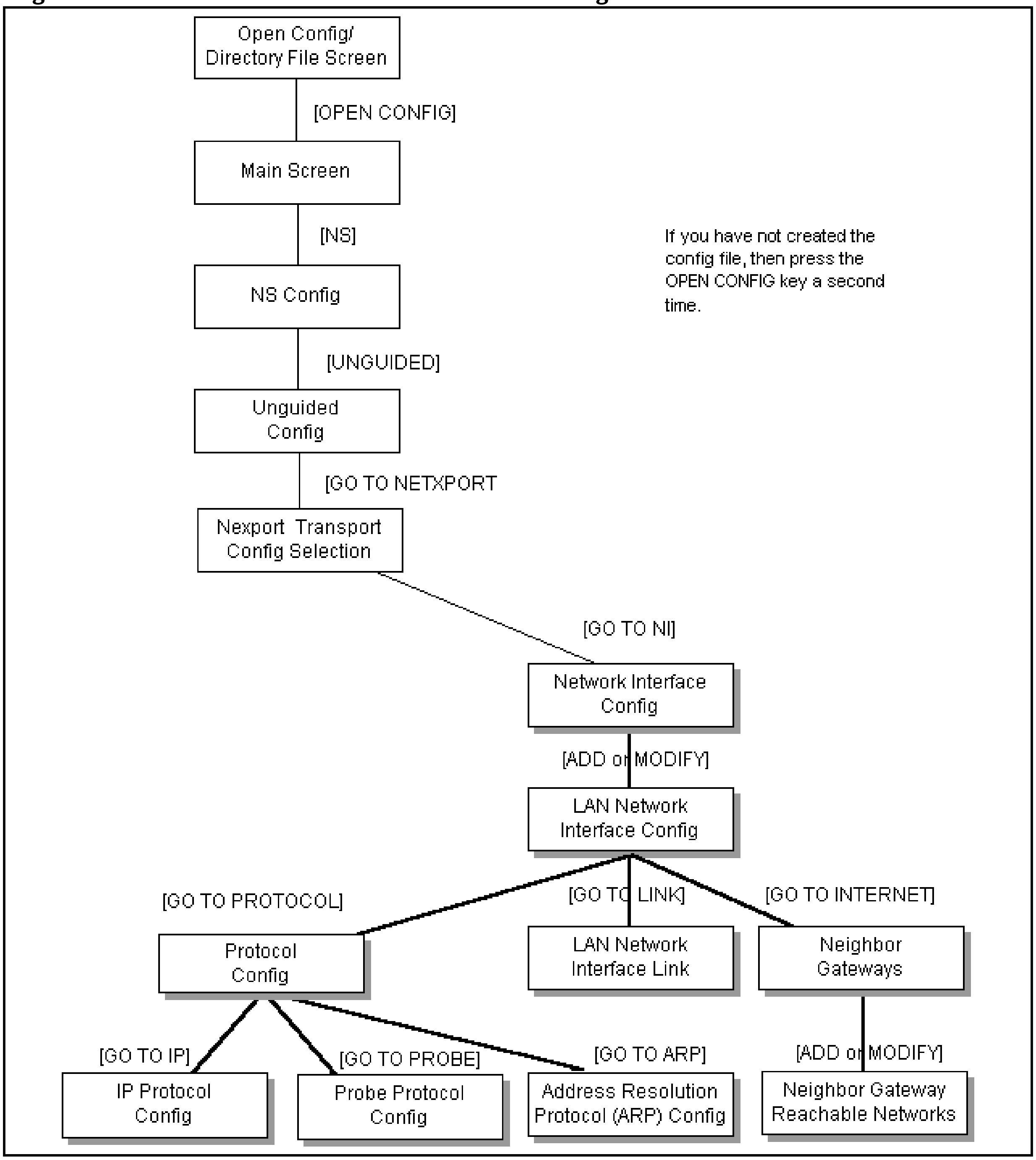
100VG-AnyLAN	Chapter 10, “100VG-AnyLAN Network Interface Configuration Screens.”
100Base-T	Chapter 11, “100Base-T Network Interface Configuration Screens.”
GATEHALF	Chapter 12, “Gateway Half Network Interface Configuration Screens.”
LOOP	Chapter 13, “Loopback Network Interface Configuration Screens.”

NS/SNA is no longer offered as a product and has been removed from the *Corporate Price List*.

5 LAN Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring an IEEE 802.3/Ethernet LAN network. Figure 5-1 shows the screen flow for configuring the IEEE 802.3/Ethernet LAN screens. Screens unique to the LAN are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 5-1 LAN Network Interface Configuratuion Screen Flow



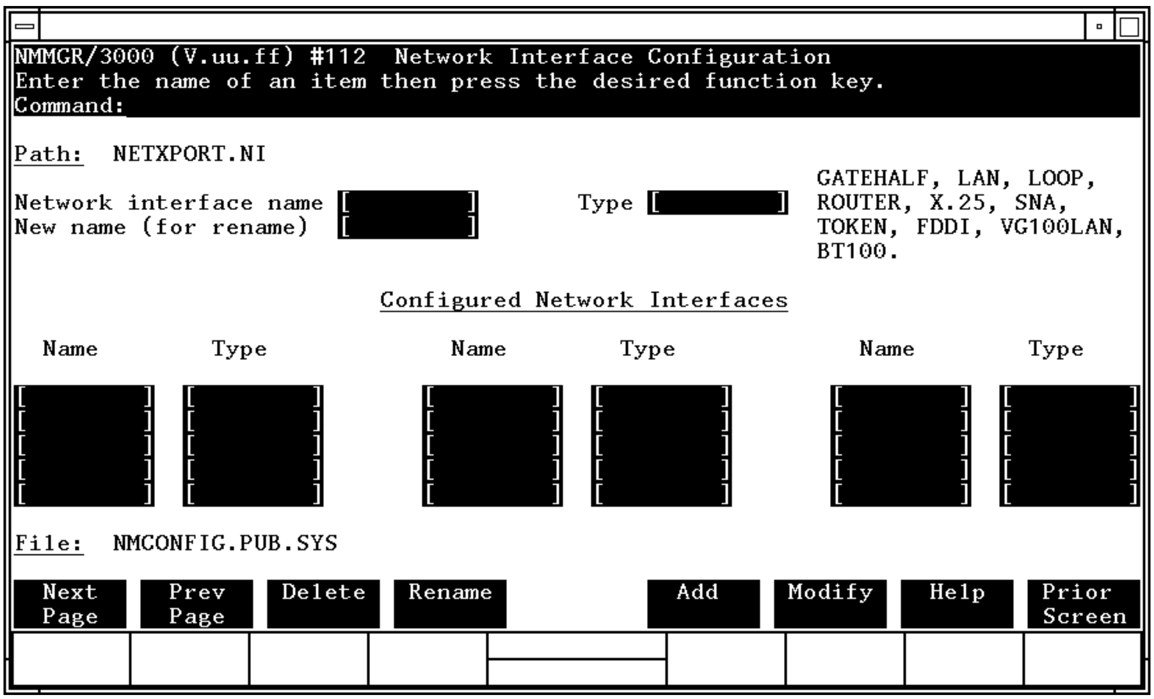
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 5-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-1). It is also displayed when you type the path name:

```
@NETXPORT.NI
```

in the command window of any screen and press the **[Enter]** key.

Figure 5-2 Network Interface Configuraiton Screen



Use the fields and the function keys of the select screen to perform the desired action:

- To define a new LAN NI, specify the NI name and NI type LAN; then press the **[Add]** function key. The path for the selected NI name is added to the configuration file and the data screen on that path is displayed. **You can have a maximum of 12 NI's per system (one NI must be used for loopback). However, HP supports up to two active LAN NI's per system.**

- To modify an existing NI configuration, specify the NI name; then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) 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.

Fields

`Network interface name` Enter the network interface name for the LAN interface. The network interface name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, 100VG-AnyLAN, 100Base-T, or FDDI)` (Required only when adding an NI.) Enter `LAN` if you are configuring a local area network.

`New name` (Required only when renaming an NI.) 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.

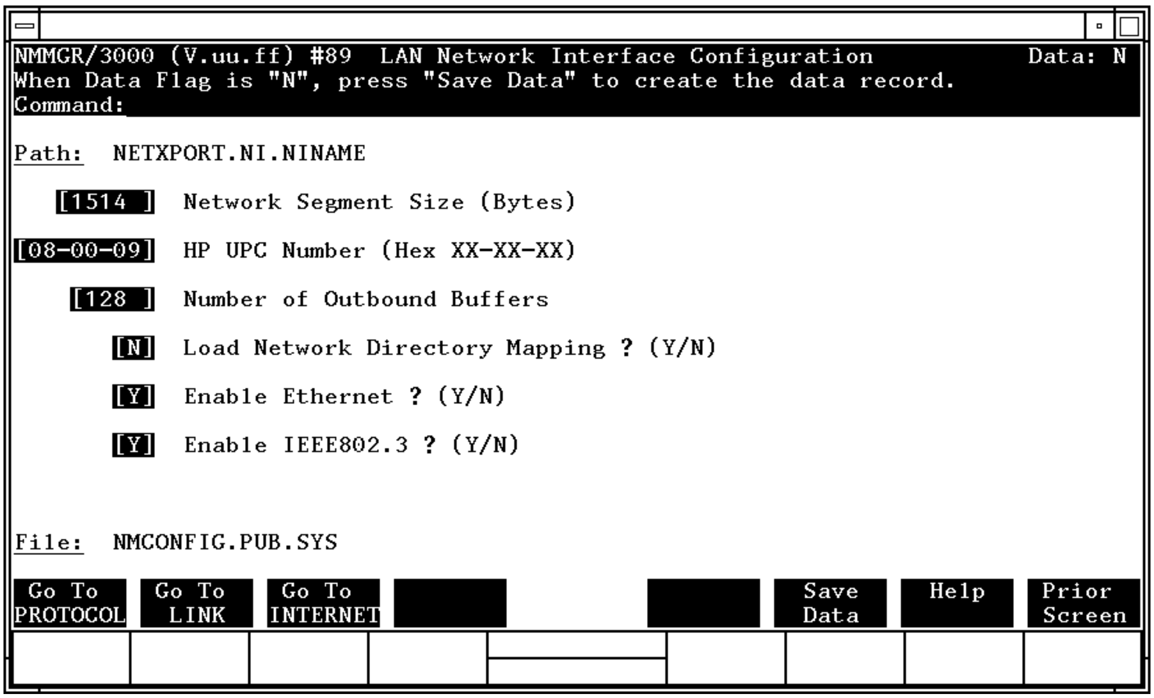
LAN Network Interface Configuration

The LAN Network Interface Configuration screen (#89) in Figure 5-3 is displayed when you select an NI name and the NI type LAN at the Network Interface Configuration screen (Figure 5-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI name.

Figure 5-3 LAN Network Interface Configuration Screen



The LAN network interface (NI) module serves to interface the upper layers of the transport product to the 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.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. 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 and internetwork routing.

Choose the item you wish to configure, and press the corresponding key.

Fields

`Network segment size (bytes)` **(HP modifiable.)** This field specifies the largest packet (including all data, protocol headers, and link level headers) that will be sent by the LAN device. The only reason for entering a value smaller than 1514 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: 1514 bytes

Range: 300–1514

`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

Change the default only in rare circumstances. If all nodes on the LAN are not configured with identical HP UPC numbers, probe multicasts will not be universally recognized by nodes on the LAN.

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Overallocation may waste core memory.

Related screen:

- `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: 128

Range: 128–4096

`Load network directory mapping? (Y/N)`

If you have non-HP nodes on the LAN (nodes that do not support either ARP or probe protocols,) you must enter these nodes into the network directory and set load network directory mapping to Y.

HP recommends the default unless non-HP nodes are on the LAN and the network directory has been configured. Refer to Chapter 15, “Network Directory,” for information about the network directory.

Default value: N

Range: Y or N

`Enable Ethernet? (Y/N)`

This flag enables the Ethernet protocol to run either by itself or with the IEEE802.3 protocol. You can enable one or the other or both of these protocols simultaneously. One or the other *must* be enabled (you cannot disable both). Ethernet is enabled by default. Disabling Ethernet has the effect of disabling the ARP protocol as well.

Default value: Y

Range: Y or N

`Enable IEEE802.3? (Y/N)`

This flag enables the IEEE 802.3 protocol to run either by itself or with the Ethernet protocol. You can enable one or the other or both of these protocols simultaneously. One or the other must be enabled (you cannot disable both). IEEE 802.3 is enabled by default. Disabling IEEE 802.3 has the effect of disabling the probe protocol as well.

Default value: Y

Range: Y or N

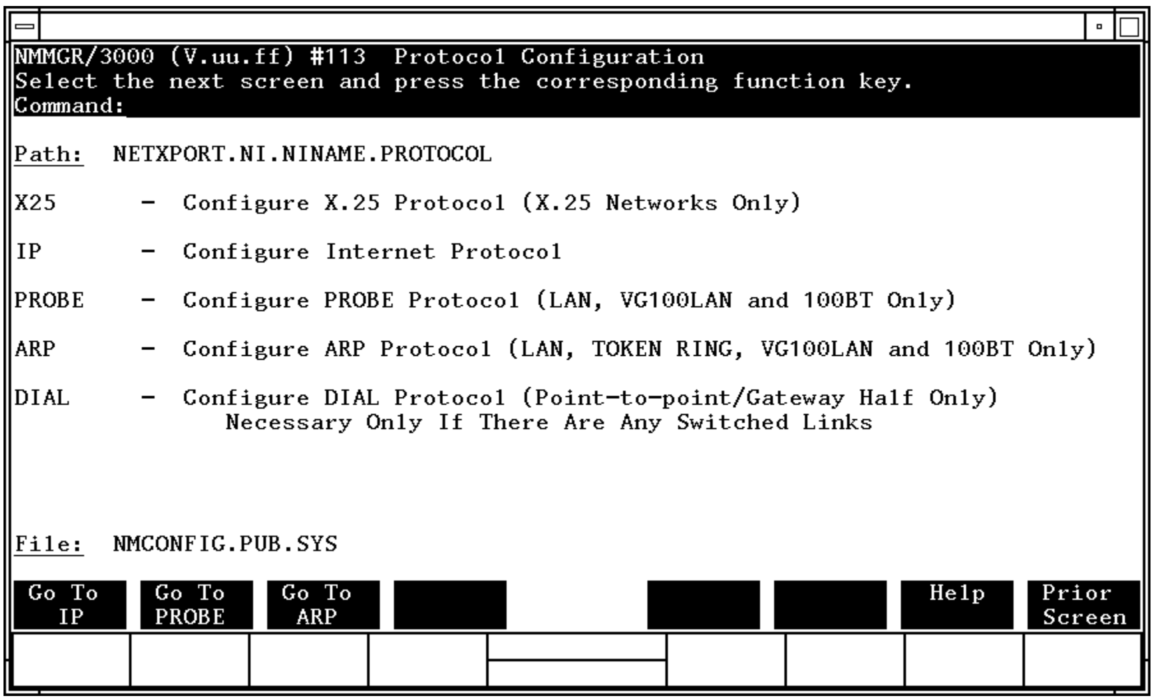
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 5-4 is displayed when you press the **[Go To PROTOCOL]** function key at the LAN Network Interface Configuration screen (Figure 5-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI.

Figure 5-4 Protocol Configuration Screen



For the LAN NI, you configure the IP, probe, and ARP protocols. Choose the protocol to configure, and press the corresponding function key.

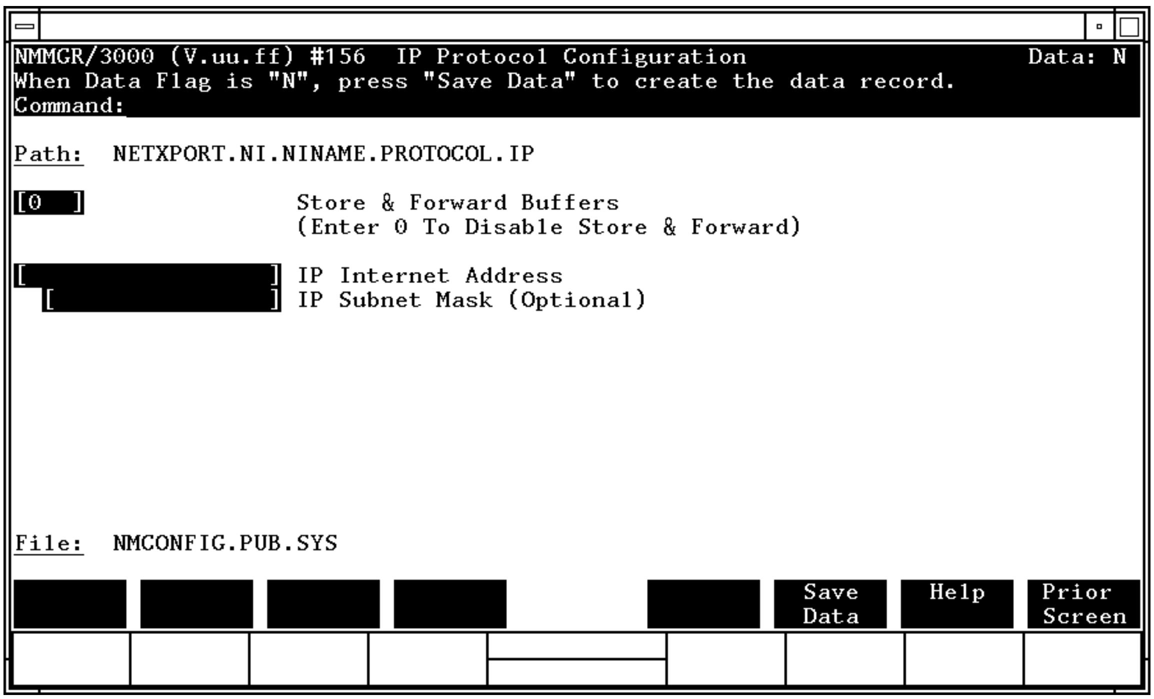
Internet Protocol Configuration

The IP Protocol Configuration screen (#156) in Figure 5-5 is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 5-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI.

Figure 5-5 IP Protocol Configuration Screen



This screen is used to supply IP protocol information for the network being configured. Each NI has an IP address. The IP address field is a key element in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI named in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

This field allocates buffers to support store-and-forward over the network interface being configured. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface. You can modify the number of store-and-forward buffers to allow performance tuning for different network types. HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

You do not need to allocate store-and-forward buffers if you are configuring a non-gateway node on this network. Leave the default (0) in this field to indicate that this is a non-gateway node.

Default value: 0

Range: 0–50

NOTE If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

`Class C:      C nnn.nnn.nnn xxx`

`Class B:     B nnn.nnn xxx.xxx`

`Class A:     A nnn xxx.xxx.xxx`

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and where *xxx* is a value ranging from 000 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:     001–126`

Network and node values of all zeroes or all ones are not allowed. These are special values.

Default value: No default, but a value *must* be supplied.

`IP subnet mask (optional)`
An IP subnet mask is used when configuring subnetworks. The mask identifies which bits of an IP address will be used to define a subnetwork. An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. For example, a mask for a Class A network with the subnet field being the first eight bits of the node part would be expressed as 255 255.000.000. The default is no IP subnet mask.

Refer to the *HP 3000/iX Network Planning and Configuration Guide* for more details on subnets.

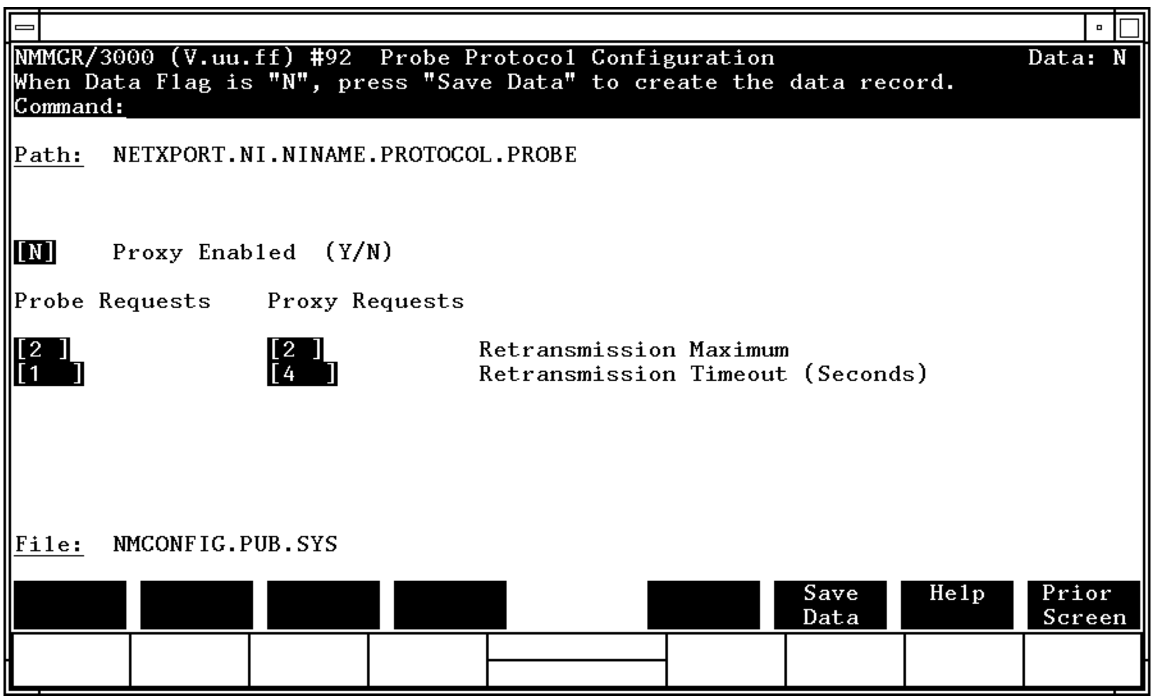
Probe Protocol Configuration

The Probe Protocol Configuration screen (#92) in Figure 5-6 is displayed when you press the **[Go To PROBE]** function at the Protocol Configuration screen (Figure 5-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.PROBE`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI.

Figure 5-6 Probe Protocol Configuration Screen



This screen allows you to configure the information required for the probe protocol. The probe protocol exists on an IEEE 802.3 LAN network to provide a means of exchanging addressing and naming information between nodes. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Proxy enabled (Y/N)`

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.

`Y` means this node may be a proxy server and to answer all proxy requests on the LAN. `N` means this node will ignore all proxy requests on the LAN.

Default value: N

Range: Y or N

`Probe requests retransmission maximum`

This is the maximum number of transmissions of probe requests (name requests and address requests) before a probe failure is reported. Because it is unlikely that probe-request data is lost, HP recommends that you keep the maximum number of retransmissions low.

Default value: 2

Range: 1–10

`Probe requests retransmission timeout (seconds)`

This field is for specifying the time limit between retransmissions of probe requests. This is the time interval in seconds 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: 1

Range: 1–10

`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 lost, HP recommends that you keep the maximum number of retransmissions low.

Default value: 2

Range: 1–10

`Proxy requests retransmission timeout (seconds)` The time interval in seconds 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: 4

Range: 1–10

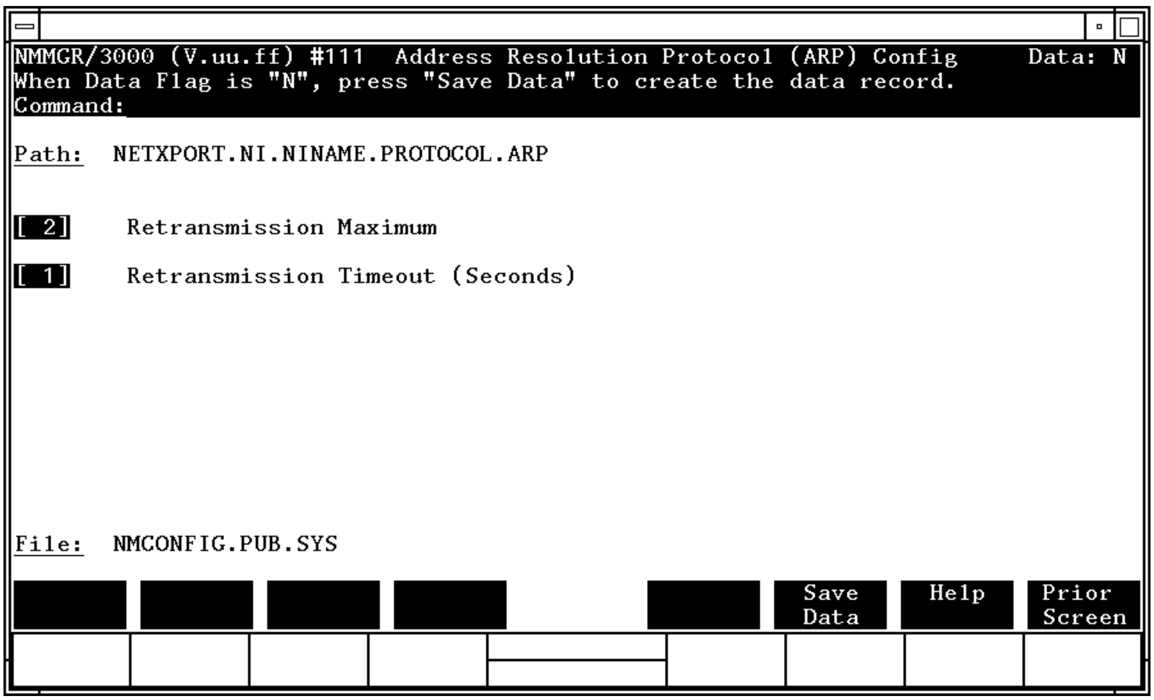
Address Resolution Protocol (ARP) Configuration

The Address Resolution Protocol (ARP) Configuration screen (#111) in Figure 5-7 is displayed when you press the **[Go To ARP]** function key at the Protocol configuration screen (Figure 5-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.ARP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI.

Figure 5-7 Address Resolution Protocol (ARP) Configuration Screen



This screen allows you to configure the information required for the address resolution protocol (ARP). The ARP protocol exists on an Ethernet LAN network to provide a means of exchanging addressing information between Ethernet nodes. With the concurrent configuration of IEEE 802.3 and Ethernet, both the probe and ARP protocols broadcast requests to all nodes on the LAN to resolve the LAN station address of a given remote node.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Retransmission maximum`

This is the maximum number of times that an ARP request packet will be retransmitted. If an ARP reply packet for this request is not received after this number of retransmissions, the attempted address resolution is considered to have failed. This value is bound closely to the retransmission timeout value as described. Taken together, they represent the total time to report an address resolution failure.

In general, the value of this field should be kept low.

Default value: 2

Range: 1–10

`Retransmission timeout (seconds)`

This is the time interval (in seconds) between ARP retransmissions. The value should be set large enough to avoid retransmissions in a temporarily overloaded environment, yet the value should be small enough to receive a timely failure report when a failure is inevitable.

Default value: 1

Range: 1–10

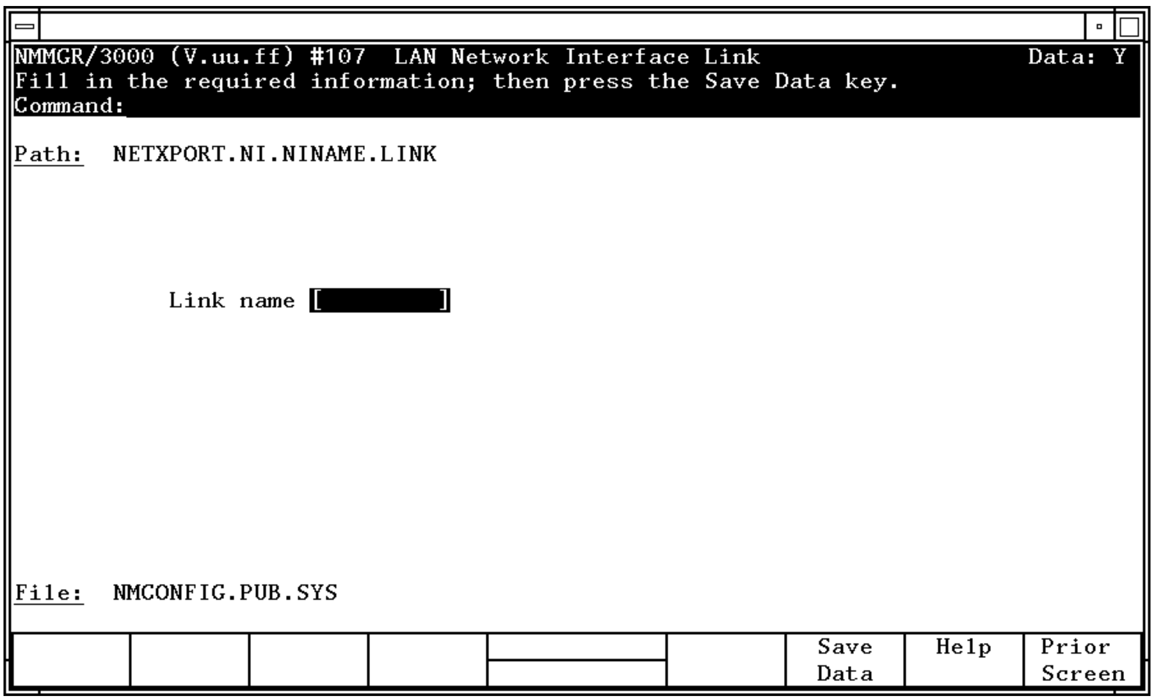
LAN Network Interface Link

The LAN Network Interface Link screen (#107) in Figure 5-8 is displayed when you press the **[Go To LINK]** function key at the LAN Network Interface Configuration screen (Figure 5-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI.

Figure 5-8 LAN Network Interface Link Screen



Use this screen to specify the link name for the NI. The link name is used by the network transport when establishing connections.

Fields

`Link name` Make sure this is the same link name configured at the LAN Link Configuration screen (path name `LINK`). Press the **[Save Data]** function key to save the link name in the configuration file. Verify that the link name has been configured by checking that the Data flag is set to `Y`.

This screen associates the link data with the LAN network interface data. The link name is used by the network transport when establishing connections. The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

To change an existing link name, enter the new name in the `Link name` field and press the **[Save Data]** function key.

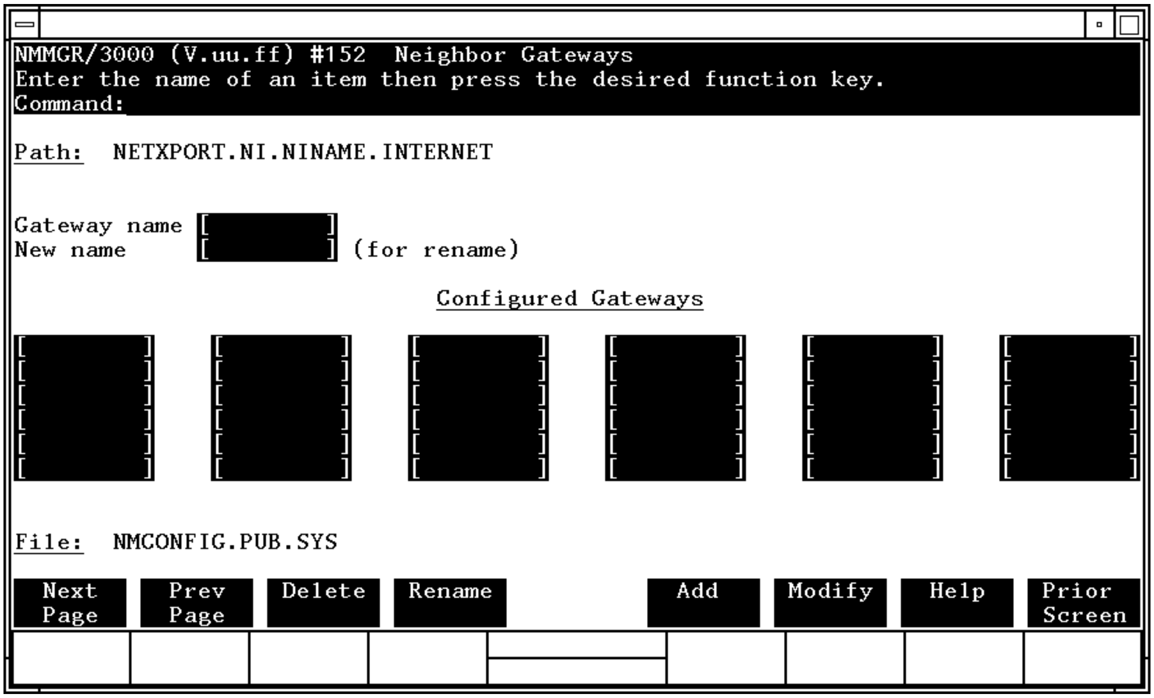
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 5-9 is displayed when you press the **[Go To INTERNET]** function key at the LAN Network Interface Configuration screen (Figure 5-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI.

Figure 5-9 Neighbor Gateways Screen



Use this screen, and the screens that follow it, to identify the gateways on this network. Use the fields and the function keys of this select screen to perform the desired action as follows:

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**
- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway, specify the gateway name and a new name; then press the **[Rename]** function key. 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, specify the gateway name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. 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 network numbers of all networks reachable from this gateway node.

Fields

`Gateway name` Enter a name to represent a gateway on this LAN 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 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.

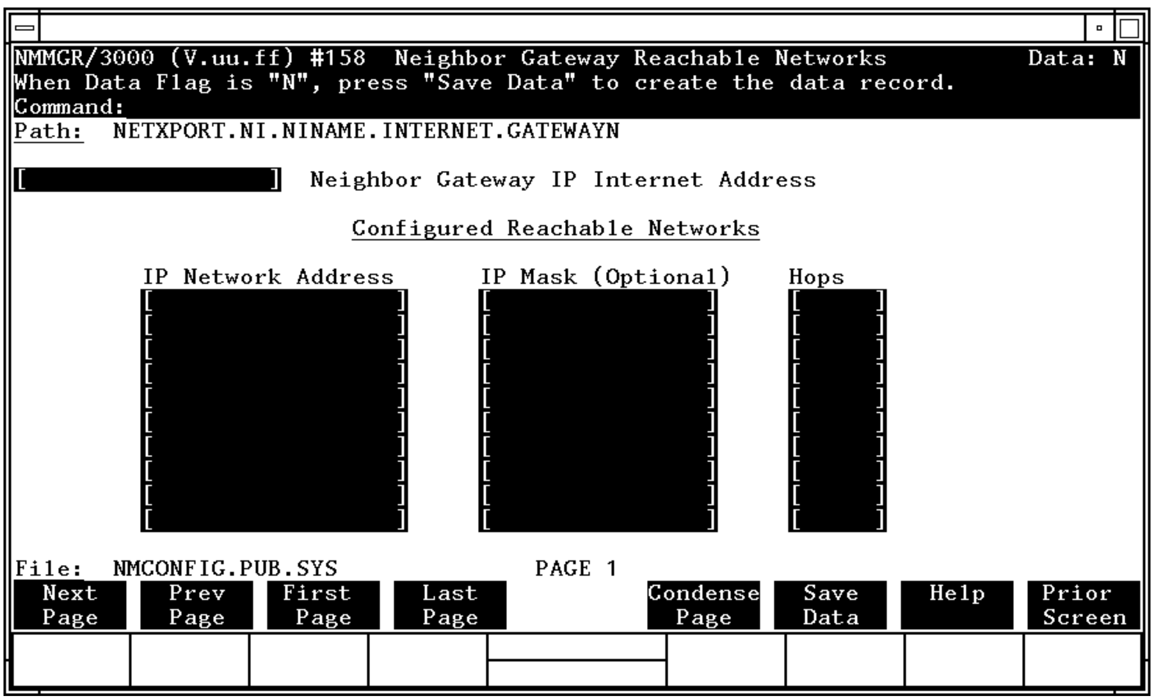
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 5-10 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 5-9) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.gatewayn`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured LAN NI, and *gatewayn* is the configured LAN NI gateway name.

Figure 5-10 Neighbor Gateway Reachable Networks Screen



After you have entered all the required data, press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE

The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 configured reachable networks. 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 internetwork 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; however, the node portion need not match.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The possible classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and xxx is a value ranging from 000 to 255, representing the node portion of the address. Note that network and node values of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:     192–223`

`Class B:     128–191`

`Class A:     001–126`

The network address (network portion of the IP address) configured in `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` must match the neighbor gateway IP internet address configured in the current screen.

Default value: None

`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.

You can also designate this gateway as a default gateway by entering an “at” sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask entered in the IP Protocol Configuration screen (Figure 5-5) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnetting.

Related screen:

- `NETXPORT.NI.`*`NIname`*`.INTERNET`

  This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask`

The IP mask identifies a portion of the IP address for subnets. The subnet is specified in the same format as an IP address; that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the *node* portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, the network transport will choose internally from among the routes with equal hop counts.

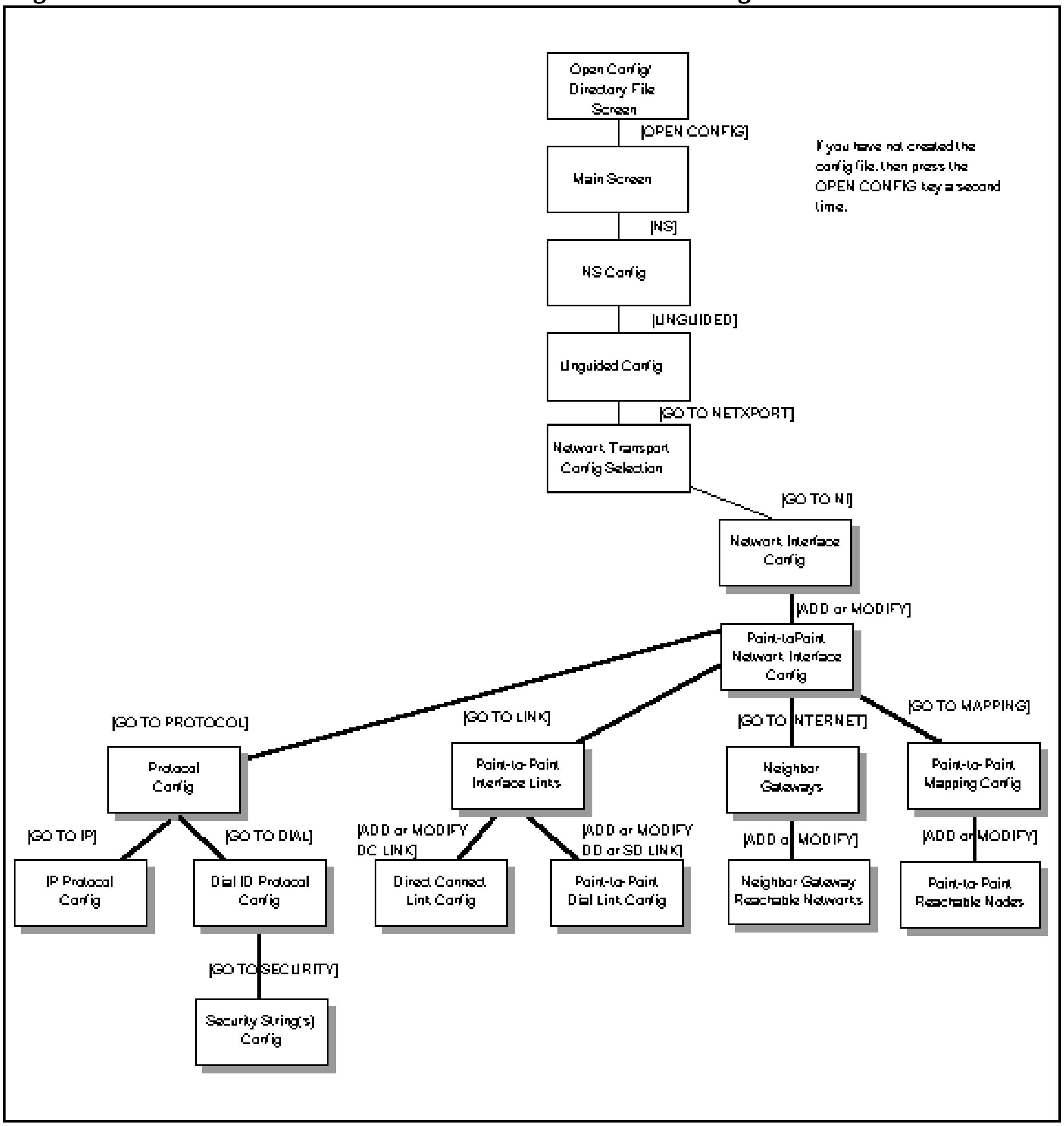
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

6 Point-to-Point (Router) Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring a Point-to-Point (router) network. The Point-to-Point Network Interface Configuration branch of NMMGR begins with a screen called the Network Interface Configuration screen. Figure 6-1 shows the screen flow for configuring the Point-to-Point (router) screens. Screens unique to Point-to-Point are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 6-1 Point-to-Point Network Interface Configuration Screen Flow



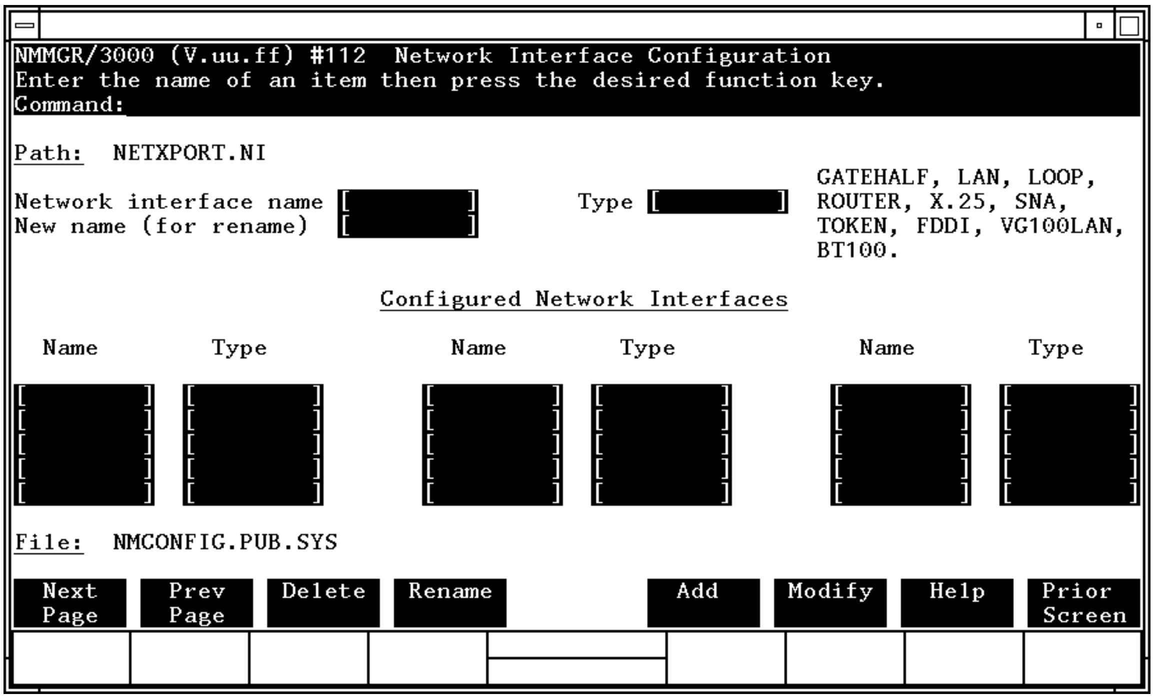
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 6-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

```
@NETXPORT.NI
```

in the Command window of any screen and press the **[Enter]** key.

Figure 6-2 Network Interface Configuration Screen



Use the fields and function keys of the select screen to perform the desired action.

- To define a new point-to-point NI configuration, specify the NI name and the NI type ROUTER; then press the **[Add]** function key. The path for the selected NI name is added to the configuration file, and the data screen on that path is displayed. **Up to 12 NI's are supported per system (one NI must be used for loopback)**.
- To modify an existing NI configuration, specify the NI name; then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) is deleted and is no longer displayed in a display field under the label Configured Network Interfaces.

The network interface provides the interface between network transport protocols and link protocols. It also provides the software loopback capability.

Fields

`Network interface name` Enter the network interface name for the point-to-point (router) interface.

The network interface name can contain as many as eight characters. The first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, FDDI, 100VG-AnyLAN or 100Base-T)` **(Required only when adding an NI.)** If you are configuring a point-to-point NI, select ROUTER.

`New name` **(Required only when renaming an existing NI.)** Enter the name you want to change in the network interface name field. Enter a new NI name in the new name field. Press the Rename function key.

The new name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

Point-to-Point Network Interface Configuration

The point-to-point network interface (NI) allows the upper layers of the transport protocol to communicate with the data link layer. The Point-to-Point Network Interface Configuration screen (#101) in Figure 6-3 is displayed when you select an NI name of NI type ROUTER at the Network Interface Configuration screen (Figure 6-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI.

Figure 6-3 Point-to-Point Network Interface Configuration Screen

```
NMMGR/3000 (V.uu.ff) #101 Point-to-Point Network Interface Config      Data: N
When Data Flag is "N", press "Save Data" to create the data record.
Command:

Path:  NETXPORT.NI.NINAME

[     ]   Network Hop Count

[      ]  Idle Device Timeout Value (Seconds)
             0 = Timer Disabled for All Devices

[128  ]   Number of Outbound Buffers





File:  NMCONFIG.PUB.SYS

 Go To    Go To    Go To    Go To                      Save     Help    Prior
PROTOCOL   LINK   INTERNET MAPPING                     Data            Screen
```

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`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

`Idle device timeout value (seconds)`

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.” The purpose of the idle device timer is to shut down dial links that have become idle.

Related screens:

- NETXPORT.NI.*NIname*.LINK.*linkname*

  An entry in this screen enables/disables the idle device timer.

- 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.

  Default value: None

  Range: 0–32400

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Overallocation may waste core memory.

Related screen:

- `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: 128

  Range: 32–2048

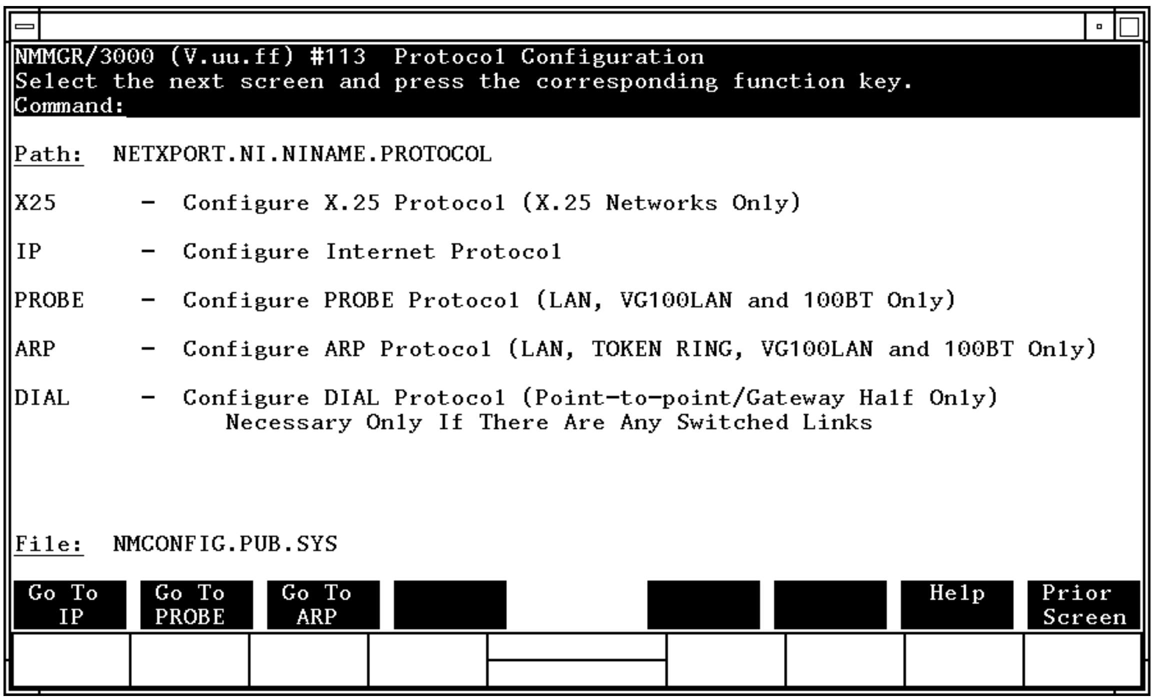
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 6-4 is displayed when you press the **[Go To PROTOCOL]** function key at the Point-to-Point Network Interface Configuration screen (Figure 6-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point (router) NI name.

Figure 6-4 Protocol Configuration Screen



For a point-to-point NI, you must configure the IP protocol. The Dial protocol must be configured if you have switched lines.

Choose the protocol to configure and press the corresponding function key.

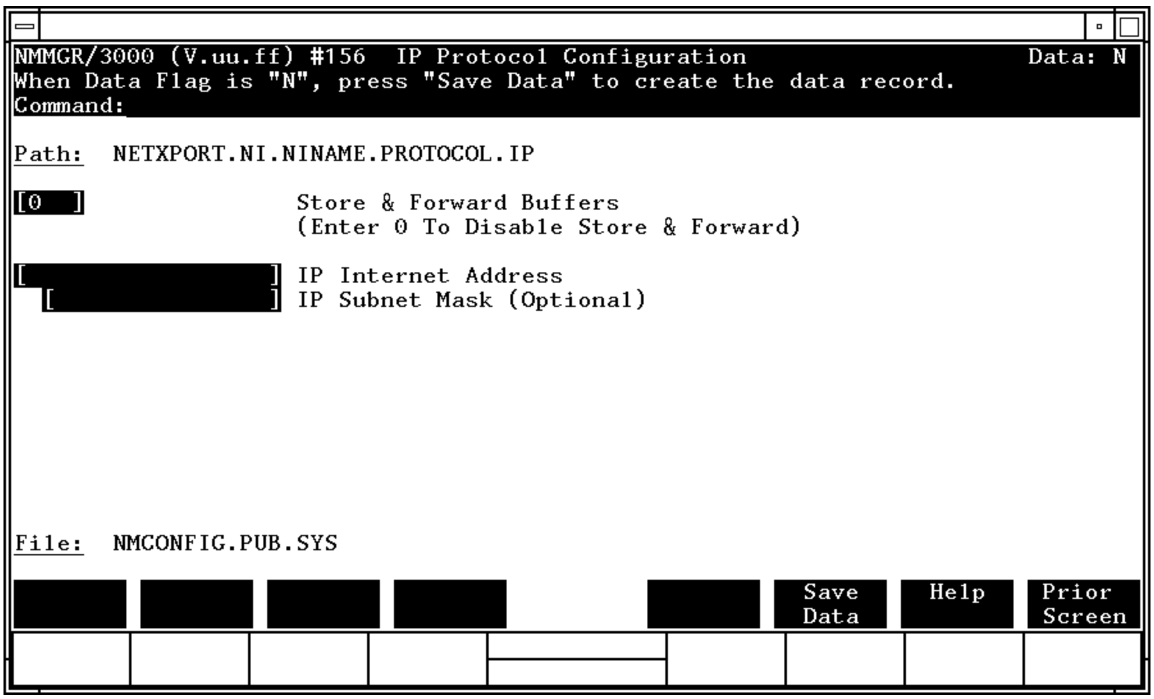
Internet Protocol Configuration

Internet protocol information must be supplied for each configured NI. The key field in the IP Protocol Configuration screen (#156) shown in 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 Configuration screen is displayed when you press the function key for **[Go To IP]** at the Protocol Configuration screen (Figure 6-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI.

Figure 6-5 IP Protocol Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

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 you are configuring a non-gateway node on this network. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface. You can modify the number of store-and-forward buffers to allow performance tuning for different network types. However, HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

If store-and-forward is to be disallowed, set this number to 0.

Default value: 0

Range: 0–50

NOTE If this is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:      C nnn.nnn.nnn xxx
```

`Class B:     B nnn.nnn xxx.xxx`

`Class A:     A nnn xxx.xxx.xxx`

where *xxx* is a value ranging from 000 to 255, representing the node portion of the address and *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address. Note the network and node values of all zeros or all ones are not allowed. These are special value. The leftmost group of *nnn* has the following ranges for each address class:

`Class C:     192–223`

`Class B:     128–191`

`Class A:     001–126`

Default value: None

`IP subnet mask`

The IP subnet mask masks a portion of the IP address for subnets. The subnet is specified in the same format as an IP address; that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. for example, a mask for a class A address with the subnet field being the first 8 bits of the node portion would be expressed as 255 255.000.000. The defaul is no IP mask.

Refer to the *HP 3000/iX Netowrk Planning and Configuration Guide* for more details on subnets.

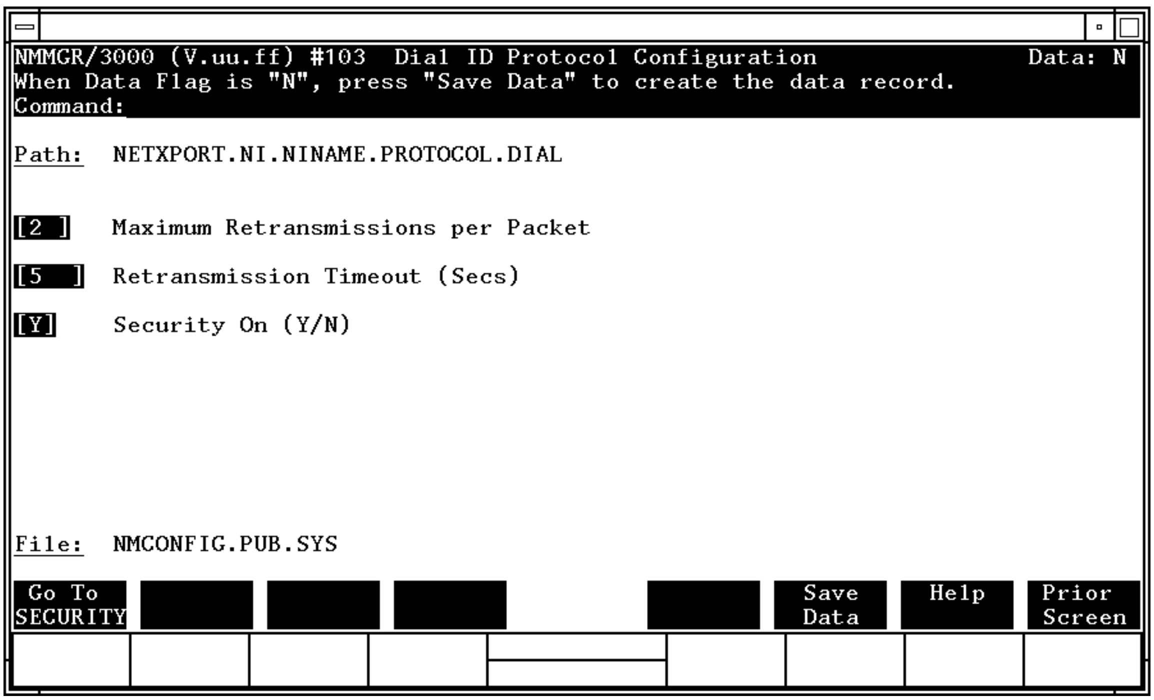
Dial ID Protocol Configuration

Along with other information, the Dial ID Protocol Configuration screen (#103) provides a means of verifying that the remote node is the intended remote node and that both local and remote nodes have proper security access. This screen, shown in Figure 6-6, is displayed when you press the function key for **[Go To DIAL]** at the Protocol Configuration screen (Figure 6-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.DIAL`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is the configured point-to-point NI.

Figure 6-6 Dial ID Protocol Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. 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.

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 connection is closed.

This value is related to the retransmission timeout value discussed.

Multiplying these values results in the total time that passes before a failure is reported (an error message is recorded when the timer expires). HP recommends that you alter this value only upon the recommendation of your HP representative. The higher the value, the longer it will take to be notified of a link failure if one occurs. The dial ID protocol is in use after the physical and data link levels have been activated and before normal communication 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. 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”). 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.

If security validation fails, an error message is logged, where `PARM` indicates if the failure was local or remote. (See the *NS 3000/iX Error Messages Reference 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

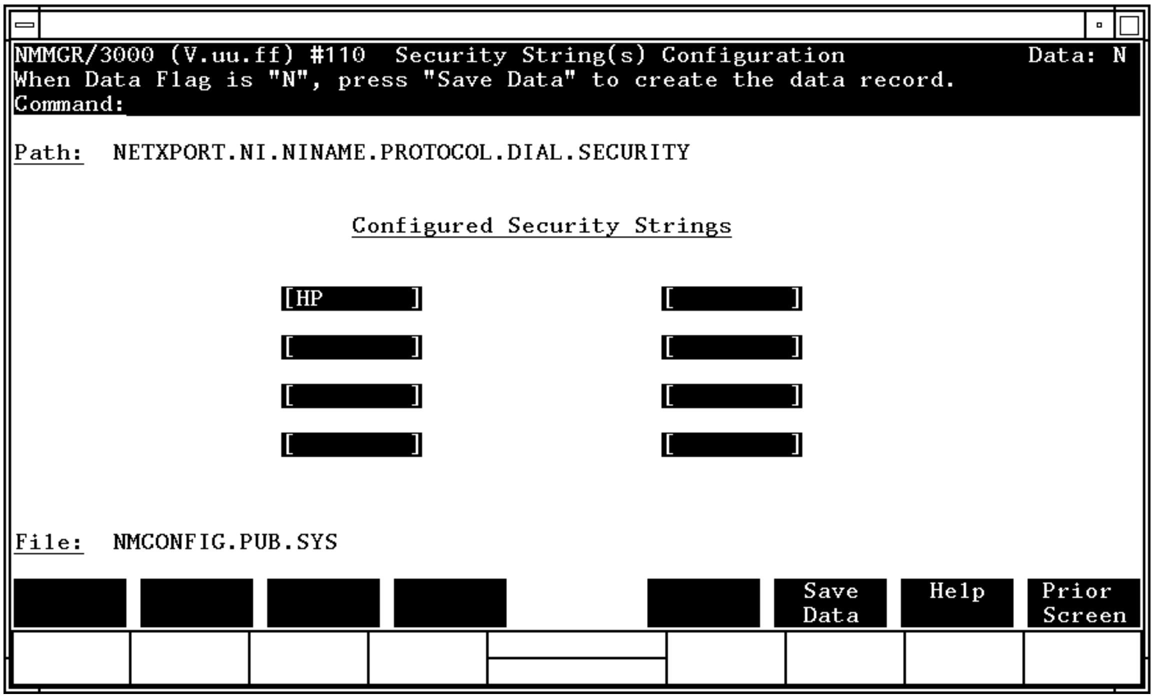
Security String(s) Configuration

The Security String(s) Configuration screen (#110) 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 6-7, is displayed if you pressed the **[Go To Security]** function key at the preceding Dial ID Protocol Configuration screen (Figure 6-6). It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.PROTOCOL.DIAL.SECURITY

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI.

Figure 6-7 Security String(s) Configuation Screen



Press the **[Save Data]** function key 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.

Fields

`Configured security strings`

Enter the security string that the 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. To delete a security string, blank out the field that contains the string you want deleted, then press the **[Save Data]** function key.

Default value: HP

Related screen:

- `NETXPORT.NI.`*`NIname`*`.LINK.`*`linkname`*

  The dial IP protocol is enabled or disabled on this screen.

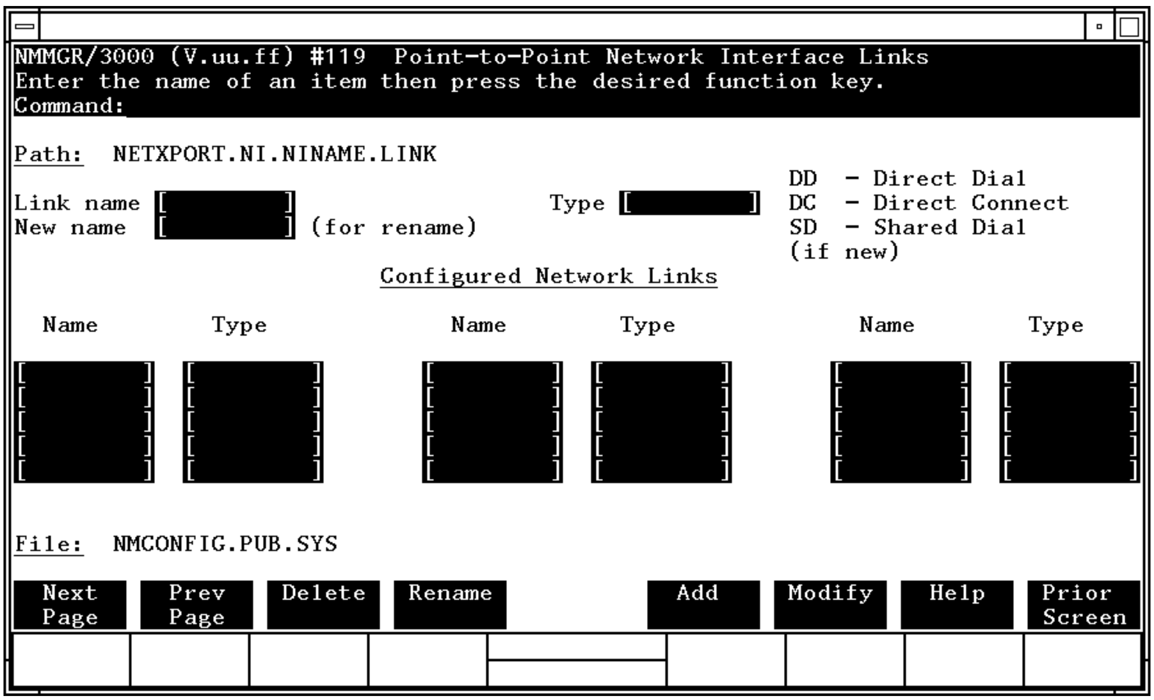
Point-to-Point Network Interface Links

The Point-to-Point Network Interface Links screen (#119) in Figure 6-8 is displayed when you press the **[Go To LINK]** function key at the Point-to-Point Network Interface Configuration screen (Figure 6-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI.

Figure 6-8 Point-to-Point Network Interface Links Screen



- To define a new NI link configuration, specify the link name and link type; then press the **[Add]** function key. The path for the selected link name is added to the configuration file, and the data screen on the path is displayed. **Up to 40 network links are supported per Router NI.**
- To modify an existing NI link configuration, specify the link name; then press the **[Modify]** function key. The data screen on the path for the specified link is displayed.

- To change the link name of an existing NI link configuration, specify the link name and a new name; then press the **[Rename]** function key. 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 NI link configuration, specify the link name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Network Links.

Fields

`Link name` Enter the same link name that you entered in the Link Configuration: LAP-B Link Data screen (Figure 3-4) for this node. This enables network transport to associate the correct link with this point-to-point NI. The link name is used by network transport when establishing connections.

The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

Related screens:

- `LINK.`*`linkname`*

  The link name of type LAP-B specified in this screen for this node must match the link name in this Point-to-Point Network Interface Link screen.

- `NETXPORT.NI.`*`NIname`*`.MAPPING.`*`mapentry`*

  This screen specifies which link to use to reach a specific node on the point-to-point network. The link specified must be one entered on the current screen.

`Type` Enter `DD`, for “direct dial,” if this is a dial link that provides a connection to a single remote system over a phone line. For direct dial links, the phone number dialed by the local node to reach the remote node never changes.

Enter `SD`, for “shared dial,” if this is a dial link that provides connection to more than one remote system. Such a link is said to be shared by more than one remote node, though the connection may only be to one remote node at a time. If you choose shared dial, no other nodes can be accessed through the remote host; it is an end point in the connection.

Enter `DC`, for “direct connect,” if this is a non-switched point-to-point link (a private line, leased line, or hardwired connection).

Related screen:

- `NETXPORT.NI.`*`NIname`*`.MAPPING.`*`mapentry`*

  This screen allows up to 1024 mappings of point-to-point 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 an existing point-to-point link.)** Enter a link name. This new link name is used in place of the current link name for an existing link configuration. Remember, the link name must be the same as the link name configured in the Link Configuration: LAP-B Link Data screen.

The name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

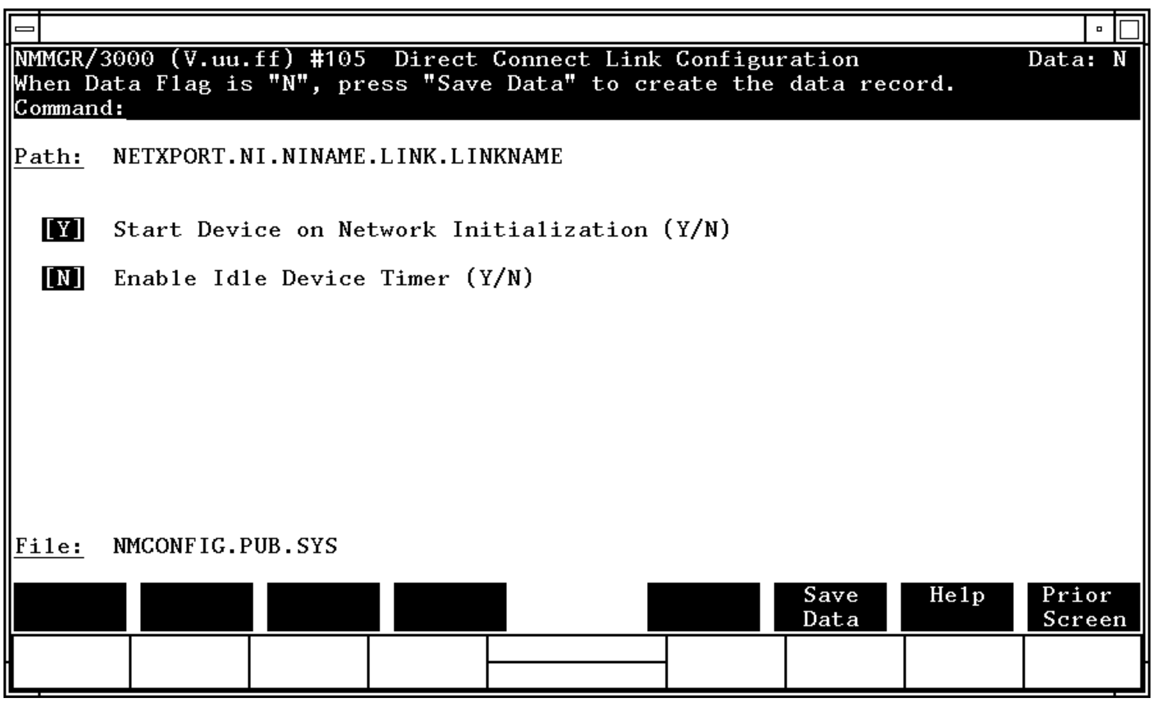
Direct Connect Link Configuration

The Direct Connect Link Configuration screen (#105) supplies the information required to interface a point-to-point NI to a direct-connect link (that is, a private line, leased line or other non-switched link). This screen, shown in Figure 6-9, is displayed when you select an NI link name and the link type DC at the Point-to-Point Network Interface Links screen (Figure 6-8) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK.`*`linkname`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI, and *linkname* is a configured point-to-point NI link.

Figure 6-9 Direct Connect Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Start device on network initialization (Y/N)`

A `Y` (Yes) value means that the device is to begin startup when a **`NETCONTROL START`** command is issued for the network interface being configured. The physical layer is activated when **`NETCONTROL START`** is issued, but the data link layer on the first remote device is not activated until the first **`REMOTE HELLO`** using that device is issued. An `N` (No) means that a **`NETCONTROL ADDLINK`** command must be used to start the device. For more information on these commands, refer to the *NS 3000/iX Operations and Maintenance Reference Manual*.

Default value: Y

Range: Y or N

`Enable idle device timer (Y/N)`

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 as listed.

Related screen:

- `NETXPORT.NI.`*`NIname`*

  The idle device timeout value is configured on this screen.

Default value: N

Range: Y or N

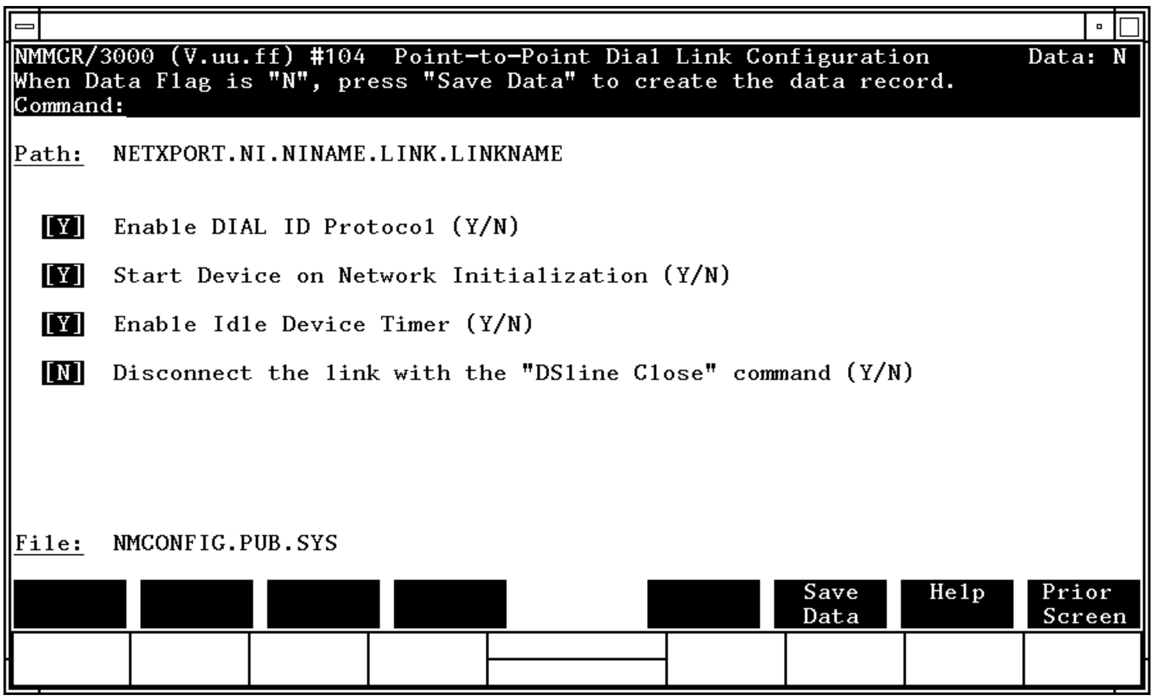
Point-to-Point Dial Link Configuration

Dial link configuration provides the information necessary to interface the point-to-point NI to a dial link. The Point-to-Point Dial Link Configuration screen (#104), shown in Figure 6-10, is displayed when you select an NI link name and link type DD or link type SD at the Point-to-Point Network Interface Links screen (Figure 6-8) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK.`*`linkname`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI, and *linkname* is a configured point-to-point NI link.

Figure 6-10 Point-to-Point Dial Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Enable dial ID protocol (Y/N)`

(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 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.`*`mapentry`*

  Configures information about reachable point-to-point 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 begin startup when a **`NETCONTROL START`** command is issued for this network interface. The physical layer is activated when **`NETCONTROL START`** is issued, but the data link layer of the first remote device is not activated until the first **`REMOTE HELLO`** using that device is issued. An `N` (No) means that a **`NETCONTROL ADDLINK`** command must be used to start the device. For more information on these commands, refer to the *NS 3000/iX Operations and Maintenance Manual*.

Default value: Y

Range: Y or N

`Enable idle device timer (Y/N)`

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 point-to-point NI screen (see “Related screens”).

Related screen:

- `NETXPORT.NI.`*`NIname`*

  Configures point-to-point network interface information. The value for idle device timeout is configured on this screen.

Default value: Y

Range: Y or N

`Disconnect the link with the DSline Close command (Y/N)`

A `Y` (Yes) value means that NS will immediately disconnect the dial phone line when the last user enters a **`DSLINE`** ***`nodename`*****`;CLOSE`** command. NS keeps track of the number of times the **`DSLINE`** ***`nodename`*** command is issued by all users on the system. When the **`DSLINE`** ***`nodename`*****`;CLOSE`** command has been issued this same number of times, NS checks to see if the dial line to the remote node is still connected and if there are any TCP connections still using the line. If the line is connected and there are no TCP connections, NS disconnects the line.

An `N` (No) value means that the dial phone line will remain connected until the idle device timer expires.

Default value: N

Range: Y or N

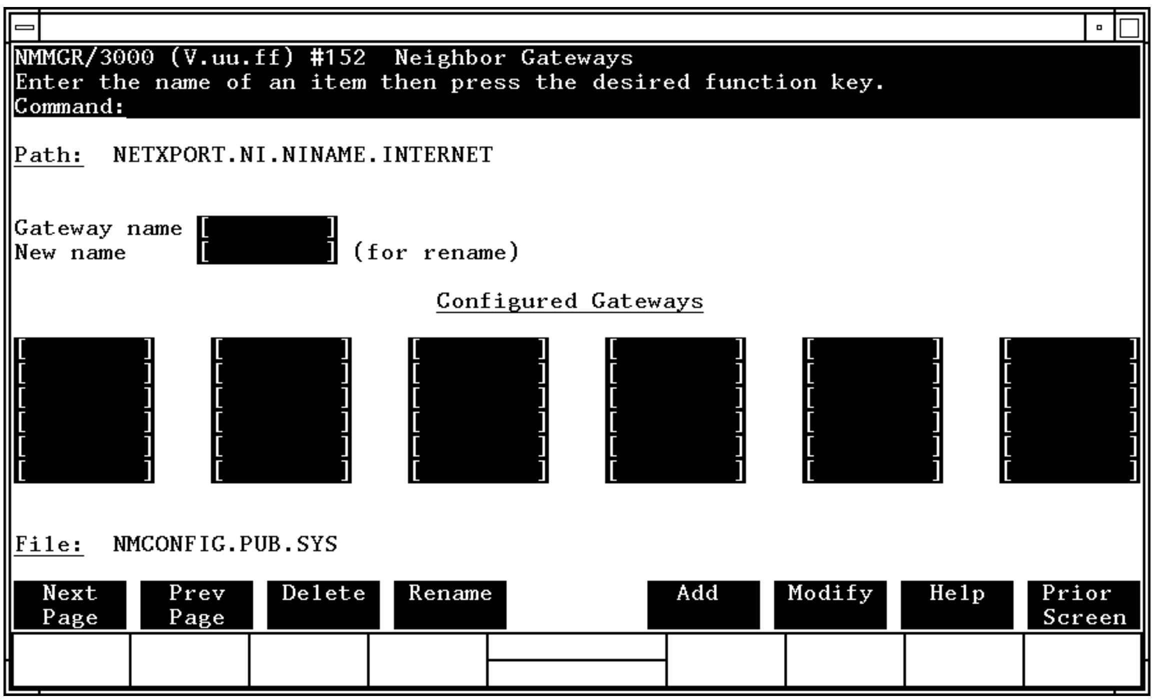
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 6-11 is displayed when you press the **[Go To INTERNET]** function key at the Point-to-Point Network Interface Configuration screen (Figure 6-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the Command window of any screen and press the **[Enter]** key, where the *NIname* is a configured point-to-point NI.

Figure 6-11 Neighbor Gateways



Use this screen, and the screens that follow it, to identify the gateways on this network. Use the fields and the function keys of this select screen to perform the desired action as follows:

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **Up to 164 gateways are supported per link.**
- To modify an existing gateway identification, specify the gateway name, then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway identification, specify the gateway name and a new name; then press the **[Rename]** function key. 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 identification, specify the gateway name, then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Gateways.

Fields

`Gateway name` Enter a name to represent a gateway node on this point-to-point 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 a gateway.)** Enter a name to represent a gateway node on this point-to-point 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.

Neighbor Gateway Reachable Networks

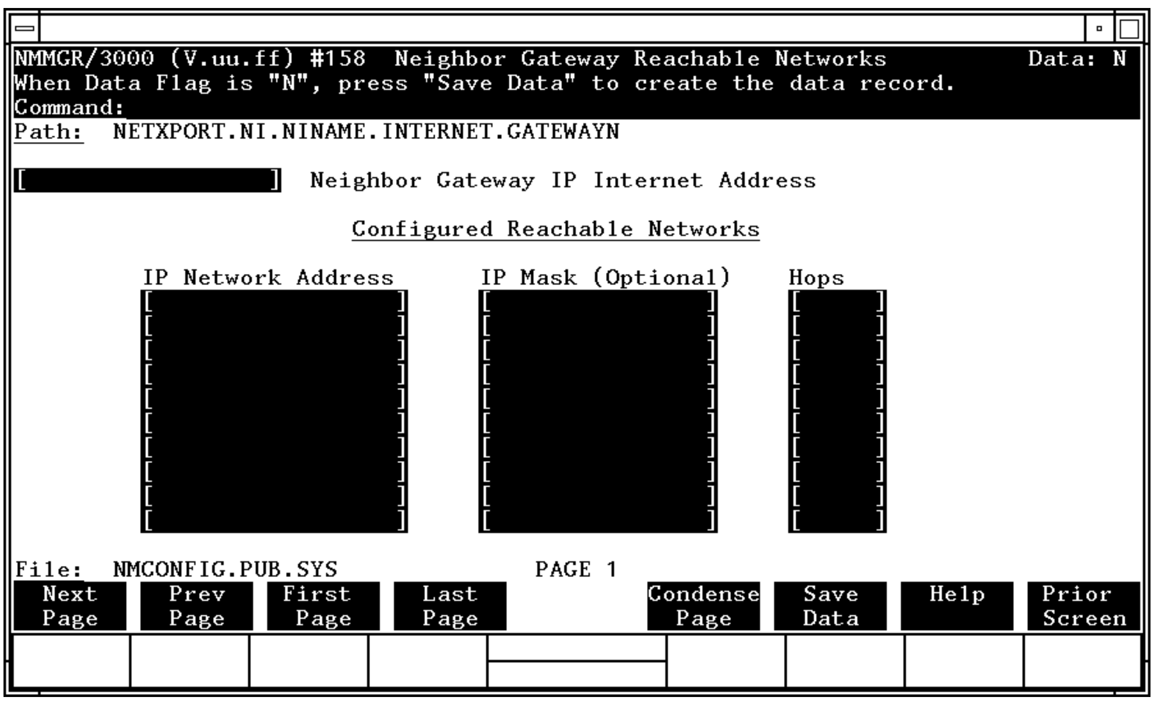
The Neighbor Gateway Reachable Networks screen (#158) is used to enter internet routing information. It supplies the internet address of a neighbor internet gateway, lists addresses of remote networks which are reachable through that gateway, and indicates the distances to those remote networks. A neighbor gateway is a gateway node that belongs to the same network as the node you are configuring. This means that the network portion of the internet address for the gateway is the same as the network portion of the address you entered for the network interface you are configuring.

The screen, shown in Figure 6-12, is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 6-11) and press the **[Add]** or **[Modify]** function keys. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.`*`gatewayn`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured point-to-point NI, and *gatewayn* is the configured point-to-point NI gateway name.

Figure 6-12 Neighbor Gateway Reachable Networks Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 internetwork 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”).

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The possible classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx

Class B:     B nnn.nnn xxx.xxx

Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing node portion of the address. Note the network and node portions of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:    192–223`

`Class B:    128–191`

`Class A:    001–126`

Default value: None

Related screen:

- `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.

You can also designate this gateway as a default gateway by entering an “at” sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP Mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask configured in the IP Protocol Configuration screen (Figure 6-5) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnets.

Related screen:

- `NETXPORT.NI.`*`NIname`*`.INTERNET`

  This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask` The IP mask masks a portion of the IP address for subnets. The subnet is specified in the same format as an IP address; that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the *node* portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, 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 the **[Save Data]** function key.

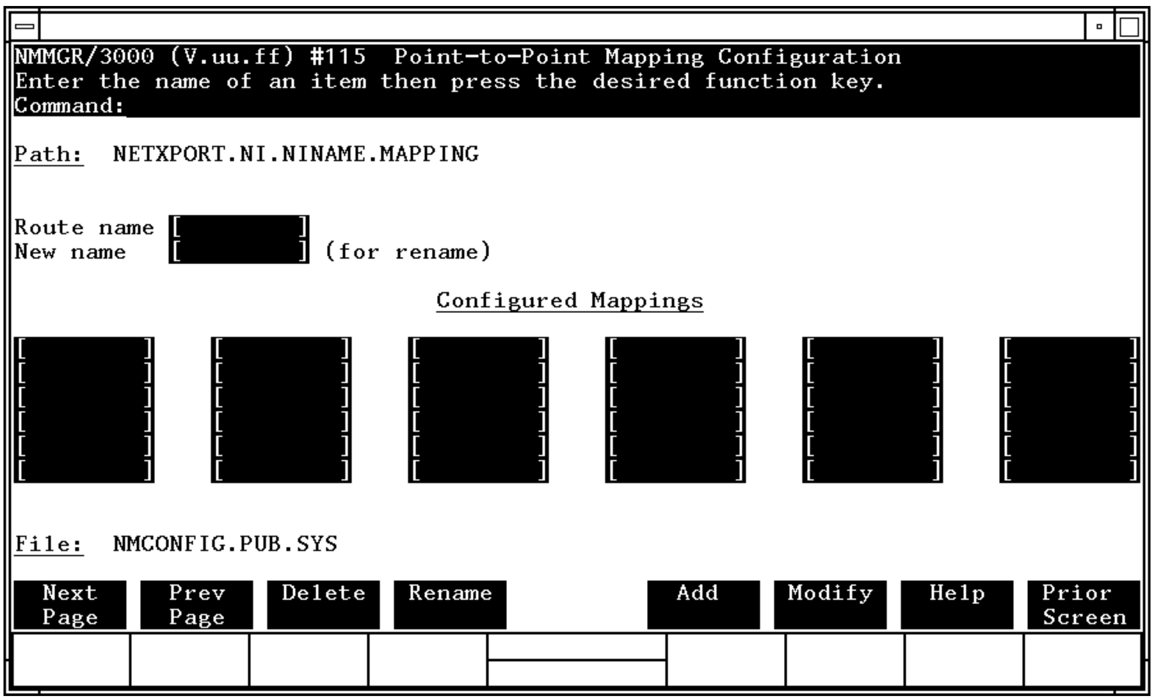
Point-to-Point Mapping Configuration

The Point-to-Point Mapping Configuration screen (#115) in Figure 6-13 is displayed when you press the **[Go To MAPPING]** function key at the Point-to-Point Network Interface Configuration screen (Figure 6-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.MAPPING`

in the Command window of any screen and press the **[Enter]** key, where the *NIname* is a configured point-to-point NI.

Figure 6-13 Point-to-Point Mapping Configuration Screen



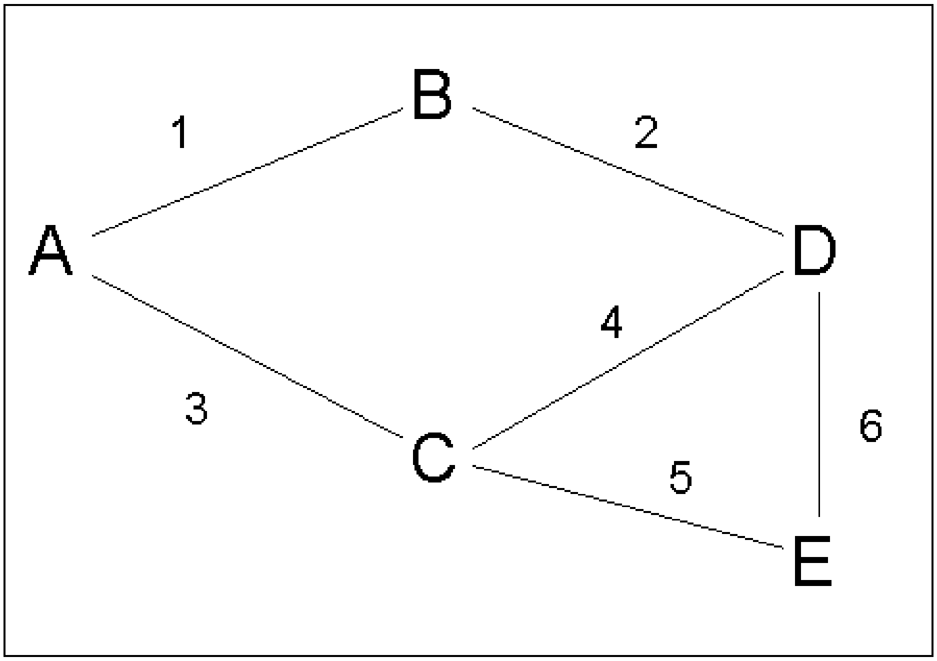
The screen following this one allows you to configure a set of characteristics for a route from the local node to a remote node.

Mapping is creating a route from this node to any other node in the network. You create routes by first assigning a name to each possible route from this node. Then you create routes to adjacent and remote nodes by identifying the adjacent or remote node's IP address and which link is used to reach the node.

12 router NI's are supported per system, depending on the number of available hardware slots (one NI must be used for loopback). Each router can have up to 1024 mappings. However, 4096 is the absolute maximum number of unique phone numbers supported per NMCONFIG File.

There may be multiple routes to a destination node; if the routes are through different adjacent nodes, a mapping may be configured for each of them. For example, Figure 6-14 shows a point-to-point network that could have eight mappings configured for node A.

Figure 6-14 Configured 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. 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 you do not need 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 provide alternate paths if the link used for the primary route fails.

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 (in the route name field) and press the **[Add]** function key. The path for the selected route is added to the configuration file, and NMMGR displays a mapping data screen (called the Point-to-Point 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 (route name) and press the **[Modify]** function key. NMMGR displays the Point-to-Point Reachable Nodes screen with the data corresponding to the specified route name.
- To change the name of an existing mapping configuration, specify the existing route name and a new name and press the **[Rename]** function key. The previously configured name is replaced, and the new name is displayed under the heading “Configured Mappings.”
- To delete an existing mapping configuration, specify the existing route name and press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured name is deleted and is no longer displayed in a field under the heading “Configured Mappings.”

Fields

`Route name` — Enter a name to represent a route between the node you are configuring and another node on the point-to-point network. This name can contain as many as eight alphanumeric characters; the first character must be alphabetic. To help keep track of routes you can use the destination node name as the route name. If you have more than one route to a given node, you can name the routes *nodename1*, *nodename2*, and so forth.

`New name` — **(Required only when renaming a route.)** Enter a new route 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. The first character must be alphabetic.

Point-to-Point Reachable Nodes

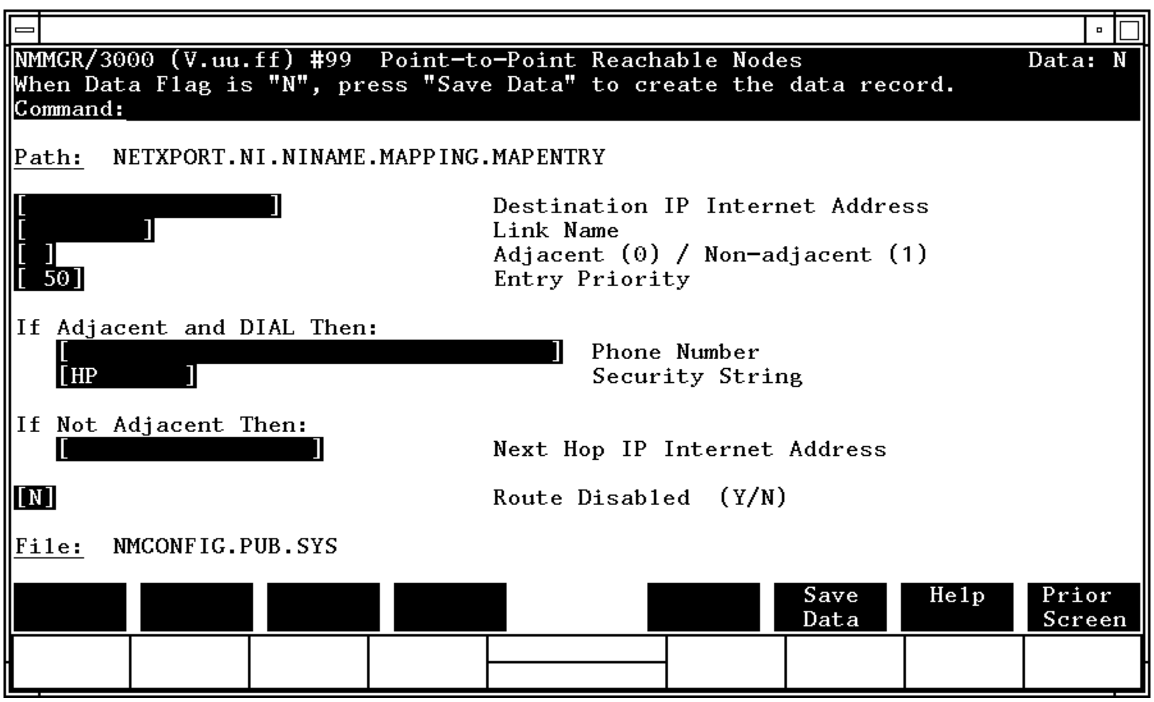
The Point-to-Point Reachable Nodes screen (#99) shown in Figure 6-15 is used to configure the route characteristics to a destination node on the point-to-point network. You must configure one mapping (i.e., one entry in this screen) for each node that you want to reach. The name of the link connecting 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 completed at least as many times as there are other nodes in the point-to-point network. 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.

The screen shown is displayed when you select a route name at the Point-to-Point Mapping Configuration screen (Figure 6-13) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.MAPPING.*mapentry*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is the configured point-to-point NI name, and *mapentry* is a configured route name.

Figure 6-15 Point-to-Point Reachable Nodes Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Destination IP internet address`

This is the internet address of the destination node to which a route is being defined.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms (note the spaces must appear where indicated):

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing node portion of the address. Note the network and node values of all zeros are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

```
Class C:     192–223
Class B:     128–191
```

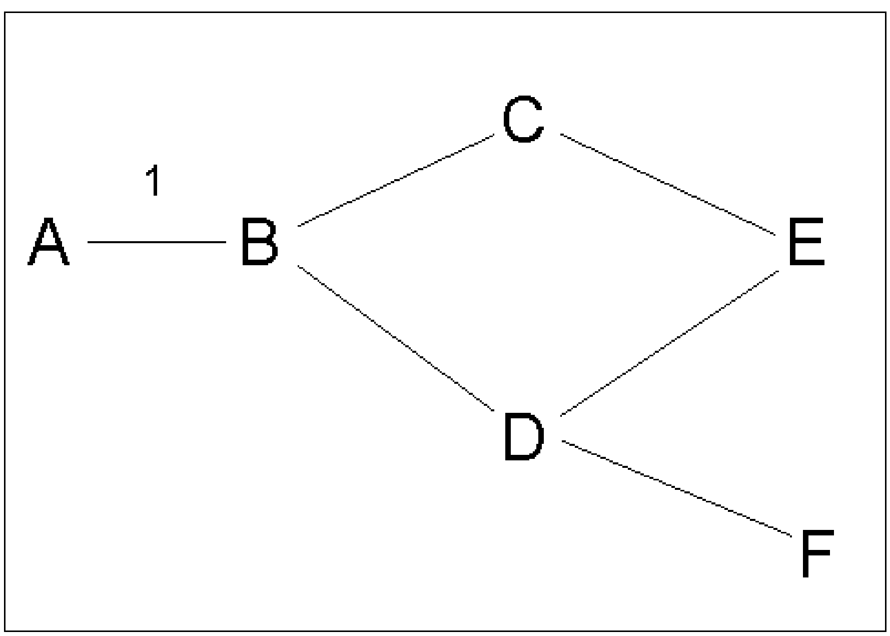
Class A: 001–126

If the link specified in the Link Name field is the only link configured for this network interface and is not a shared dial link, 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 point-to-point nodes on this network can be reached via the link specified in the link name field. (Non-adjacent links are not allowed to use a shared dial link.) 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 6-16 shows a point-to-point 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, one mapping would have to be configured at node A: the mapping from node A to the adjacent node B.

Default value: None

Figure 6-16 Using an @ for Mapping Configuration



`List 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).

Related screens:

- `NETXPORT.NI.`*`NIname`*`.LINK`

  This screen configures the link name.

- `LINK.`*`linkname`*

  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 point-to-point 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.

You can have 4096 unique phone numbers in your NM configuration file.

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.`*`linkname`*

  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

`Next hop IP internet address`

This parameter specifies the correct path for a message to take when there is more than a single hop between the sending node and the destination.

Default value: None

`Route disabled (Y/N)`

Use this field to disable routing to the remote node. Disabling routing might be useful if you are testing another link and want to temporarily disable this one.

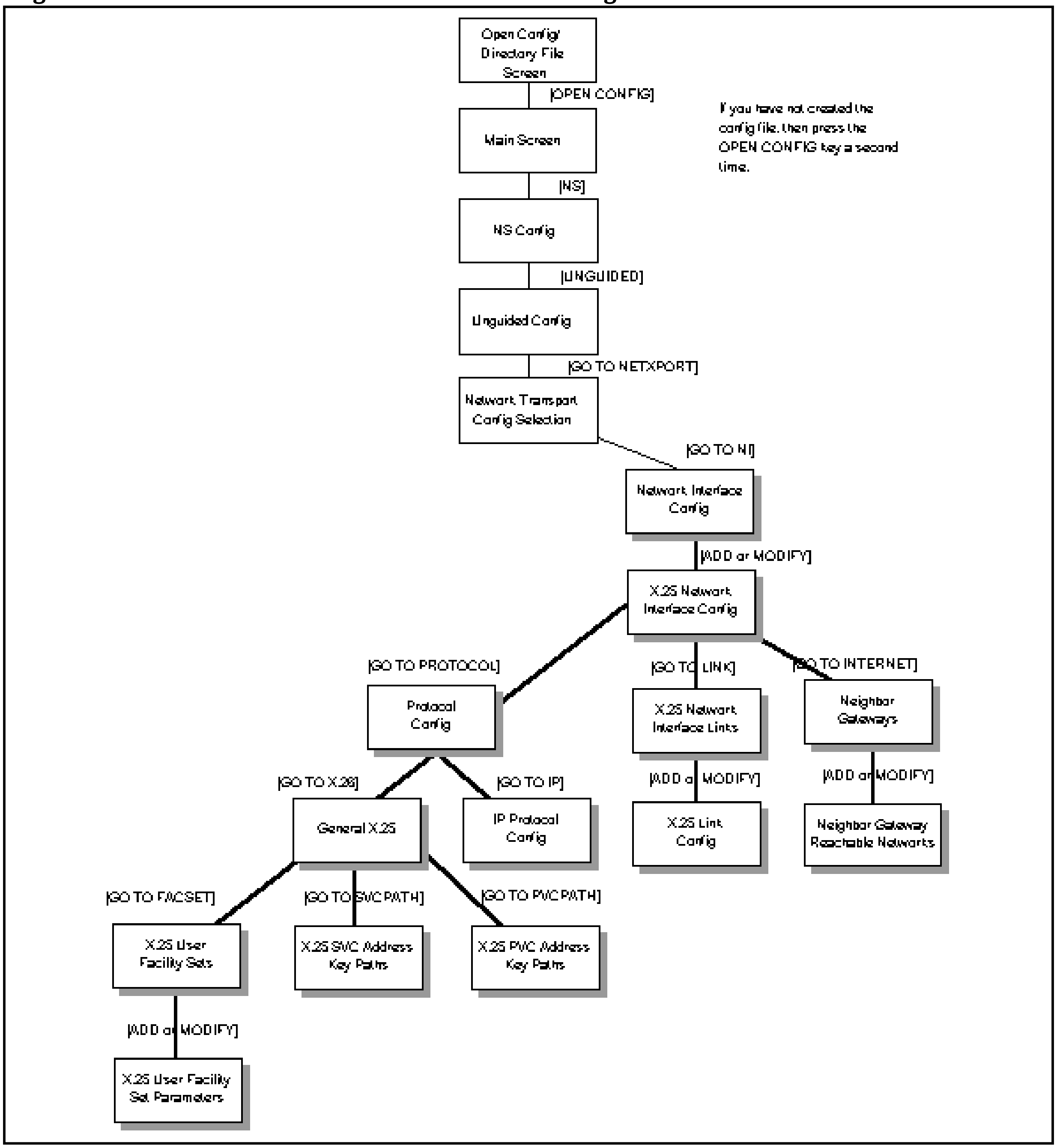
Default value: N

Range: Y or N

7 X.25 Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring an X.25 network. The X.25 Network Interface Configuration branch of NMMGR begins with a screen called the Network Interface Configuration screen. Figure 7-1 shows the screen flow for configuring the X.25 screens. Screens unique to X.25 are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 7-1 X.25 Network Interface Configuration Screen Flow



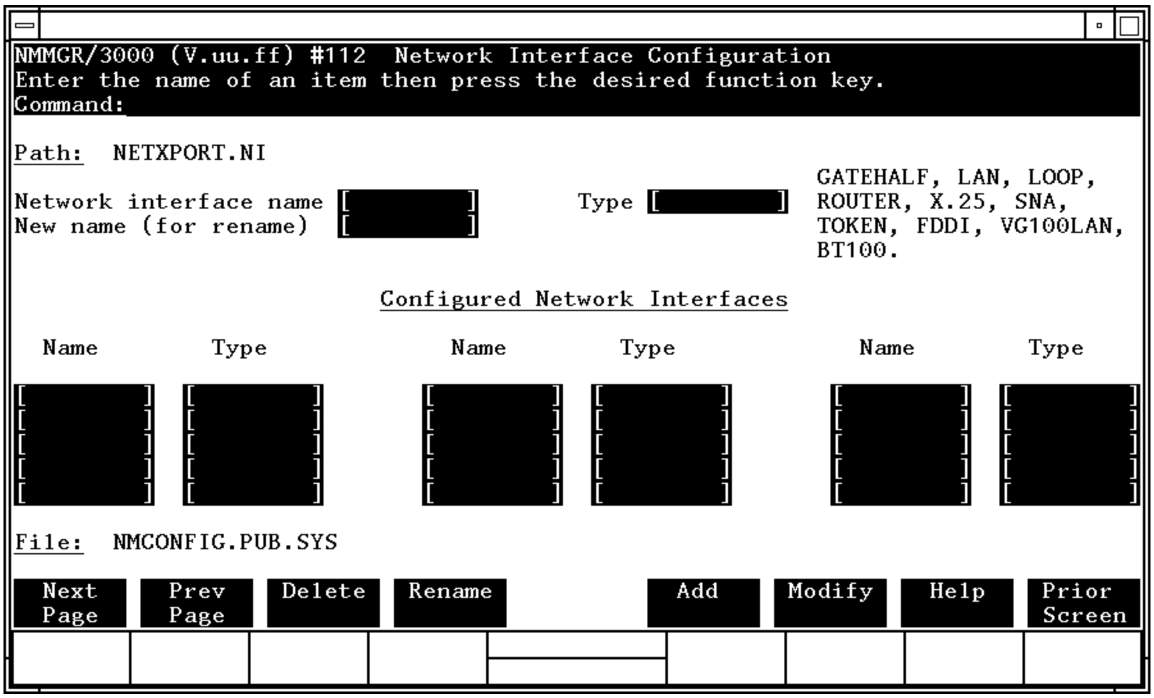
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 7-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

```
@NETXPORT.NI
```

in the Command window of any screen and press the **[Enter]** key.

Figure 7-2 Network Interface Configuration Screen



Use the fields and the function keys of the select screen to perform the desired action.

- To define a new X.25 NI, specify an NI name and NI type `X.25`; then press the **[Add]** function key. The path for the selected NI name is added to the configuration file and the next screen for configuring an X.25 NI is displayed. **You may configure up to 12 NI's per system (one NI must be used for loopback).**
- To modify an existing NI, specify the NI name and press the **[Modify]** function key. The next screen is displayed with the configuration data for that NI.

- To change the name of an existing NI configuration, specify the NI name and a new name; then press the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) is deleted and is no longer displayed in a display field under the label Configured Network Interfaces.

The network interface provides the interface between the network transport protocols and the link protocols. It also provides software loopback capability.

Fields

`Network interface name` **(Required.)** This is the name of the network interface you wish to configure. The name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

Default value: None.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN,FDDI, 100VG-AnyLAN, or 100Base-T` This field is required if you are adding a network interface. If you are configuring an X.25 NI, select `X.25`.

`New name` **(Required only when you are renaming an existing network interface.)** Enter the current name in the network interface name field. Enter the new name in the new name field. Press the **[Rename]** function key.

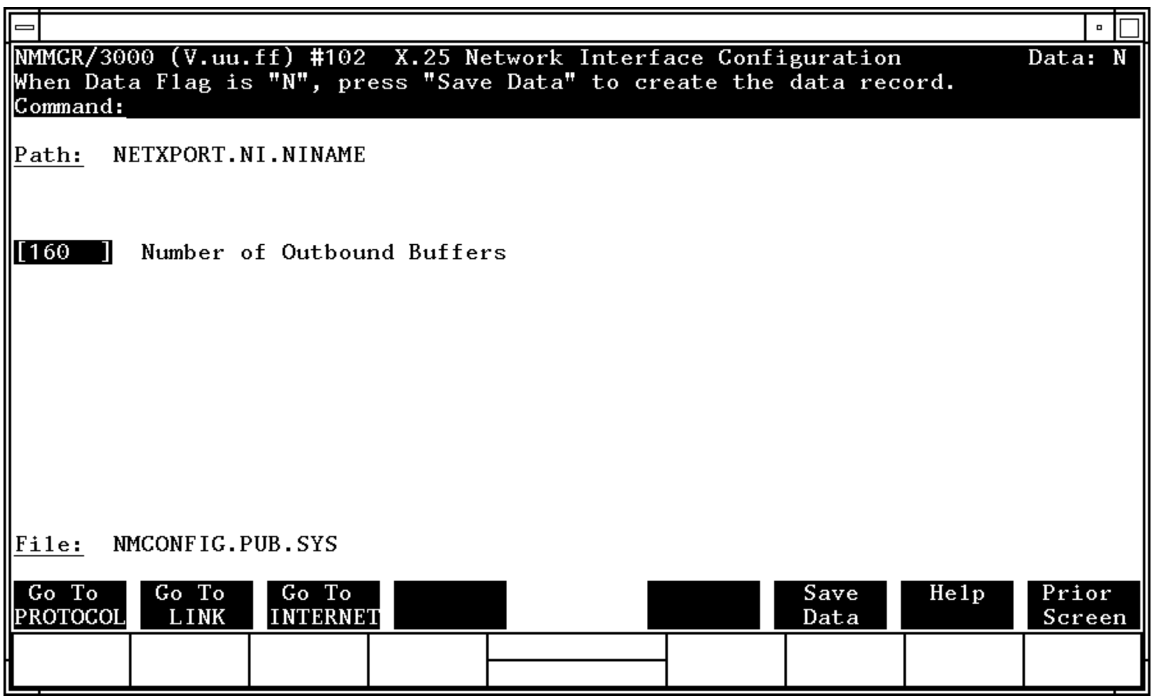
X.25 Network Interface Configuration

The X.25 Network Interface Configuration screen (#102) in Figure 7-3 is displayed when you add an X.25 interface to the Network Interface Configuration screen (Figure 7-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-3 X.25 Network Interface Configuration Screen



Use the fields and the function keys of the select screen to perform the desired action. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Number of outbound buffers`

(Required.) Enter the number of buffers that are allocated to the X.25 network interface.

If direct level 3 access is being used, or large (over 5000 bytes) blocks of data are being sent, or multiple no-wait sends are being issued, then more buffers may be needed. Logging location code 174, CLAS0003, tells you that the X.25 subsystem does not have enough buffers, in which case you can increase the number of outbound buffers. (If the outbound buffers are exhausted, the transport will continue to function, but at a significantly reduced efficiency.)

Default value: 160

Range: 32–1060

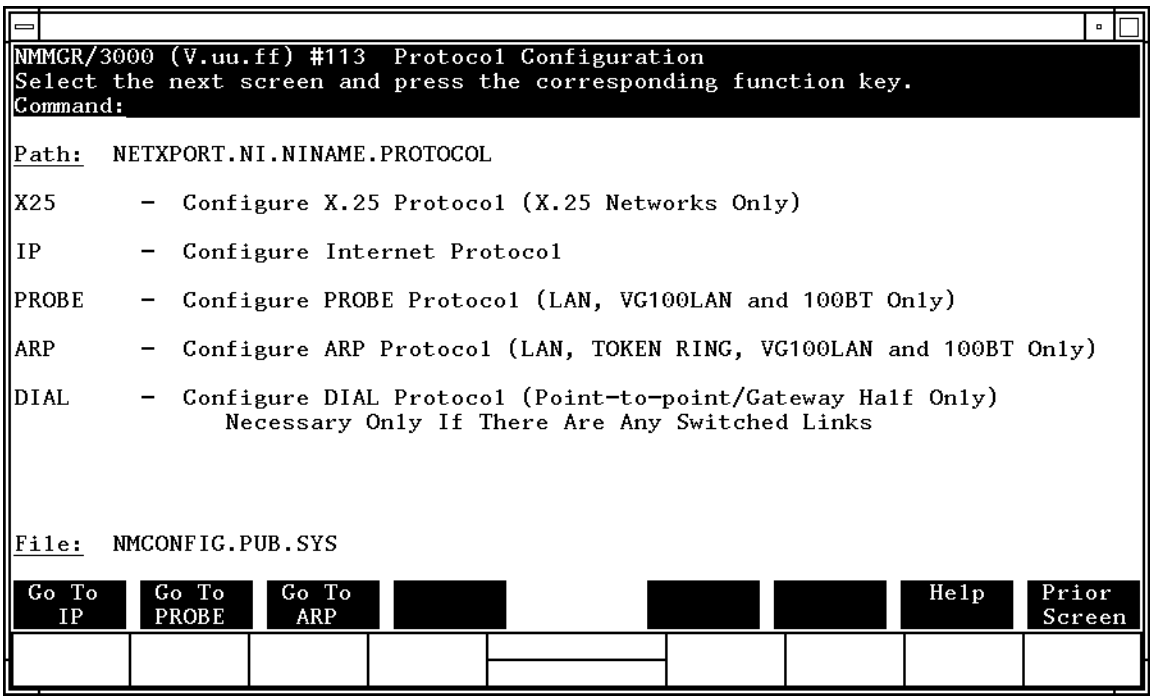
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 7-4 is displayed when you press the **[Go To Protocol]** function key at the X.25 Network Interface Configuration screen (Figure 7-3). This screen is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-4 Protocol Configuration Screen



For the X.25 NI, you configure the X.25 and IP protocols. Choose the protocol to configure and press the corresponding function key.

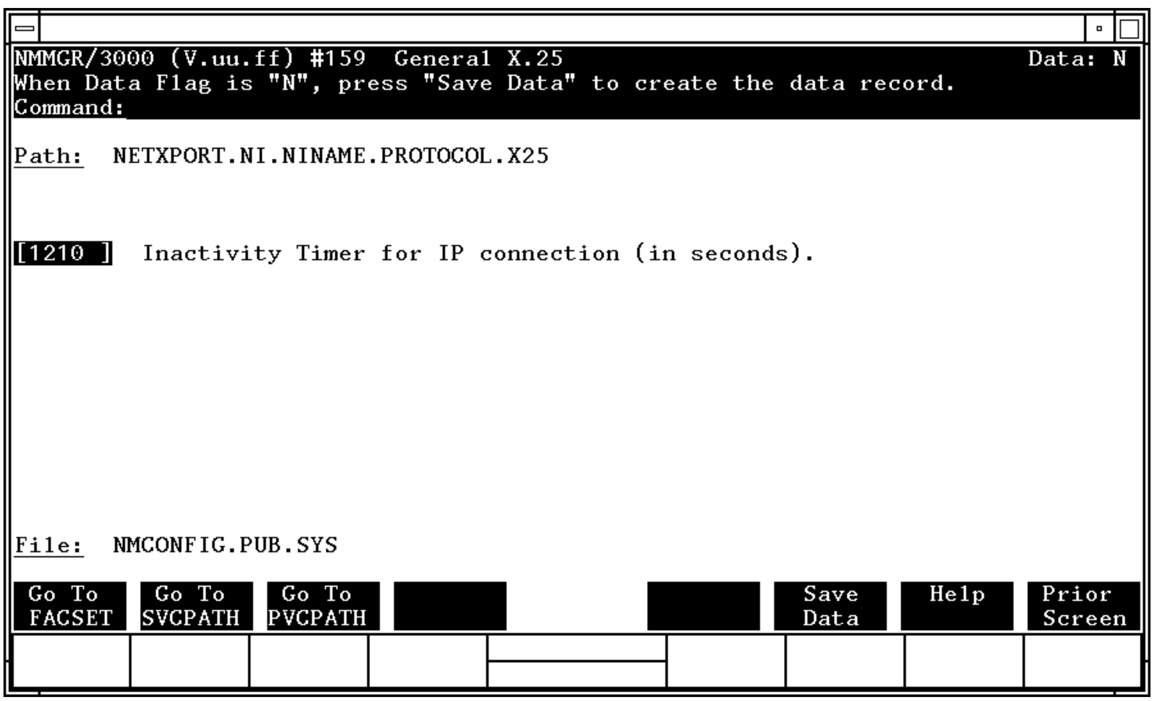
General X.25 Configuration

The General X.25 screen (#159) in Figure 7-5 is displayed when you press the **[Go To X25]** function key at the Protocol Configuration screen (Figure 7-4). It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.PROTOCOL.X25

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-5 General X.25 Protocol Screen



Use the fields and the function keys of the select screen to perform the desired action. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Inactivity timer for IP connections (in seconds)` **(Required.)** Enter a number of seconds after which any inactive switched virtual circuits (SVC) being used for TCP/IP connections are automatically disconnected. If no inactivity timer is to be set, enter a 0 in this field.

It is best to set this timer at more than two times the value of the TCP connection assurance timer. This keeps the X.25 virtual circuit for a remote session active, even when no user data is being transferred.

Default value: 1210

Range: 0, 30–32767

Related screen:

- `NETXPORT.GPROT.TCP`

  The TCP connection assurance timer is set in this screen.

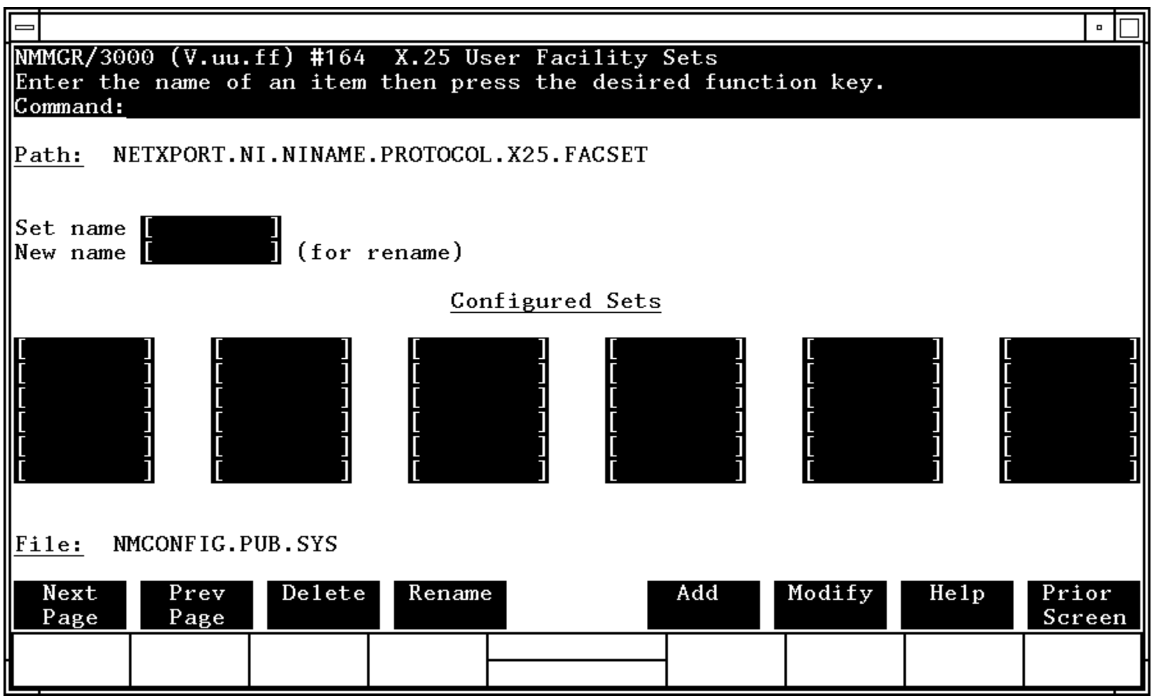
X.25 User Facility Sets

The X.25 User Facility Sets screen (#164) in Figure 7-6 is displayed when you press the **[Go To FACSET]** function key at the General X.25 Configuration screen (Figure 7-5). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.FACSET`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-6 X.25 User Facility Sets



To edit an existing X.25 facility set, enter the name of the X.25 facility set to be modified and press the **[Modify]** function key. To add a new X.25 facility set, enter a new facility set name and press the **[Add]** function key.

You may configure up to 128 User Facility Sets under an X.25 NI.

Fields

`Set name` This name defines a set of X.25 parameters that can be associated with an SVCPATH or a PVCPATH. The name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

`New name` This field is used to rename a facility set. Enter the current name in the set name field. Enter the new name in the new name field and press the **[Rename]** function key.

The name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

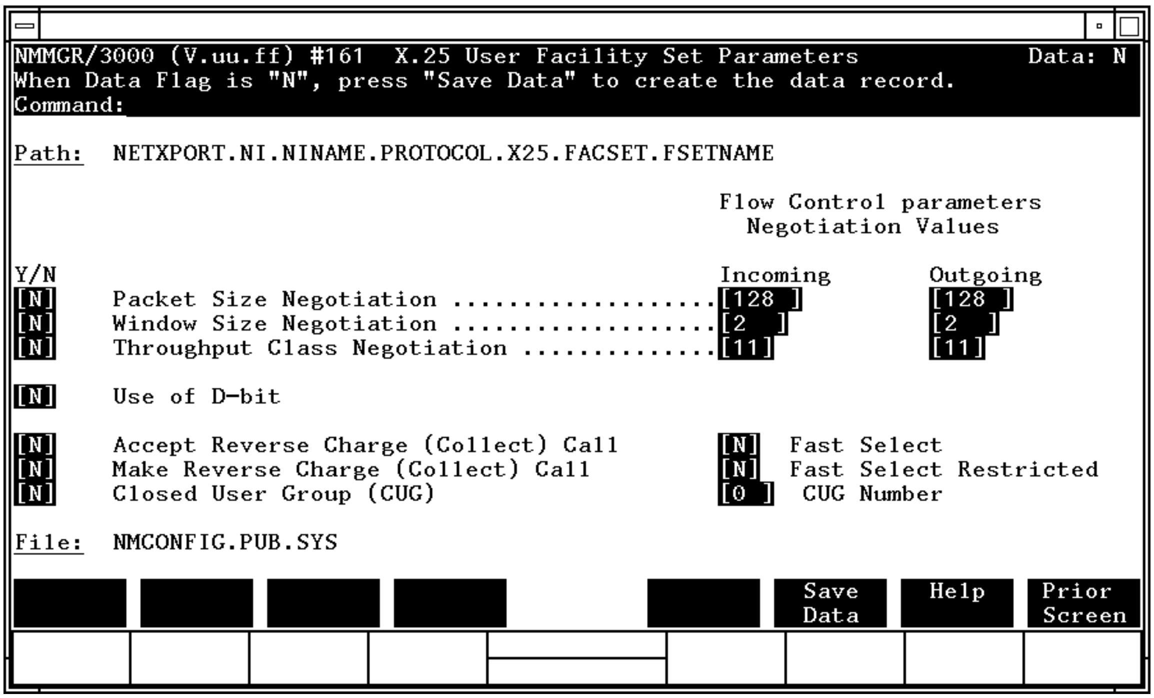
X.25 User Facility Set Parameters

The X.25 User Facility Set Parameters screen (#161) in Figure 7-7 is displayed when you press the **[Add]** or **[Modify]** function key at the X.25 User Facility Sets screen (Figure 7-6). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.FACSET.`*`fsetname`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI and *fsetname* is a configured X.25 facility set.

Figure 7-7 X.25 user Facility Set Parameters Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Packet size negotiation`

(Required.) Enter Y if you want to implement packet size negotiation. Enter N if you do not wish to implement packet size negotiation.

Default: N

Range: Y or N

`Packet size negotiation values`
These are the packet sizes that will be negotiated for incoming and outgoing packets if packet size negotiation is set to Y.

Default: 128

Range: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096

`Window size negotiation`
(Required.) Enter `Y` if you want to implement window size negotiation. Enter `N` if you do not wish to implement window size negotiation.

Default: N

Range: Y or N

`Window size negotiation values`
These are the window sizes that will be negotiated for incoming and outgoing packets if window size negotiation is set to Y.

Default: 2

Range: 1–7

`Throughput class negotiation`
(Required.) Enter `Y` if you want to implement throughput class negotiation. Enter `N` if you do not wish to implement throughput class negotiation.

Default: N

`Throughput class negotiation values`
Throughput class negotiation values depend upon the speed of the link. Table 7-1 shows the throughput classes and associated link speeds.

Range: 7–12, depending upon the speed of the link.

Default: 11

Table 7-1 Throughput Class and Line Speed

Throughput Class	Line Speed
7	1200
8	2400
9	4800
10	9600
11	19200
12	48000

CAUTION Answer `Y` (Yes) to negotiation only if you subscribed for negotiation. Some networks will reject a call with negotiation if you did NOT subscribe for negotiation. Also, if you did subscribe for negotiation, it is preferable to answer `Y` because certain networks will clear a call if you subscribe for negotiation but answer `N` (No) for negotiation.

`Use of D-bit` **(Required.)** Enter `Y` if you want to enable delivery confirmation with this set of circuits. Enter `N` if you either do not subscribe to this facility, or do not want delivery confirmation enabled for this set of circuits.

`Accept reverse charge (collect) call` **(Required.)** Enter `Y` if you wish to configure the link to receive reverse charge calls on this set of circuits. Enter `N` if you either do not subscribe to this facility, or do not want to accept reverse charging on this set of circuits.

Default: N

Range: Y or N

`Make reverse charge (collect) call` **(Required.)** Enter `Y` if all calls sent by this set of switched virtual circuits (SVC) request reverse charging. Enter `N` if you either do not subscribe to this facility, or do not want reverse charging capabilities enabled for this set of circuits.

Default: N

Range: Y or N

`Closed user group (CUG)` **(Required.)** The closed user group (CUG) facility enables a group of DTE devices to communicate only with other members of the same CUG and prevents access from any device or user that is not in this CUG. Answer `Y` if you subscribed to a CUG using the basic format and if you want to use this CUG with this SVC set. Answer `N` if you did not subscribe to a CUG using the basic format or if you do not want this SVC set to belong to a CUG.

Default: N

Range: Y or N

`Fast select` Answer `Y` if you wish to make or receive a fast select call with this set of circuits. Enter `N` if you either do not subscribe to this facility, or do not want fast select capability enabled for this set of circuits.

Default: N

`Fast select restricted` Enter `Y` if you want the remote node(s) to reject any call made with the fast select facility. You can answer `Y` in this field only if you answered `Y` in the fast select field. Enter `N` to enable the remote node(s) to accept or reject fast-select calls.

Default: N

Range: Y or N

`CUG number` If the closed user group facility is enabled for this set of circuits, specify the number of the CUG to be used.

Default: 0

Range: 0–99

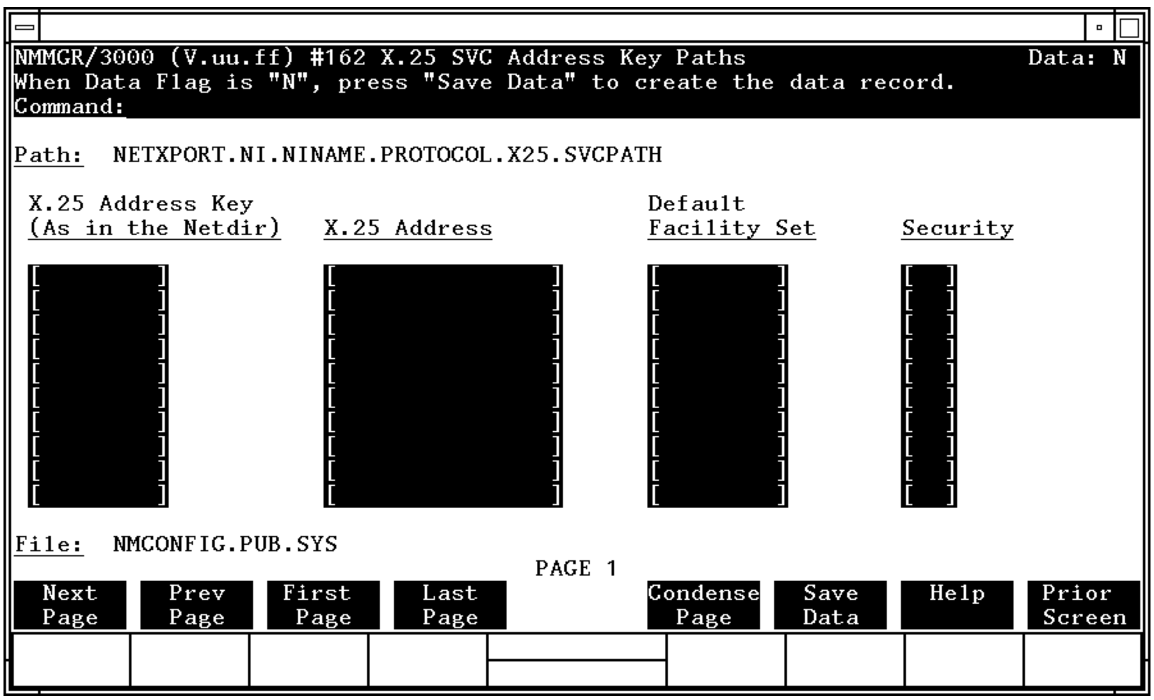
X.25 SVC Address Key Paths

The X.25 SVC Address Key Paths screen (#162) in Figure 7-8 is displayed when you press the **[Go To SVCPATH]** function key at the General X.25 Configuration screen (Figure 7-5). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.SVCPATH`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-8 X.25 SVC Address Key Paths



The X.25 address key is a label which associates an X.25 address with an IP address from the network directory. This provides you the address of the remote host and the values of the connection parameters you selected to use when communicating with that host. Every remote address defined in the path table must be assigned a default facilities set. **You may configure up to 2048 SVC address keys under an X.25 NI, and if configuring multiple X.25 NI's, no address key can be used more than once per system.**

The default facilities set must be one of the defined facility sets in the X.25 User Facility Set screen (`NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.FACSET`).

POOL is the X.25 address key reserved for calls to and from nodes whose addresses are not defined in this X.25 SVC Address Key Path screen. When a POOL X.25 address key is used, any system, even one that is not identified in this screen, can access this node. HP recommends that you use the *name* portion of the formal node name (`name.domain.organization`) as the X.25 address key. You can have a maximum of 2048 address keys in the SVC path tables and 128 address keys in the PVC path tables. **If configuring multiple X.25 NI's, no address key can be used more than once per system.** POOL can also be used with level 3 programmatic access when specifying an X.25 address directly in a NetIPC call (for example, the IPCDEST call)

NOTE For DDN networks, the X.25 address is derived from the remote IP address and you are not required to know the remote X.25 address. Mapping is only required between the X.25 address key and the facility set.

Fields

`X.25 address key` **(Required.)** The X.25 address key identifies a remote node to which your node can establish a connection. The address key can have up to eight alphanumeric characters, the first of which must be alphabetic.

`X.25 address` This is the X.25 address of the remote node for X.25 public data networks (PDN) or a private X.25 network. The X.25 address can have up to 15 digits. The X.25 address will not be used if you configure a POOL address key, or if you are configuring a link for a DDN network.

Default: None.

`Default facilities set name` The name of one of the facility sets you defined at the User Facility Set screen. This set of facilities is associated with the connections you have previously defined. This field is required if you define an address key.

Default: None

`Security` The level of security you wish to assign to this particular entry. The possible values are as follows:

- IN is the level of security you assign to accept only incoming calls from the specified remote address.
- OU is the level of security you assign to accept only outgoing calls to the specified remote address. All incoming calls are rejected.

- IO is the level of security you assign to accept both incoming and outgoing calls.
- LK is the level of security you assign to lock this entry so that no calls, incoming or outgoing, are accepted. LK is useful if you are using POOL to accept calls from all nodes, but you want to exclude a few nodes from accessing this node. Enter the nodes you want to restrict in this screen and specify LK as the security.

This field is required if you defined an address key.

Default: IO

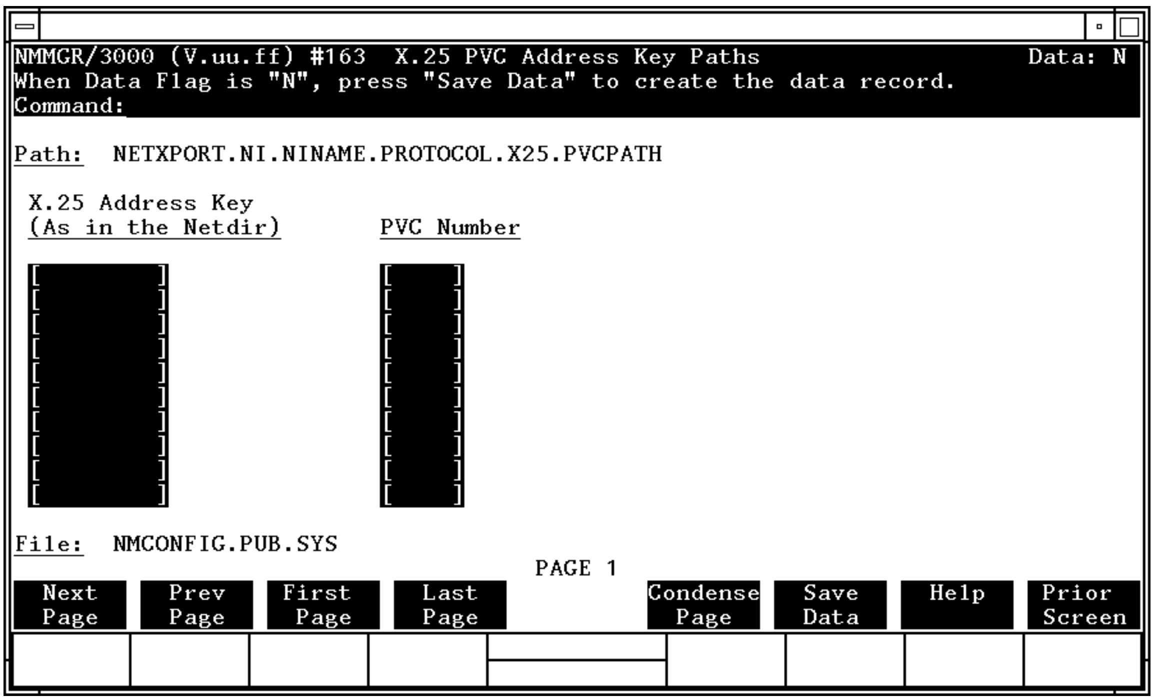
X.25 PVC Address Key Paths

The X.25 PVC Address Key Paths screen (#163) in Figure 7-9 is displayed when you press the **[Go To PVCPATH]** function key at the General X.25 Configuration screen (Figure 7-5). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.PVCPATH`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-9 X.25 PVC Address Key Paths Screen



You may configure up to 128 PVC address keys under an X.25 NI, and if configuring multiple X.25 NI's, no address key can be used more than once per system.

Fields

`X.25 address key` The X.25 address key is used to identify a remote node to which this node will communicate. The address key can have up to eight alphanumeric characters, the first of which must be alphabetic.

Default: None.

`PVC number` The PVC number is a permanent virtual circuit number which identifies the remote host for the node you are configuring. This number must be in the PVC range you defined in the OpenView DTC Manager configuration. This is a required field if you defined a corresponding X.25 address key.

Default: None

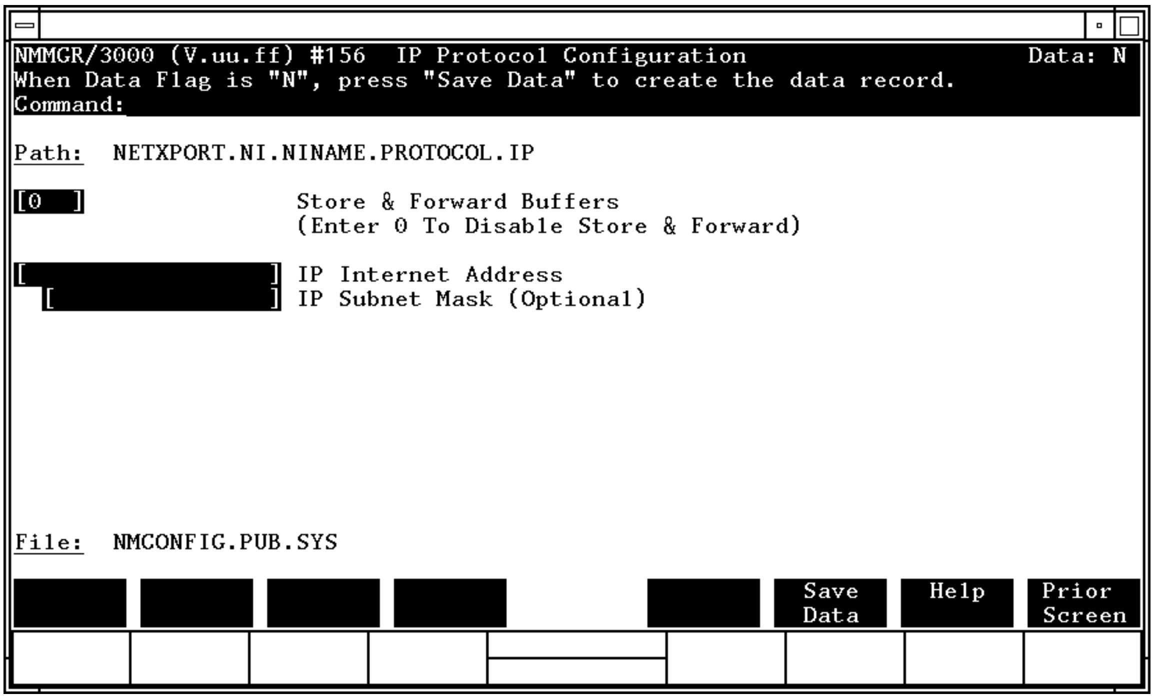
Internet Protocol Configuration

The IP Protocol Configuration screen (#156) in Figure 7-10 is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 7-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-10 IP Protocol Configuration Screen



This screen is used to supply IP protocol information for the network being configured. Each NI has an IP address. The IP Address field is a key element in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI names in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

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 you are configuring a non-gateway node on this network. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface. You can modify the number of store-and-forward buffers to allow performance tuning for different network types. However, HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

If store-and-forward is to be disallowed, set this number to 0.

Default value: 0

Range: 0–50

NOTE If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bit of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node 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:     001–126
```

Network and node values of all zeros or all ones are not allowed. These are special values.

Default value: None, but a value *must* be supplied.

`IP subnet mask`

The IP subnet mask masks a portion of the IP address for subnets. The subnet is specified in the same format as an IP address; that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the **node** portion would be expressed as 255 255.000.000. The default is no IP mask.

Refer to the *HP 3000/iX Network Planning and Configuration Guide* for more details on subnets.

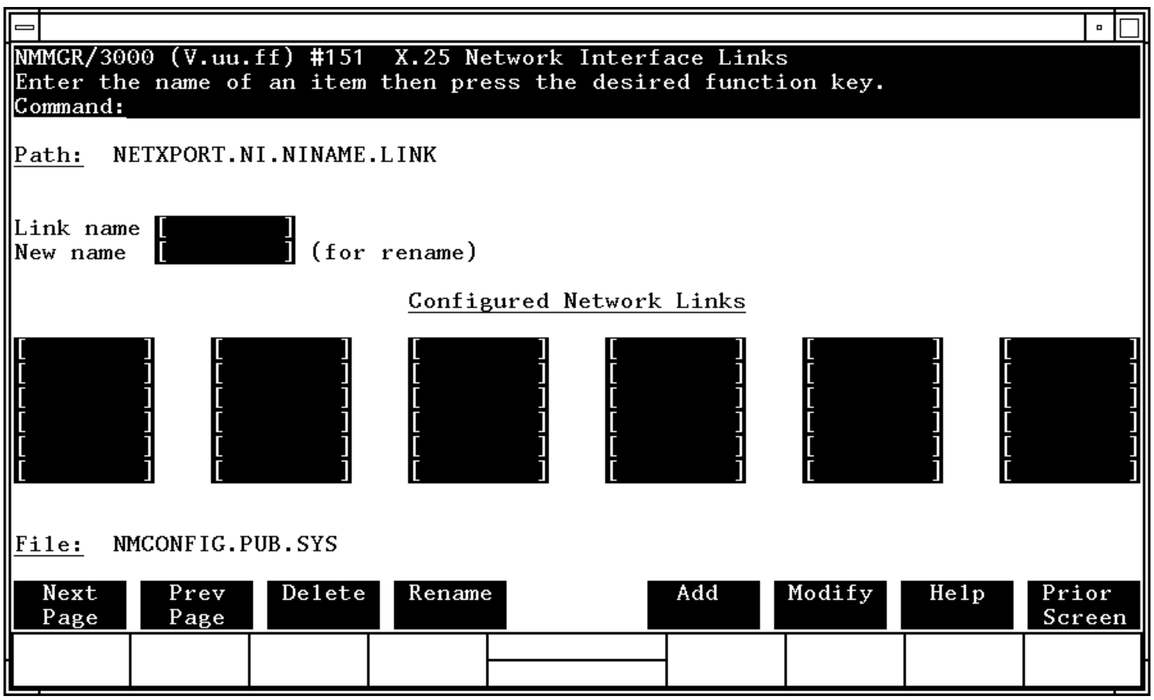
X.25 Network Interface Links

The X.25 Network Interface Links screen (#151) in Figure 7-11 is displayed when you press the **[Go To LINK]** function key at the X.25 Network Interface Configuration screen (Figure 7-3). It is also displayed when you type the path name:

`@NETXPORT.`*`NI.NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-11 X.25 Network Interface Links Screen



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 the **[Add]** function key. The path for the added link name is put in the configuration file, and the data screen on the path is displayed. **You can associate 12 links with a single X.25 NI.**
- To modify an existing link configuration, specify the link name; then press the **[Modify]** function key. The next screen 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Network Links.

Fields

`Link name` Make sure this is the same link name configured at the X.25 Link Configuration screen (path name `LINK`). This screen associates the link data with the X.25 network interface data. 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. **You can associate up to twelve (12) links with a single X.25 NI.** All links associated with an NI have equal value (no primary or secondary weightings are assigned).

`New name` **(Required when renaming an existing X.25 link.)** 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.

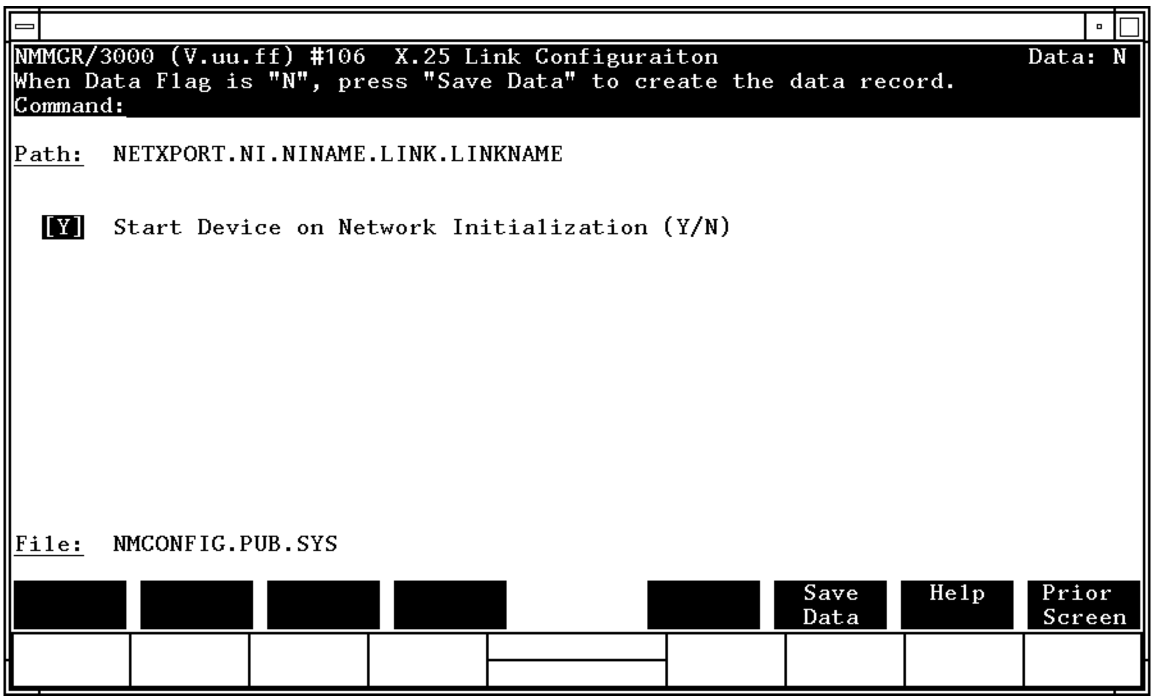
X.25 Link Configuration

The X.25 Link Configuration screen (#106) shown in Figure 7-12 is displayed when you select an NI link name and press the **[Add]** or **[Modify]** function key at the X.25 Network Interface Link screen (Figure 7-11). It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.LINK.*linkname*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI, and *linkname* is a configure X.25 link.

Figure 7-12 X.25 Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Start device on network initialization (Y/N)`

Answer `Y` (Yes) if you want the device connected over this link to be started when the network is first initialized. Answer `N` (No) if you do NOT want the device started when the network is first initialized.

Default value: Y

Range: Y or N

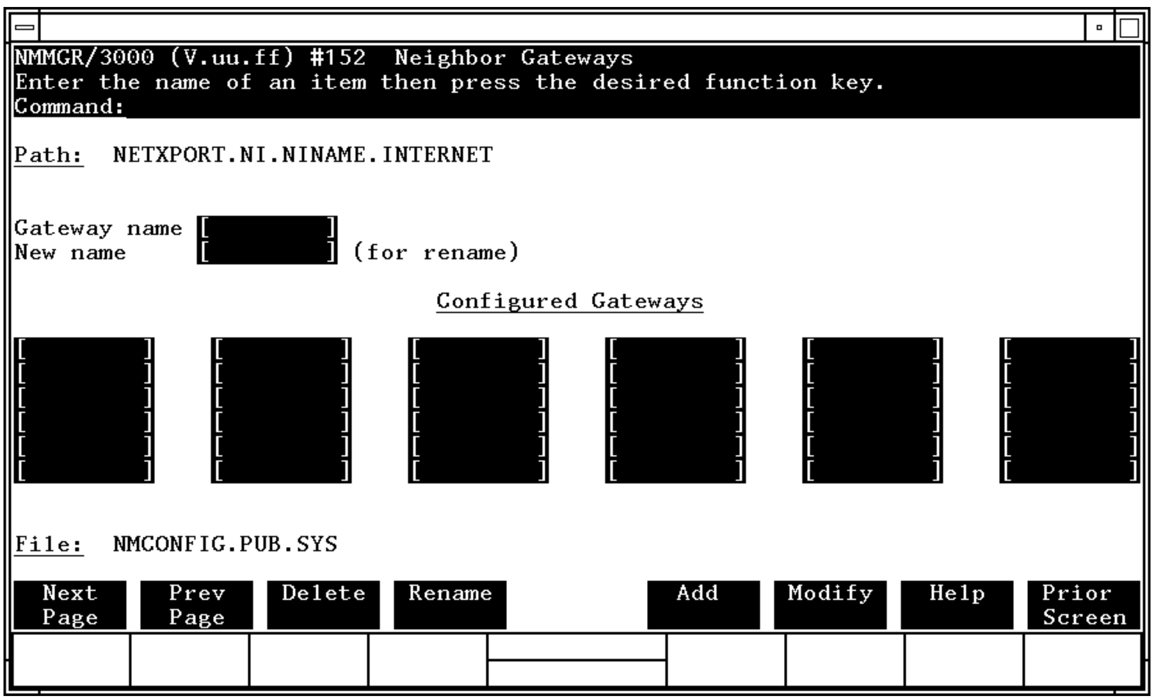
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 7-13 is displayed when you press the **[Go To INTERNET]** function key at the X.25 Network Interface Configuration screen (Figure 7-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI.

Figure 7-13 Neighbor Gateways Screen



Use this screen, and the screens that follow it, to identify to your node the gateways on your network. Use the fields and the function keys of this select screen to perform the desired action.

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**
- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway, specify the gateway name and a new name; then press the **[Rename]** function key. 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, specify the gateway name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. 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 network numbers of all networks reachable from this gateway node.

Fields

`Gateway name` Enter a name to represent a gateway on this X.25 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. The gateway name is not the same as the node name of the gateway, however you can use the node name to make it easier to identify the gateway.

`New name` **(Required only when renaming an existing gateway.)** 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.

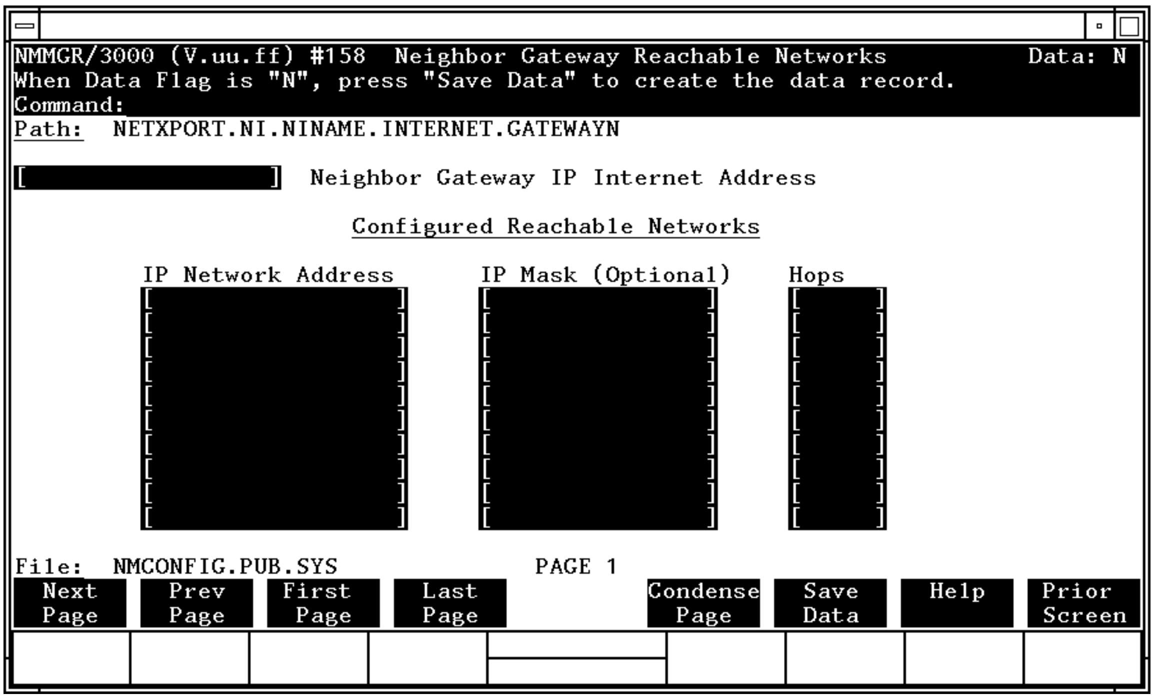
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 7-14 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 7-13) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.`*`gatewayn`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured X.25 NI, and *gatewayn* is the configured X.25 NI gateway name.

Figure 7-14 Neighbor Gateways Reachable Networks Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE

The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 internetwork 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; however, the node portion need not match.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node portion of the address.

Note that network and node values of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:` `192–223`

`Class B:` `128–191`

`Class A:` `001–126`

The network address (network portion of the IP address) configured in `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` must match the neighbor gateway IP internet address configured in the current screen.

Default value: None

`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.

You can also designate this gateway as a default gateway by entering an "at" sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask, one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask configured in the IP Protocol Configuration screen (Figure 7-10) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnets.

  Related screen:

  - `NETXPORT.NI.`*`NIname`*`.INTERNET`

    This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask` The IP mask masks a portion of the IP address for subnets. The subnet is specified in the same format as an IP address, that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the node portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, the network transport will choose internally from among the routes with equal hop counts.

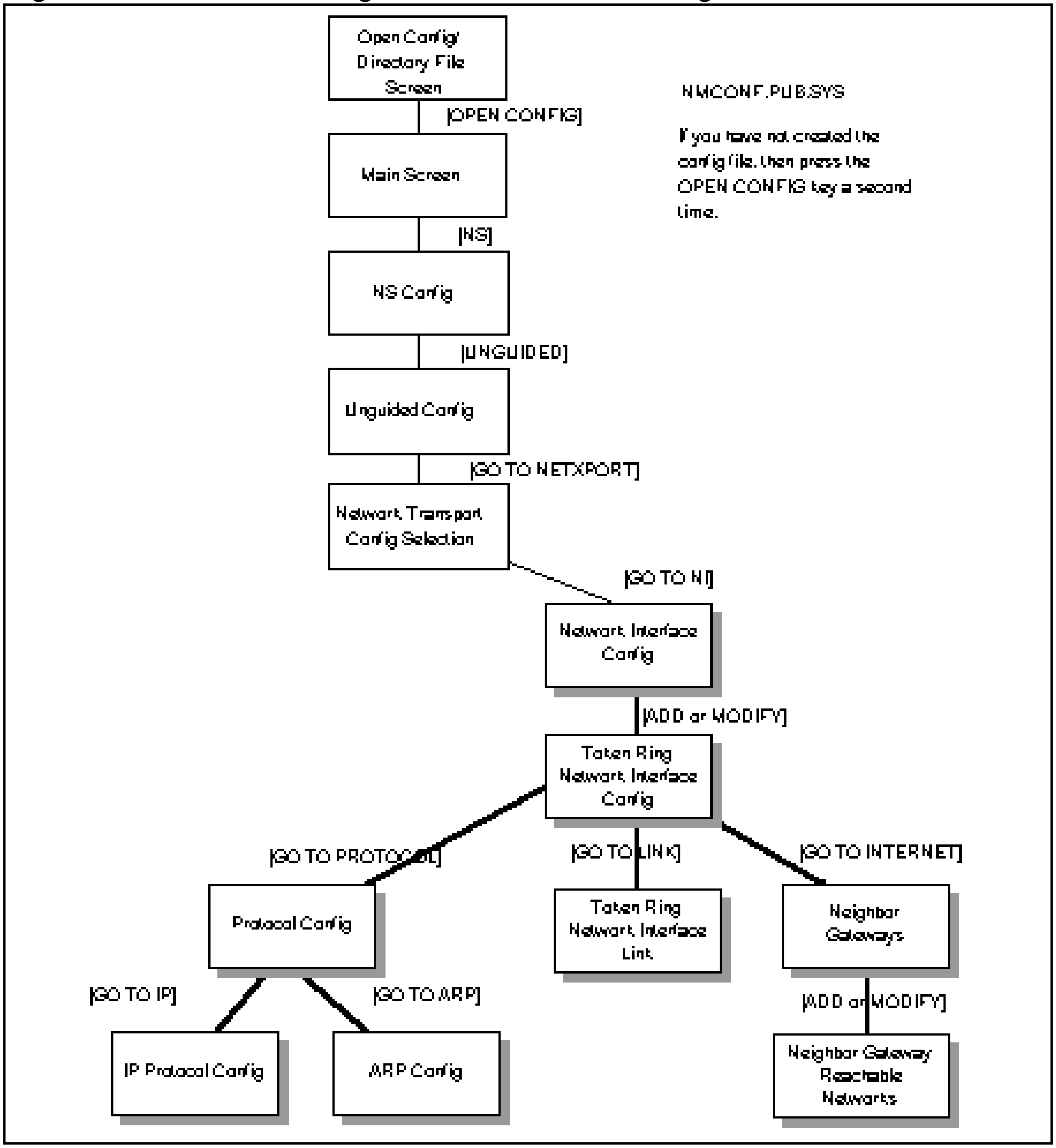
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

8 Token Ring Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring a Token Ring network. The Token Ring Network Interface Configuration branch of NMMGR begins with a screen called the Network Interface Configuration screen. Figure 8-1 shows the screen flow for configuring the Token Ring screens. Screens unique to Token Ring are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 8-1 Token Ring Network Interface Configuration Screen Flow



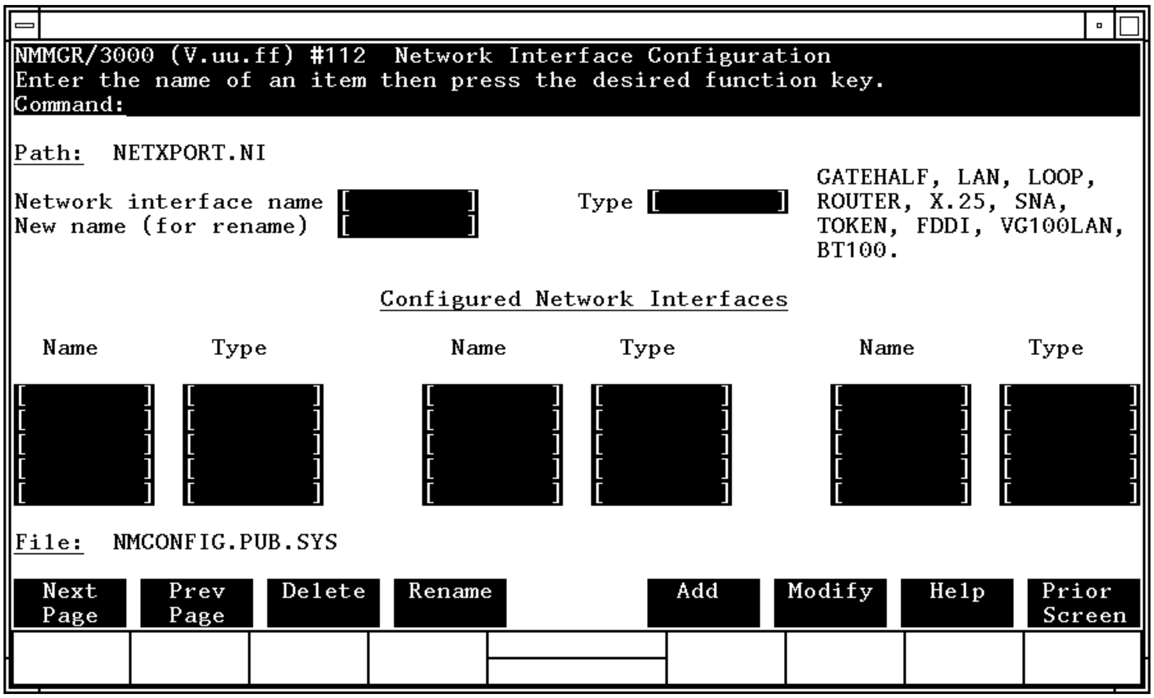
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 8-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

```
@NETXPORT.NI
```

in the Command window of any screen and press the **[Enter]** key.

Figure 8-2 Network Interface Configuration Screen



Use the fields and the function keys of the select screen to perform the desired action.

- To define a new token ring NI, specify an NI name and NI type `TOKEN`; then press the **[Add]** function key. The path for the selected NI name is added to the configuration file and the data screen on that path is displayed. **You can have a maximum of 12 NI's per system (one NI must be used for loopback). However, HP supports only one active Token Ring NI per system.**
- To modify an existing NI configuration, specify the NI name; and then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) 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 software loopback capability.

Fields

`Network interface name` Enter the network interface name for the token ring interface.

The network interface name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, FDDI, 100VG-AnyLAN, or 100Base-T)` **(Required only when adding an NI.)** Enter `TOKEN` if you are configuring a token ring network.

`New name` **(Required only when renaming an NI.)** 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.

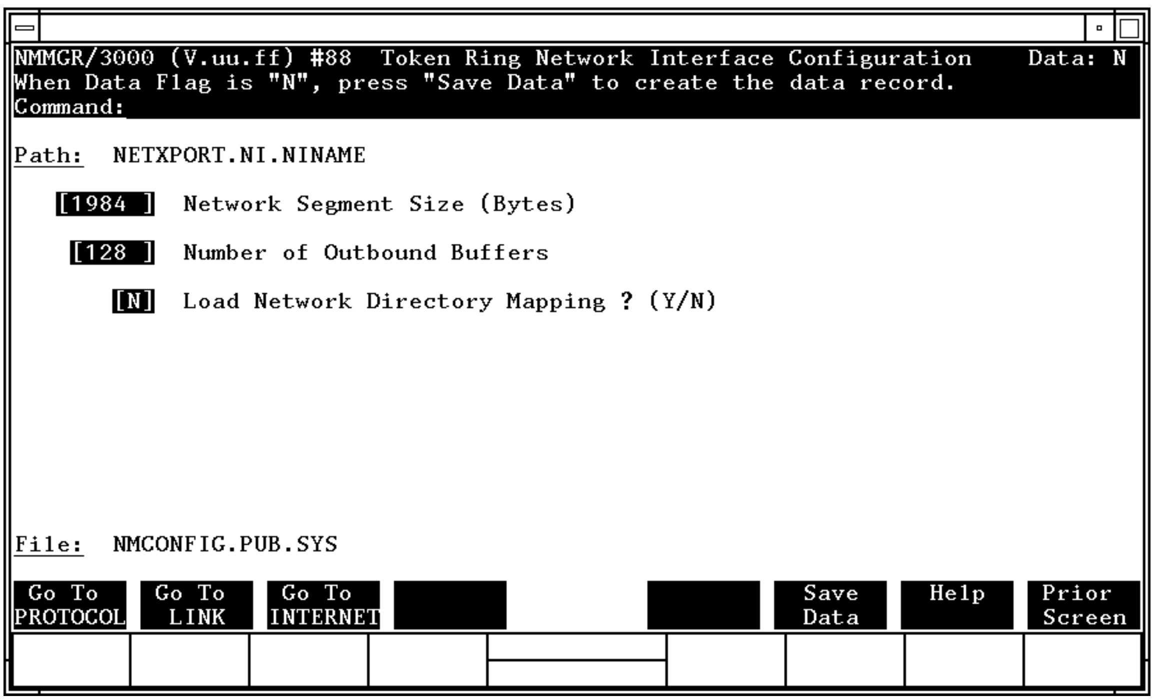
Token Ring Network Interface Configuration

The Token Ring Network Interface Configuration screen (#88) in Figure 8-3 is displayed when you select an NI name and the NI type `TOKEN` at the Network Interface Configuration screen (Figure 8-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI name.

Figure 8-3 Token Ring Network Interface Configuration Screen



The token ring network interface (NI) module serves to interface the upper layers of the transport product to the link layer. This screen supplies the information required for that interface. All of the fields are used for internal resource allocation.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. 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 network layer protocols, the token ring network interface link, and internetwork routing.

Fields

`Network segment size` This field specifies the largest packet that will be sent by the token ring device. The only reason for entering a value smaller than 1984 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: 1984 bytes

Range: 300–1984

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Overallocation may waste core memory.

Related screen:

- `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: 128

Range: 128–4096

`Load network directory mapping? (Y/N)` Specifies whether or not the system should load mappings from the network directory at network startup. If you have nodes on the token ring that do not support the ARP protocol, you must enter these nodes into the network directory and set load network directory mapping to Y. HP nodes support the ARP protocol.

HP recommends the default unless it is for the situation describe above. Refer to Chapter 15, “Network Directory,” for information about the network directory.

Default value: N

Range: Y or N

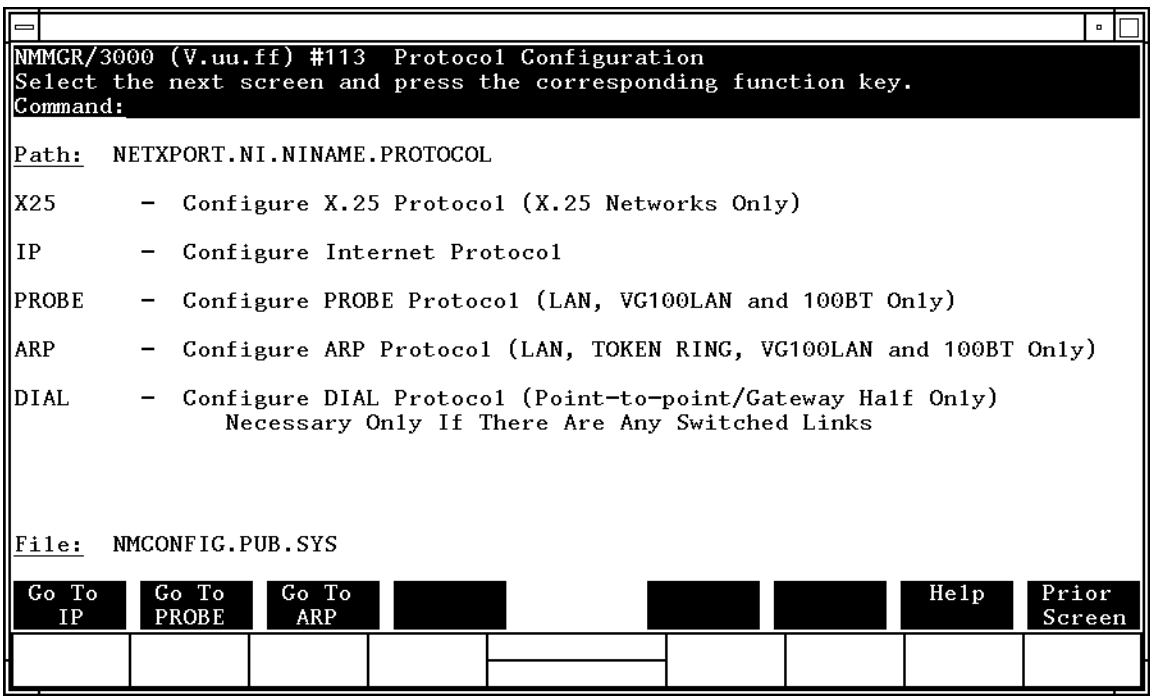
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 8-4 is displayed when you press the **[Go To Protocol]** function key at the Token Ring Network Interface Configuration screen (Figure 8-3). This screen is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI.

Figure 8-4 Protocol Configuration Screen



For the token ring NI, you configure the IP and ARP protocols. Choose the protocol to configure and press the corresponding function key.

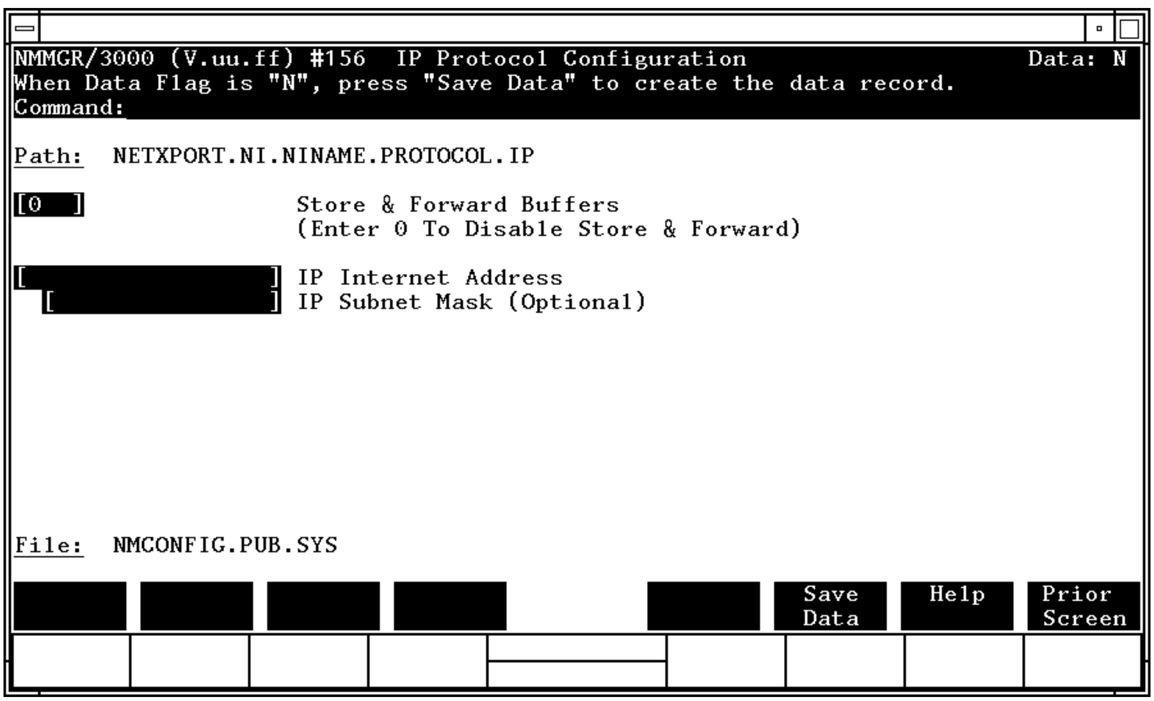
Internet Protocol Configuration

The IP Protocol Configuration screen (#156) in Figure 8-5 is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 8-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI.

Figure 8-5 IP Protocol Configuration Screen



This screen is used to supply IP protocol information for the network being configured. Each NI has an IP address. The IP Address field is a key element in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI named in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

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 you are configuring a non-gateway node on this network. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface.

The number of store-and-forward buffers can be configured to allow performance tuning for different network types. However, HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

If store-and-forward is to be disallowed, set this number to 0.

Default value: 0

Range: 0–50

NOTE

If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:    C nnn.nnn.nnn xxx
Class B:    B nnn.nnn xxx.xxx
Class A:    A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node 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:    001–126
```

Network and node values of all zeros or all ones are not allowed. These are special values.

Default value: No default, but a value *must* be supplied.

`IP subnet mask`

An IP subnet mask is used when configuring subnetworks. The mask identifies the network portion of an IP address and the bit of the node portion of an IP address used to define a subnetwork. An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by a period "." or a space. For example, a mask for a class A network with the subnet field being the first 8 bits of the **node** portion would be expressed as 255 255.000.000. The default is no IP mask.

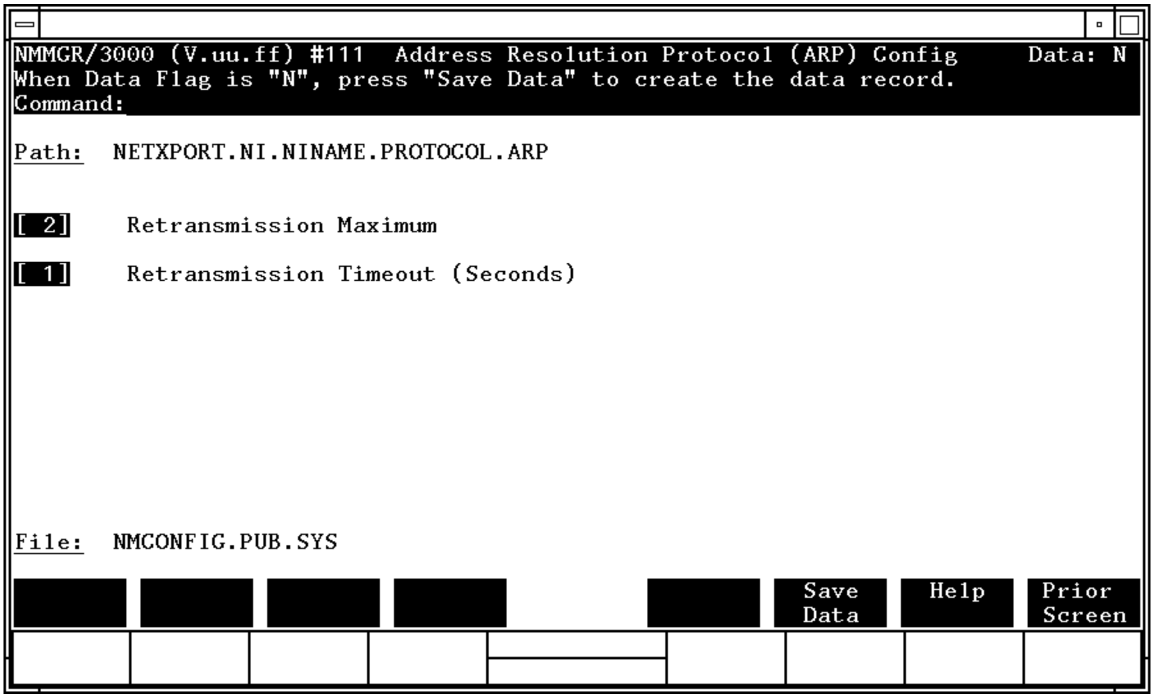
Address Resolution Protocol (ARP) Configuration

The Address Resolution Protocol (ARP) Configuration screen (#111) in Figure 8-6 is displayed when you press the **[Go To ARP]** function key at the Protocol Configuration screen (Figure 8-4). It is also displayed when you type the path name:

`@NETXPORT.`*`NI.NIname`*`.PROTOCOL.ARP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI.

Figure 8-6 Address Resolution Protocol (ARP) Configuration Screen



This screen allows you to configure the information required for the address resolution protocol (ARP). The ARP protocol exists on a token ring network to provide a means of exchanging addressing information between nodes.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking the Data flag is set to Y.

Fields

`Retransmission maximum`

This is the maximum number of times that an ARP request packet will be retransmitted. If an ARP reply packet for this request is not received after this number of retransmissions, the attempted address resolution is considered to have failed. This value is bound closely to the retransmission timeout value. Taken together, they represent the total time to report an address resolution failure.

In general, the value of this field should be kept low.

Default value: 2

Range: 1–10

`Retransmission timeout (seconds)`

This is the time interval (in seconds) between ARP retransmissions. The value should be set large enough to avoid retransmissions in a temporarily overloaded environment, yet the value should be small enough to receive a timely failure report when a failure is inevitable.

Default value: 1

Range: 1–10

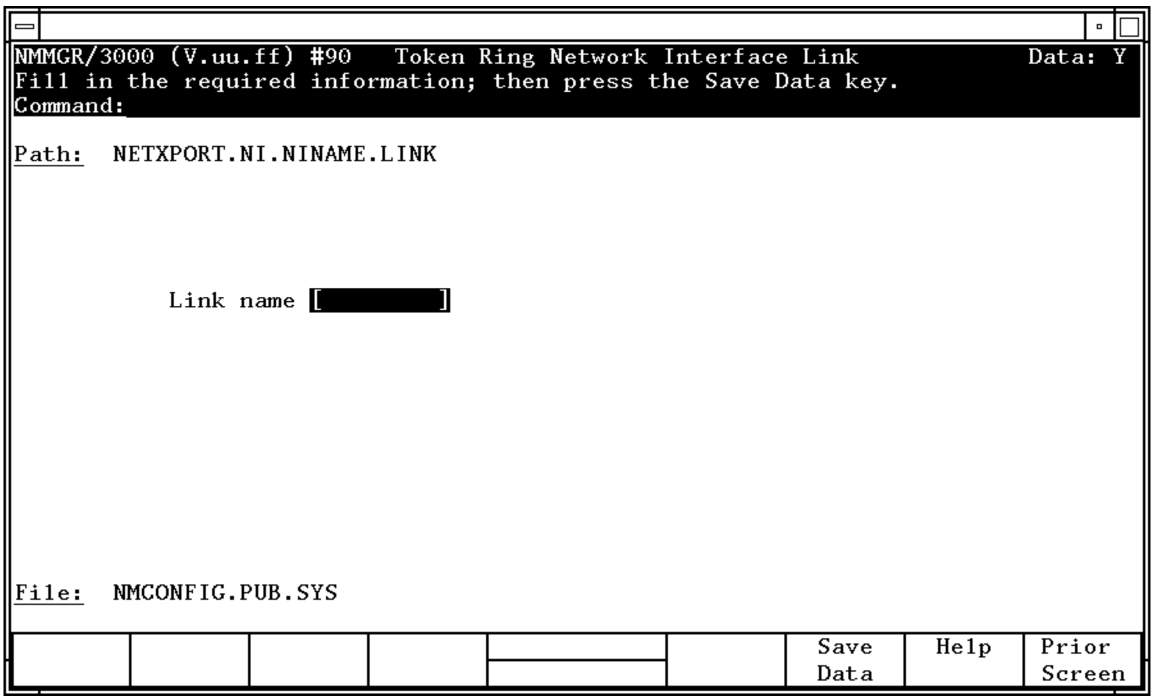
Token Ring Network Interface Links

The Token Ring Network Interface Links screen (#90) in Figure 8-7 is displayed when you press the **[Go To LINK]** function key at the Token Ring Network Interface Configuration screen (Figure 8-3). It is also displayed when you type the path name:

`@NETXPORT.`*`NI.NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI.

Figure 8-7 Token Ring Network Interface Links Screen



Use the fields and the function keys of this select screen to bind the token ring NI to the link. Enter the link name in the `Link name` field and press the **[Save Data]** key. (If you wish to rename the link, simply enter the new name and press the **[Save Data]** key.)

Fields

`Link name` Make sure this is the same link name configured at the Token Ring Link Configuration screen (#87) (path name `LINK`). Press the **[Save Data]** function key to save the link name in the configuration file. Verify that the link name has been configured by checking that the Data flag is set to Y.

This screen associates the link data with the token ring network interface data. The link name is used by the network transport when establishing connections. The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

To change an existing link name, enter the new name in the `Link name` field and press the **[Save Data]** function key.

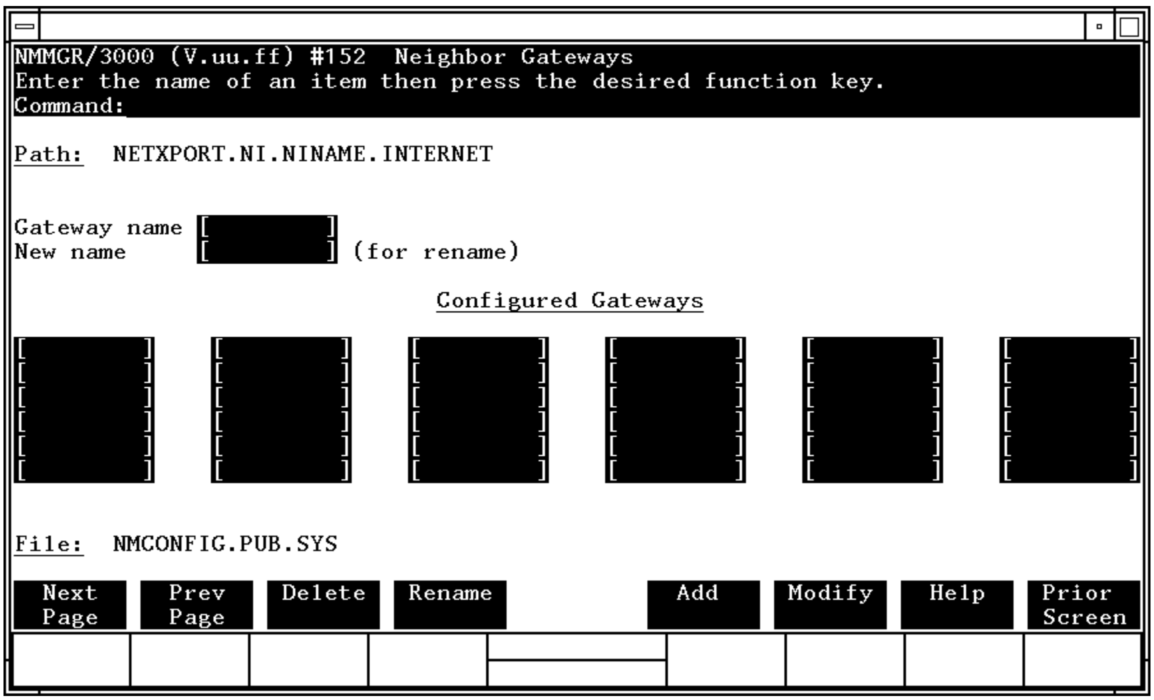
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 8-8 is displayed when you press the **[Go To INTERNET]** function key at the Token Ring Network Interface Configuration screen (Figure 8-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI.

Figure 8-8 Neighbor Gateways Screen



Use this screen, and the screens that follow it, to identify the gateways on this network. Use the fields and the function keys of this select screen to perform the desired action.

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**

- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway, specify the gateway name and a new name; then press the **[Rename]** function key. 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, specify the gateway name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. 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 network numbers of all networks reachable from this gateway node.

Fields

`Gateway name` Enter a name to represent a gateway on this token ring 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 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.

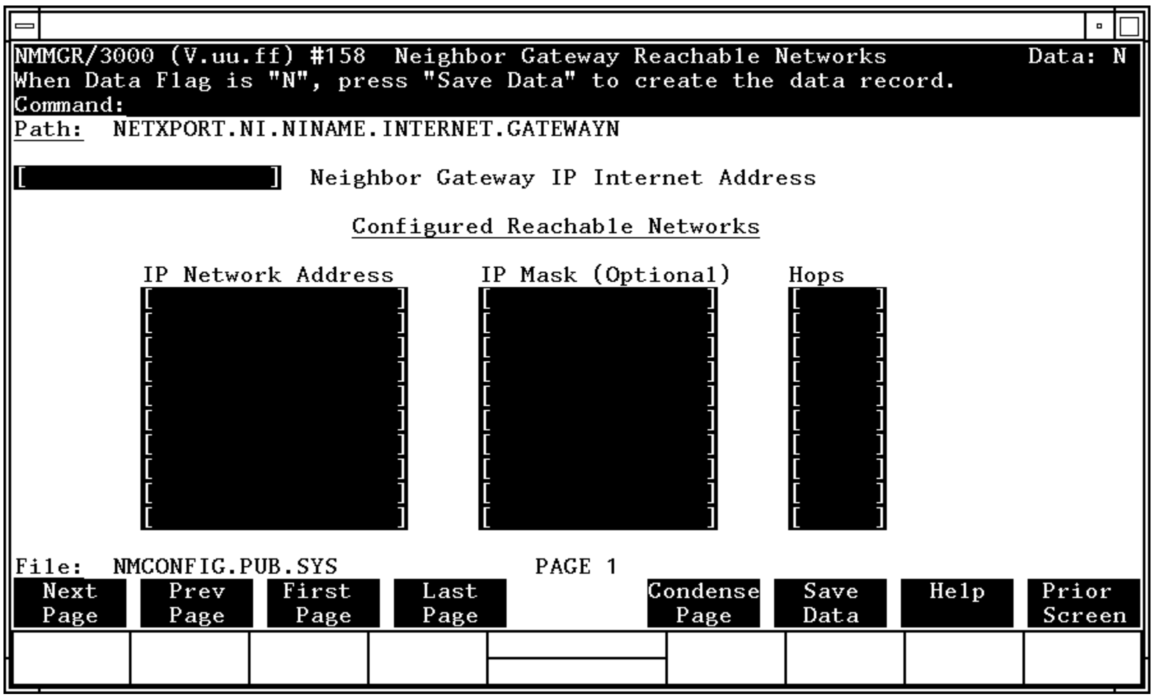
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 8-9 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 8-8) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.`*`gatewayn`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured token ring NI, and *gatewayn* is the configured token ring neighbor gateway name.

Figure 8-9 Neighbor Gateways Reachable Networks Screen



After you have entered all the required data, press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 internetwork 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; however, the node portion need not match.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node portion of the address.

Note that network and node values of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:     192–223`

`Class B:     128–191`

`Class A:     001–126`

The network address (network portion of the IP address) configured in `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` must match the neighbor gateway IP internet address configured in the current screen.

Default value: None

`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.

You can also designate this gateway as a default gateway by entering an “at” sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask, one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask configured in the IP Protocol Configuration screen (Figure 8-5) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnets.

  Related screen:

  - `NETXPORT.NI.`*`NIname`*`.INTERNET`

    This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask` The IP mask identifies a portion of the IP address for subnets. The subnet is specified in the same format as an IP address, that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the **node** portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, the network transport will choose internally from among the routes with equal hop counts.

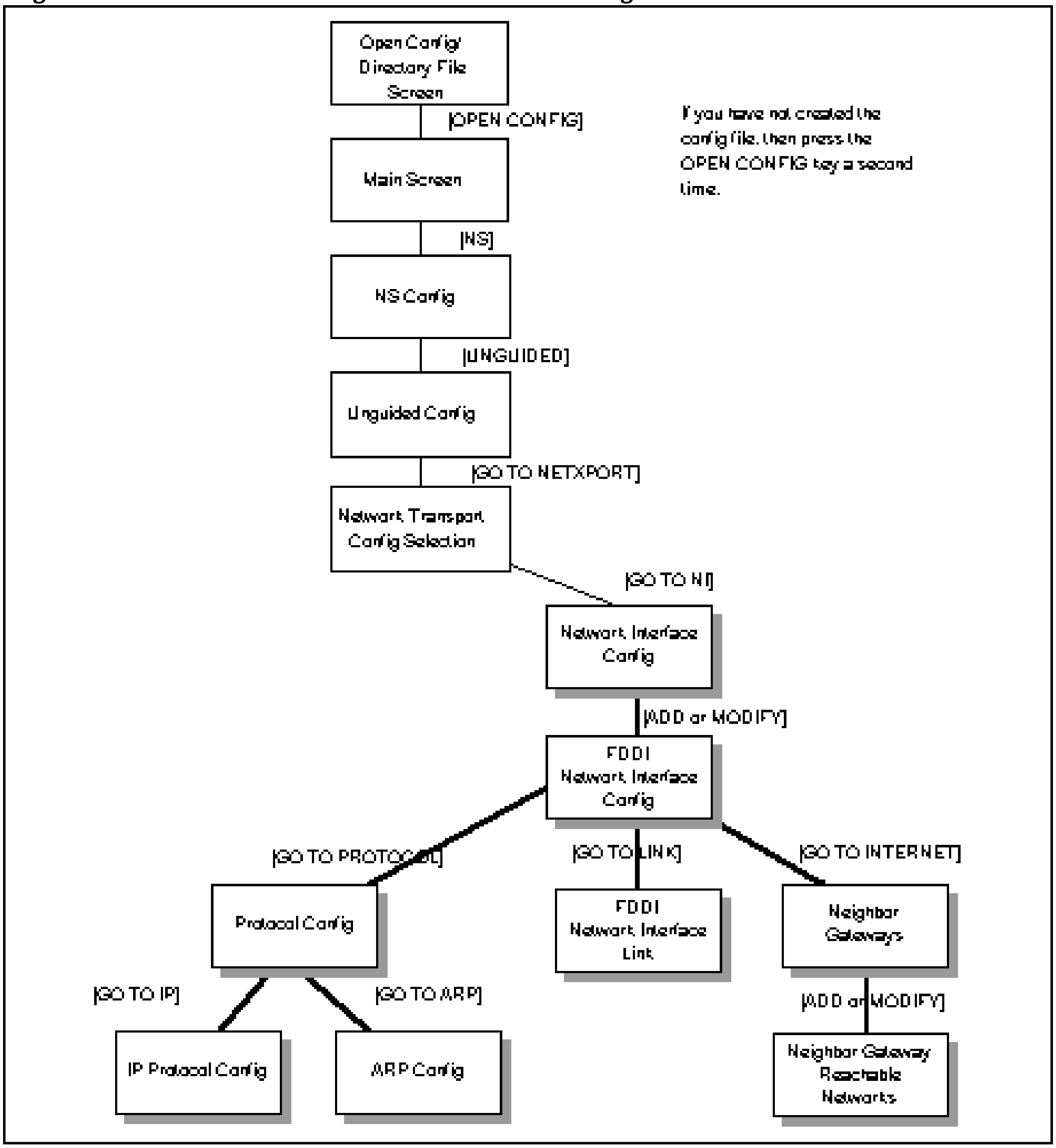
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

9 FDDI Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring a FDDI network. The FDDI Network Interface Configuration branch of NMMGR begins with a screen called the Network Interface Configuration screen. Figure 9-1 shows the screen flow for configuring the FDDI screens. Screens unique to FDDI are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 9-1 FDDI Network Interface Configuration Screen Flow



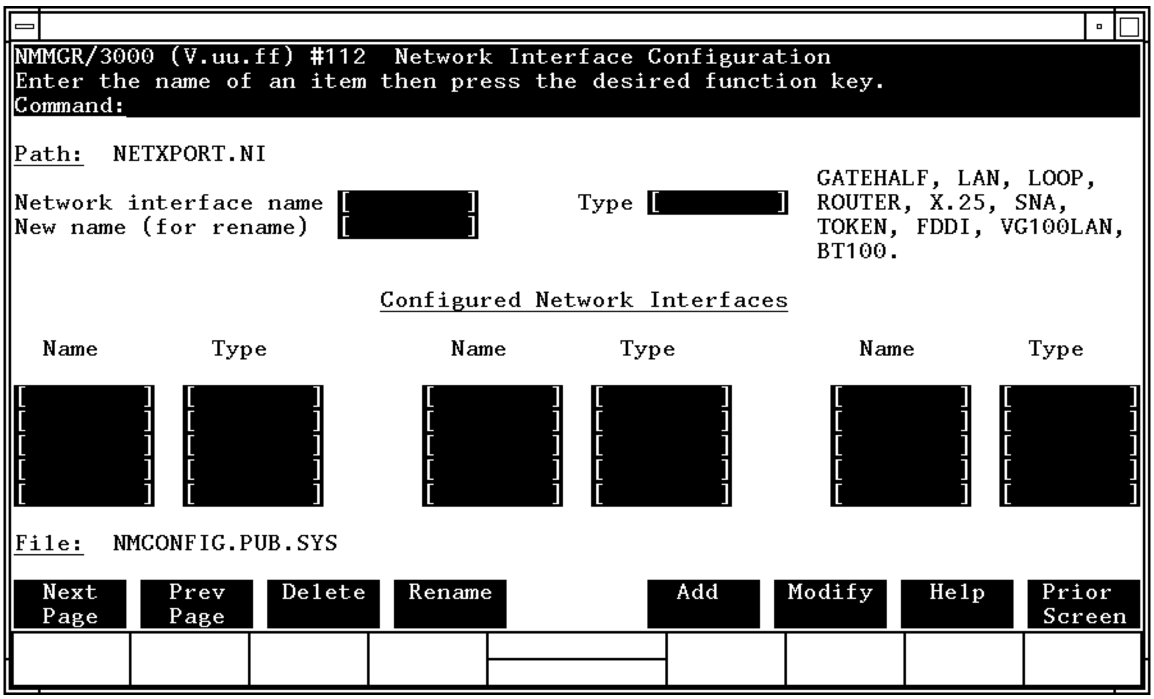
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 9-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

```
@NETXPORT.NI
```

in the Command window of any screen and press the **[Enter]** key.

Figure 9-2 Network Interface Configuration Screen



Use the fields and the function keys of the select screen to perform the desired action.

- To define a new FDDI NI, specify an NI name and NI type `FDDI`; then press the [**Add**] function key. The path for the selected NI name is added to the configuration file and the data screen on that path is displayed. **You can have a maximum of 12 NI's per system (one NI must be used for loopback). However, HP supports only one active FDDI NI per system.**
- To modify an existing NI configuration, specify the NI name; and then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) 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 software loopback capability.

Fields

`Network interface name` Enter the network interface name for the FDDI interface.

The network interface name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, FDDI. 100VG-AnyLAN, or 100Base-T.` **(Required only when adding an NI.)** Enter `FDDI` if you are configuring a FDDI network.

`New name` **(Required only when renaming an NI.)** 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.

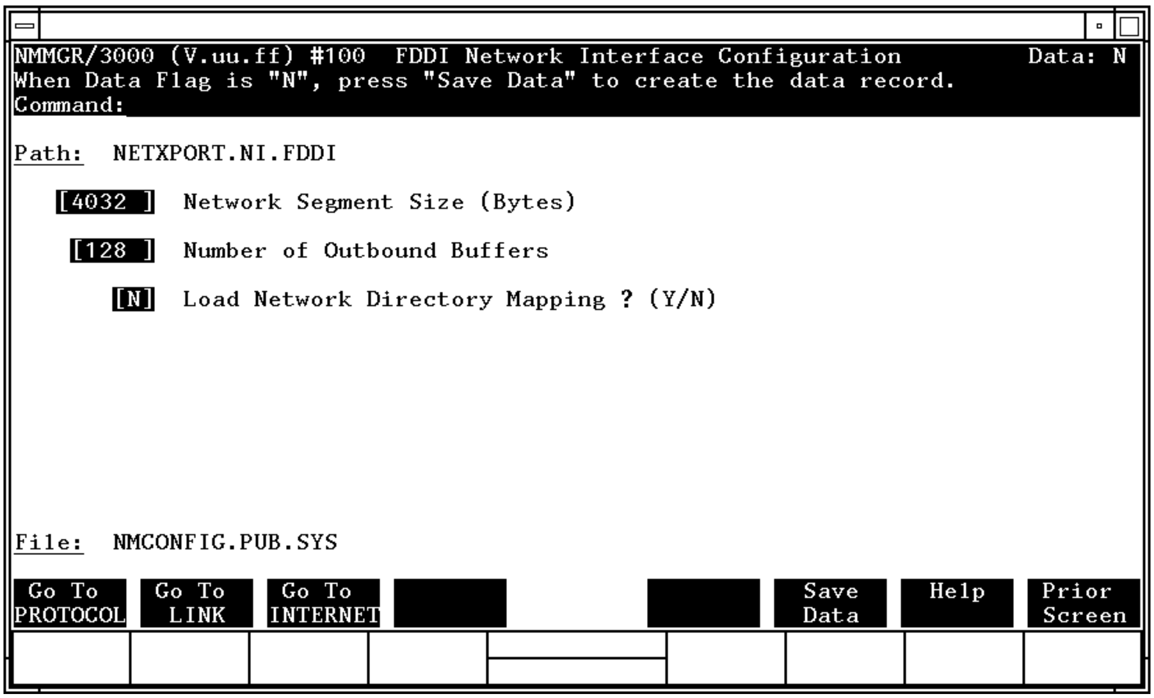
FDDI Network Interface Configuration

The FDDI Network Interface Configuration screen (#100) in Figure 9-3 is displayed when you select an NI name and the NI type `FDDI` at the Network Interface Configuration screen (Figure 9-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI name.

Figure 9-3 FDDI Network Interface Configuration Screen



The FDDI network interface (NI) module serves to interface the upper layers of the transport product to the link layer. This screen supplies the information required for that interface. All of the fields are used for internal resource allocation.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. 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 FDDI network interface link, and internetwork routing.

Choose the item you wish to configure, and press the corresponding key.

Fields

`Network segment size` This field specifies the largest packet that will be sent by the FDDI device. The only reason for entering a value smaller than 4032 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: 4032 bytes

Range: 256–4600

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Overallocation may waste core memory.

Related screen:

- `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: 128

Range: 128–4096

`Load network directory mapping? (Y/N)` Specifies whether or not the system should load mappings from the network directory at network startup. If you have non-HP nodes on the FDDI (nodes that do not support the ARP protocol,) you must enter these nodes into the network directory and set load network directory mapping to Y.

HP recommends the default unless non-HP nodes are on the network and the network directory has been successfully completed. Refer to Chapter 15, “Network Directory,” for information about the network directory.

Default value: N

Range: Y or N

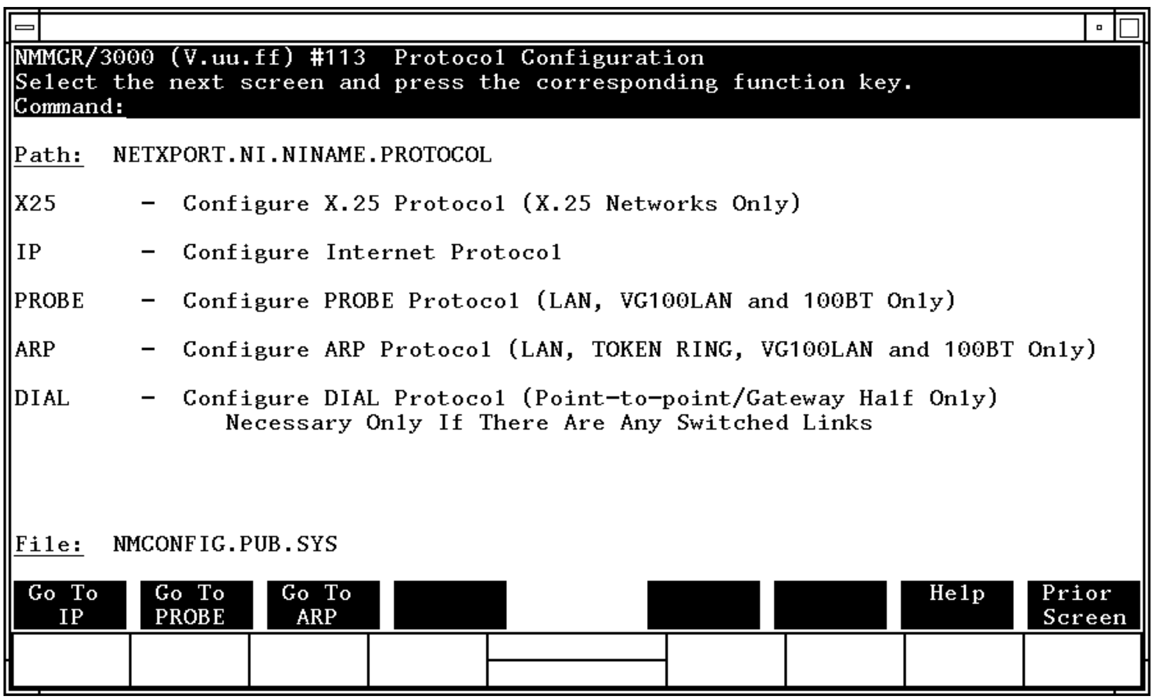
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 9-4 is displayed when you press the **[Go To Protocol]** function key at the FDDI Network Interface Configuration screen (Figure 9-3). This screen is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the Command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI.

Figure 9-4 Protocol Configuration Screen



For the FDDI NI, you configure the IP and ARP protocols. Choose the protocol to configure and press the corresponding function key.

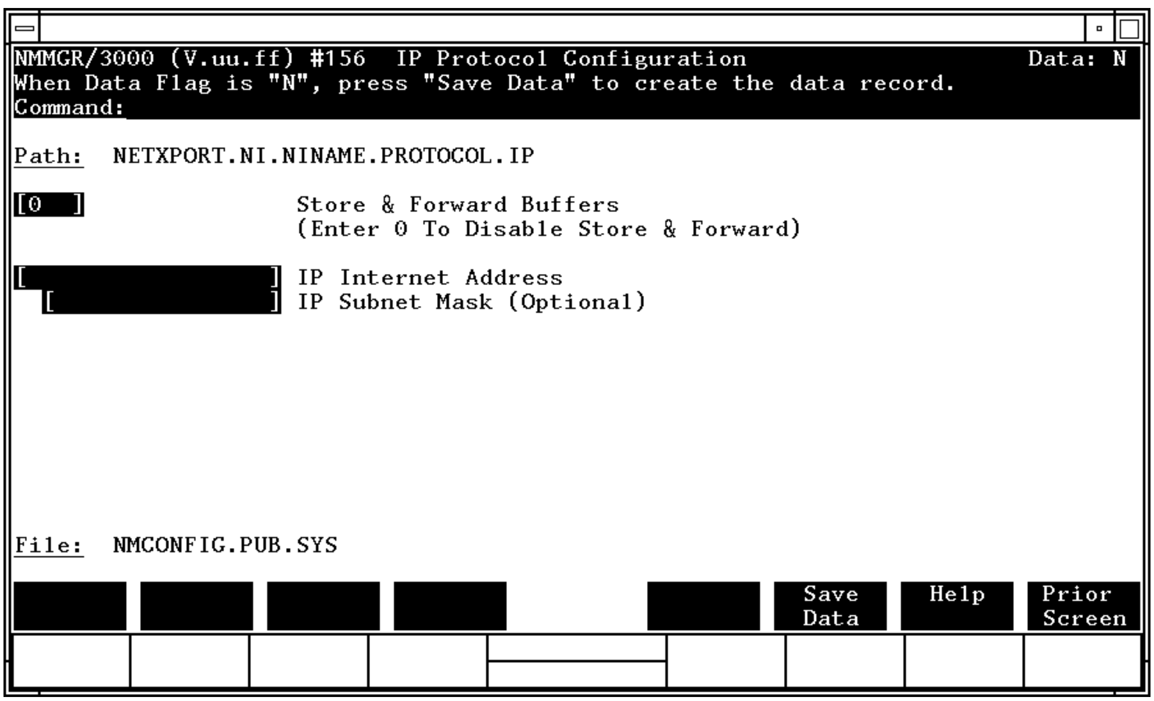
Internet Protocol Configuration

The IP Protocol Configuration screen (#156) in Figure 9-5 is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 9-4). It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.PROTOCOL.IP

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI.

Figure 9-5 IP Protocol Configuration Screen



This screen is used to supply IP protocol information for the network being configured. Each NI has an IP address. The IP address field is a key element in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI named in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

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 you are configuring a non-gateway node on this network. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface.

The number of store-and-forward buffers can be configured to allow performance tuning for different network types. However, HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

If store-and-forward is to be disallowed, set this number to 0.

Default value: 0

Range: 0–50

NOTE If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

`Class C:     C nnn.nnn.nnn xxx`

`Class B:     B nnn.nnn xxx.xxx`

`Class A:     A nnn xxx.xxx.xxx`

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node 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:     001–126`

Network and node values of all zeros or all ones are not allowed. These are special values.

Default value: No default, but a value *must* be supplied.

`IP subnet mask (optional)` An IP subnet mask is used when configuring subnetworks. The mask identifies which bits on an IP address will be used to define a subnetwork. An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by a period "." or a space. For example, a mask for a class A network with the subnet field being the first 8 bits of the **node** portion would be expressed as 255 255.000.000. The default is no IP mask.

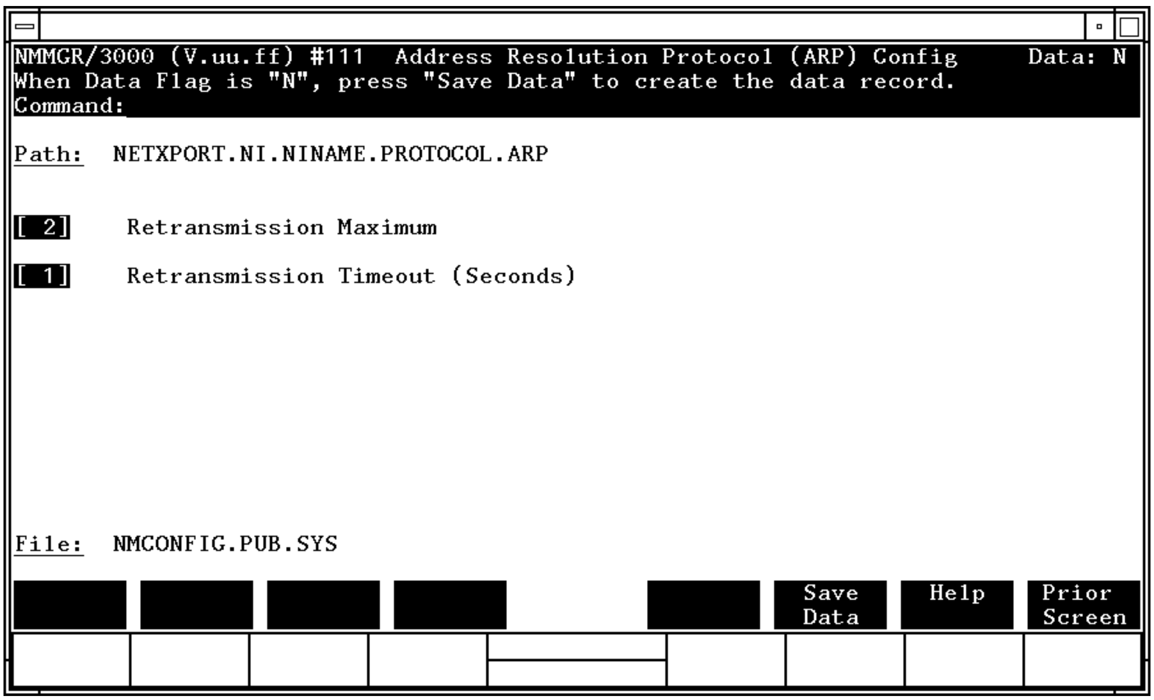
Address Resolution Protocol (ARP) Configuration

The Address Resolution Protocol (ARP) Configuration screen (#111) in Figure 9-6 is displayed when you press the **[Go To ARP]** function key at the Protocol Configuration screen (Figure 9-4). It is also displayed when you type the path name:

`@NETXPORT.`*`NI.NIname`*`.PROTOCOL.ARP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI.

Figure 9-6 Address Resolution Protocol (ARP) Configuration Screen



This screen allows you to configure the information required for the address resolution protocol (ARP). The ARP protocol exists on a FDDI network to provide a means of exchanging addressing information between nodes.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking the Data flag is set to Y.

Fields

`Retransmission maximum`

This is the maximum number of times that an ARP request packet will be retransmitted. If an ARP reply packet for this request is not received after this number of retransmissions, the attempted address resolution is considered to have failed. This value is bound closely to the retransmission timeout value. Taken together, they represent the total time to report an address resolution failure.

In general, the value of this field should be kept low.

Default value: 2

Range: 1–10

`Retransmission timeout (seconds)`

This is the time interval (in seconds) between ARP retransmissions. The value should be set large enough to avoid retransmissions in a temporarily overloaded environment, yet the value should be small enough to receive a timely failure report when a failure is inevitable.

Default value: 1

Range: 1–10

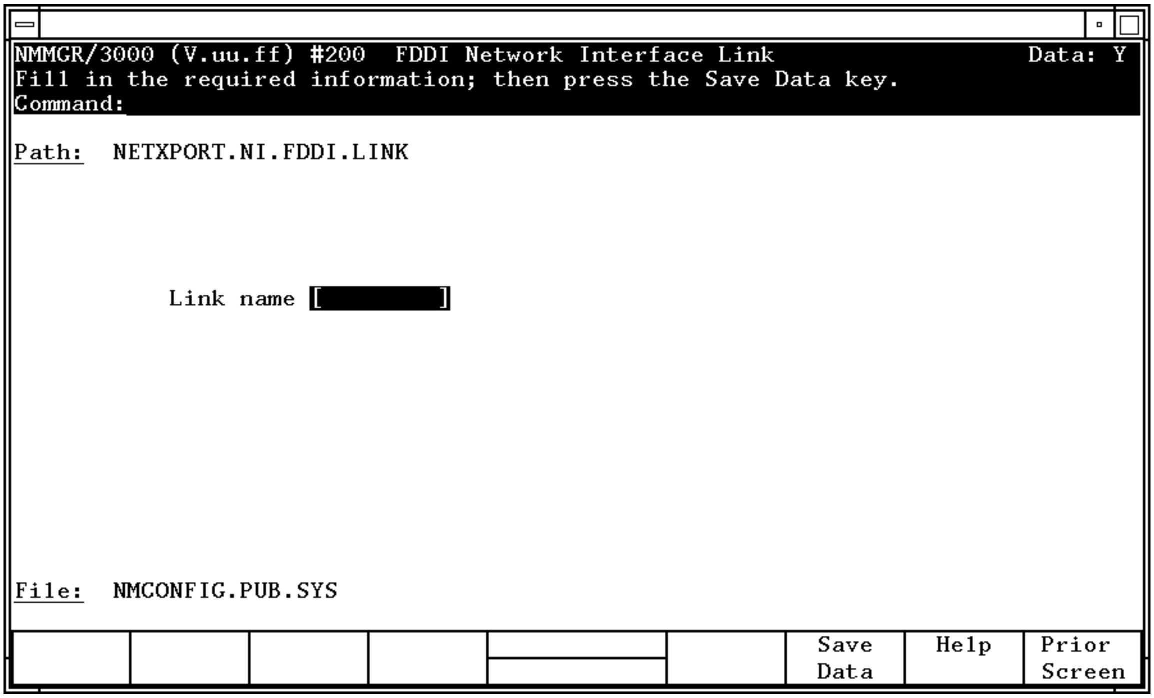
FDDI Network Interface Links

The FDDI Network Interface Links screen (#200) in Figure 9-7 is displayed when you press the **[Go To LINK]** function key at the FDDI Network Interface Configuration screen (Figure 9-3). It is also displayed when you type the path name:

`@NETXPORT.`*`NI.NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI.

Figure 9-7 FDDI Network Inteface Links Screen



Use the fields and the function keys of this select screen to bind the FDDI NI to the link. Enter the link name in the `Link name` field and press the **[Save Data]** key. (If you wish to rename the link, simply enter the new name and press the **[Save Data]** key.)

Fields

`Link name` Make sure this is the same link name configured at the FDDI Link Configuration screen (path name `LINK`). Press the **[Save Data]** function key to save the link name in the configuration file. Verify that the link name has been configured by checking that the Data flag is set to Y.

This screen associates the link data with the FDDI network interface data. The link name is used by the network transport when establishing connections. The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

To change an existing link name, enter the new name in the `Link name` field and press the **[Save Data]** function key.

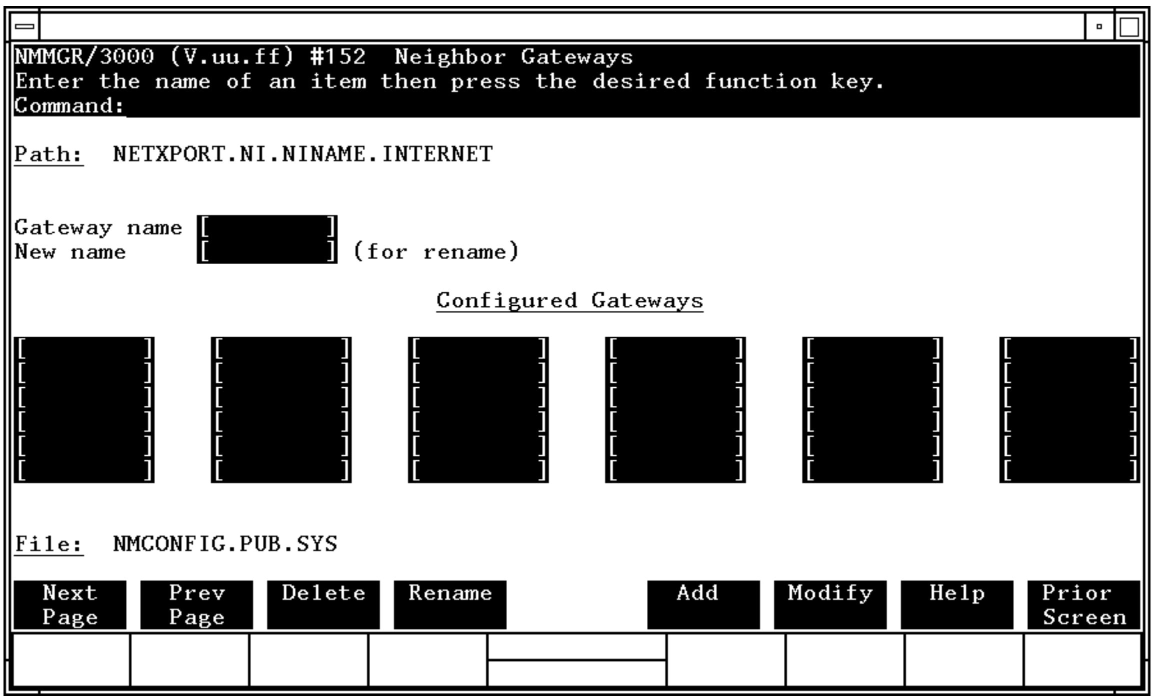
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 9-8 is displayed when you press the **[Go To INTERNET]** function key at the FDDI Network Interface Configuration screen (Figure 9-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI.

Figure 9-8 Neighbor Gateways Screen



Use this screen, and the screens that follow it, to identify the gateways on this network. Use the fields and the function keys of this select screen to perform the desired action.

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**

- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway, specify the gateway name and a new name; then press the **[Rename]** function key. 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, specify the gateway name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. 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 network numbers of all networks reachable from this gateway node.

Fields

`Gateway name` Enter a name to represent a gateway on this FDDI 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 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.

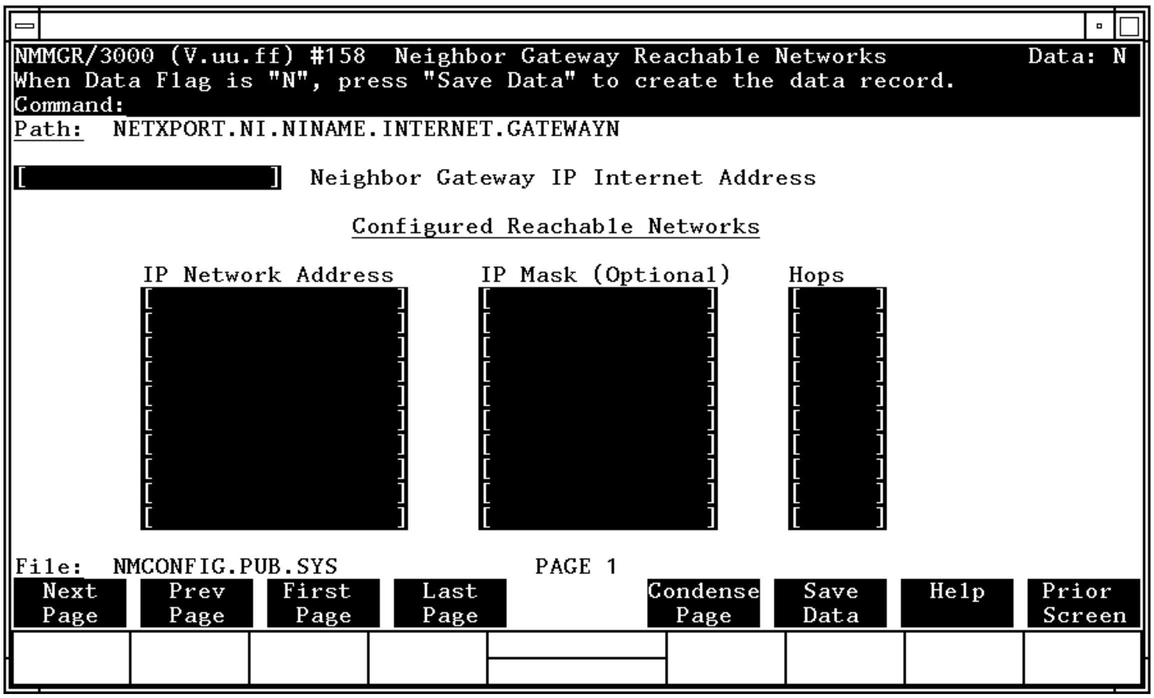
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 9-9 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 9-8) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.`*`gatewayn`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured FDDI NI, and *gatewayn* is the configured FDDI neighbor gateway name.

Figure 9-9 Neighbor Gateways Reachable Networks Screen



After you have entered all the required data, press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 internetwork 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; however, the node portion need not match.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node portion of the address.

Note that network and node values of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:     192–223`

`Class B:     128–191`

`Class A:     001–126`

The network address (network portion of the IP address) configured in `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` must match the neighbor gateway IP internet address configured in the current screen.

Default value: None

`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.

You can also designate this gateway as a default gateway by entering an "at" sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask, one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask configured in the IP Protocol Configuration screen (Figure 9-5) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnets.

  Related screen:

  - `NETXPORT.NI.`*`NIname`*`.INTERNET`

    This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask` The IP mask identifies a portion of the IP address for subnets. The subnet is specified in the same format as an IP address, that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the **node** portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, the network transport will choose internally from among the routes with equal hop counts.

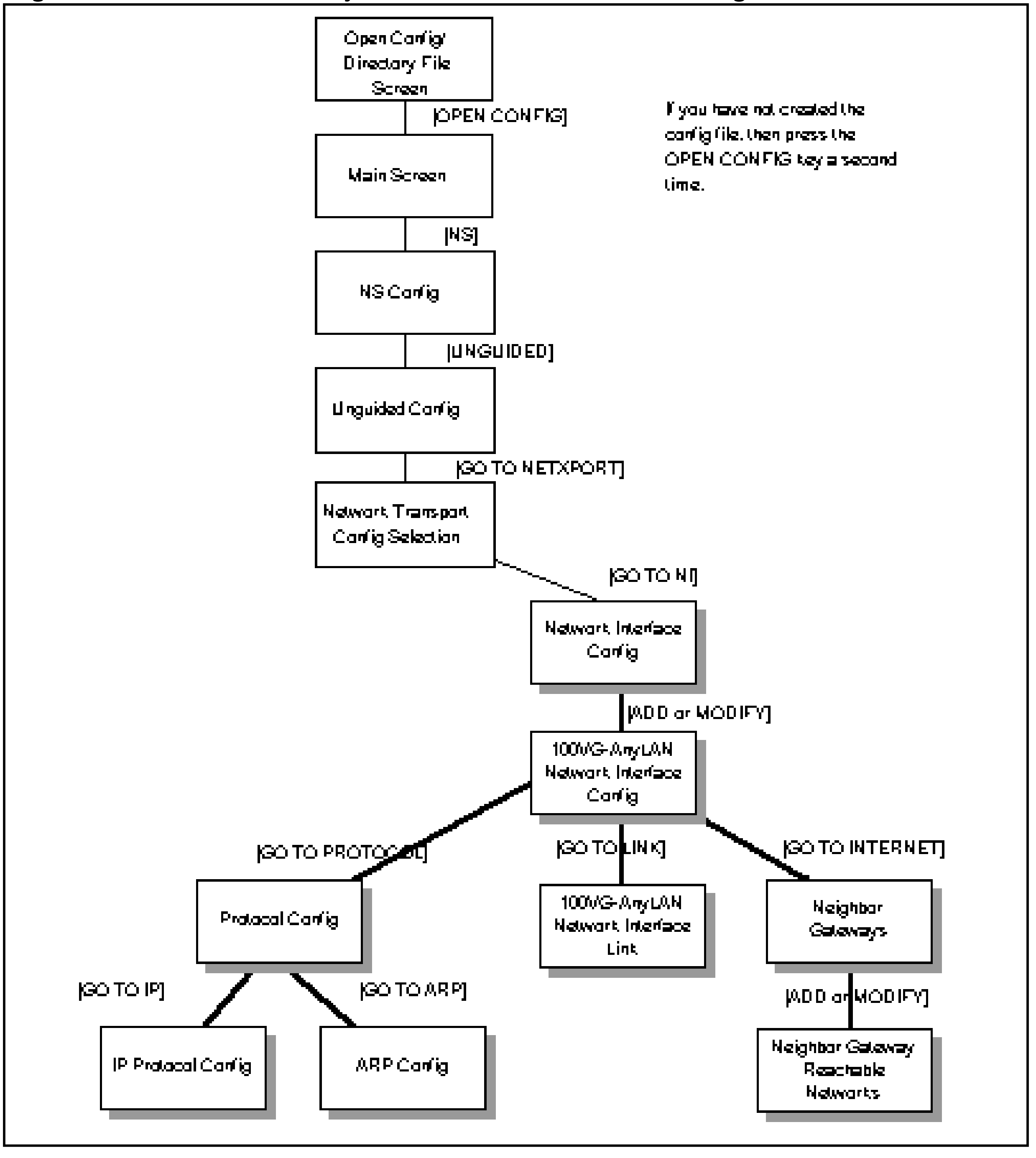
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

10 100VG-AnyLAN Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring an 100VG-AnyLAN network. Figure 10-1 shows the screen flow for configuring the 100VG-AnyLAN screens. Screens unique to the 100VG-AnyLAN network are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 10-1 100VG-AnyLAN Network Interface Configuration Screen Flow



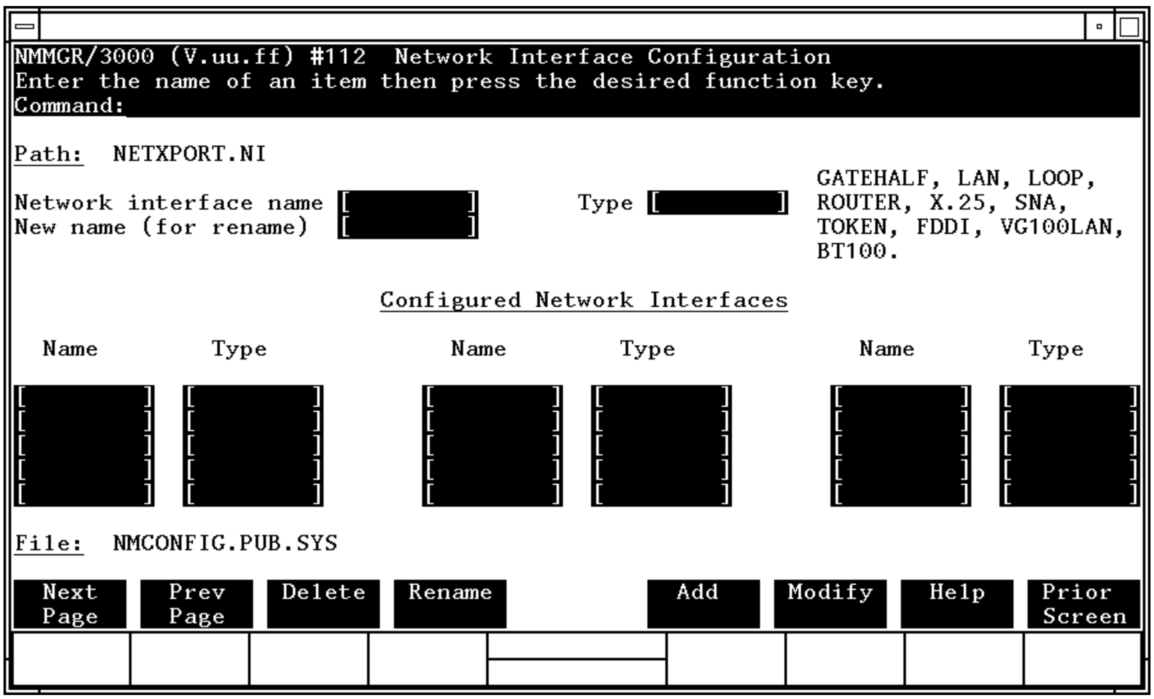
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 10-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

`@NETXPORT.NI`

in the command window of any screen and press the **[Enter]** key.

Figure 10-2 Network Interface Configuration Screen



Use the fields and the function keys of the select screen to perform the desired action:

- To define a new VG100LAN NI, specify the NI name and NI type `VG100LAN`; then press the **[Add]** function key. The path for the selected NI name is added to the configuration file and the data screen on that path is displayed. **You can have a maximum of 12 NI's per system (one NI must be used for loopback). However, HP supports up to two active VG100LAN NI's per system.**
- To modify an existing NI configuration, specify the NI name; then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) 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.

Fields

`Network interface name` Enter the network interface name for the LAN interface. The network interface name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, FDDI, VG100LAN,or BT100)` (Required only when adding an NI.) Enter `LAN` if you are configuring a local area network.

`New name` (Required only when renaming an NI.) 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.

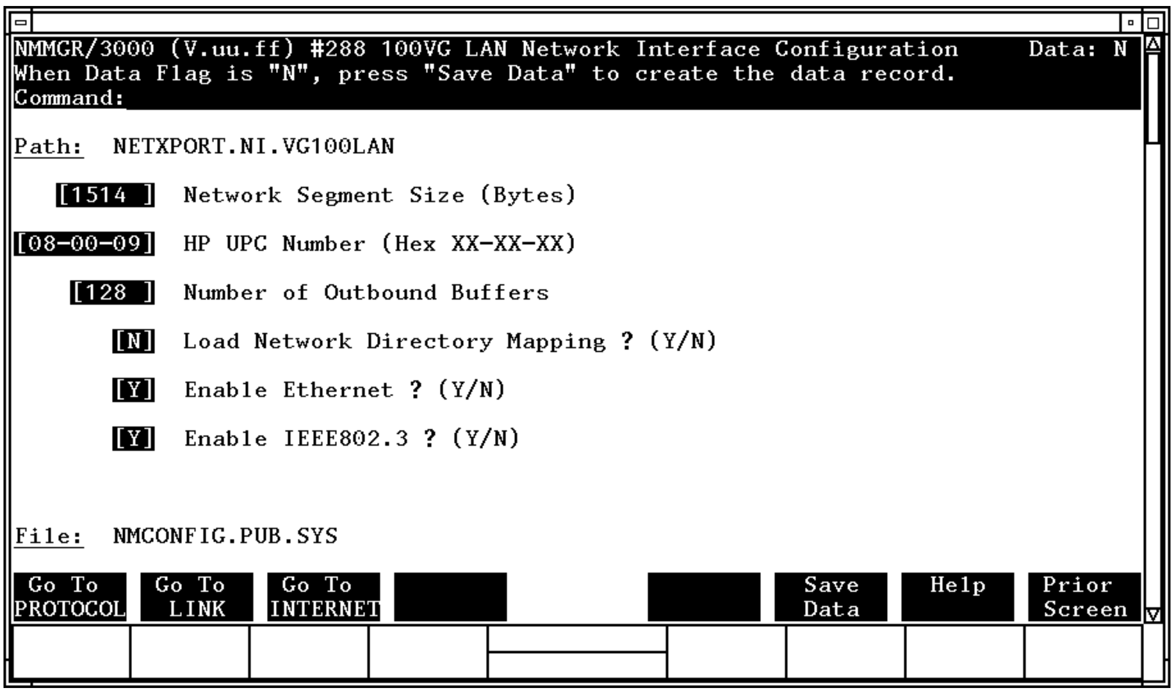
100VG-AnyLAN Network Interface Configuration

The 100VG-AnyLAN Network Interface Configuration screen (#288) in Figure 10-3 is displayed when you select an NI name and the NI type `VG100LAN` at the Network Interface Configuration screen (Figure 10-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI name.

Figure 10-3 VG100LAN Network Interface Configuration Screen



The VG100LAN network interface (NI) module serves to interface the upper layers of the transport product to the 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.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. 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 VG100LAN link and internetwork routing.

Choose the item you wish to configure, and press the corresponding key.

Fields

`Network segment size (bytes)` **(HP modifiable.)** This field specifies the largest packet (including all data, protocol headers, and link level headers) that will be sent by the 100VG-AnyLAN device. The only reason for entering a value smaller than 1514 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: 1514 bytes

Range: 300–1514

`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

Change the default only in rare circumstances. If all nodes on the LAN are not configured with identical HP UPC numbers, probe multicasts will not be universally recognized by nodes on the network.

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Overallocation may waste core memory.

Related screen:

- `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: 128

Range: 128–4096

`Load network directory mapping? (Y/N)`

If you have non-HP nodes on the network(nodes that do not support either ARP or probe protocols,) you must enter these nodes into the network directory and set load network directory mapping to Y.

HP recommends the default unless non-HP nodes are on the network and the network directory has been configured. Refer to Chapter 15, “Network Directory,” for information about the network directory.

Default value: N

Range: Y or N

`Enable Ethernet? (Y/N)`

This flag enables the Ethernet protocol to run either by itself or with the IEEE802.3 protocol. You can enable one or the other or both of these protocols simultaneously. One or the other *must* be enabled (you cannot disable both). Ethernet is enabled by default. Disabling Ethernet has the effect of disabling the ARP protocol as well.

Default value: Y

Range: Y or N

`Enable IEEE802.3? (Y/N)`

This flag enables the IEEE 802.3 protocol to run either by itself or with the Ethernet protocol. You can enable one or the other or both of these protocols simultaneously. One or the other must be enabled (you cannot disable both). IEEE 802.3 is enabled by default. Disabling IEEE 802.3 has the effect of disabling the probe protocol as well.

Default value: Y

Range: Y or N

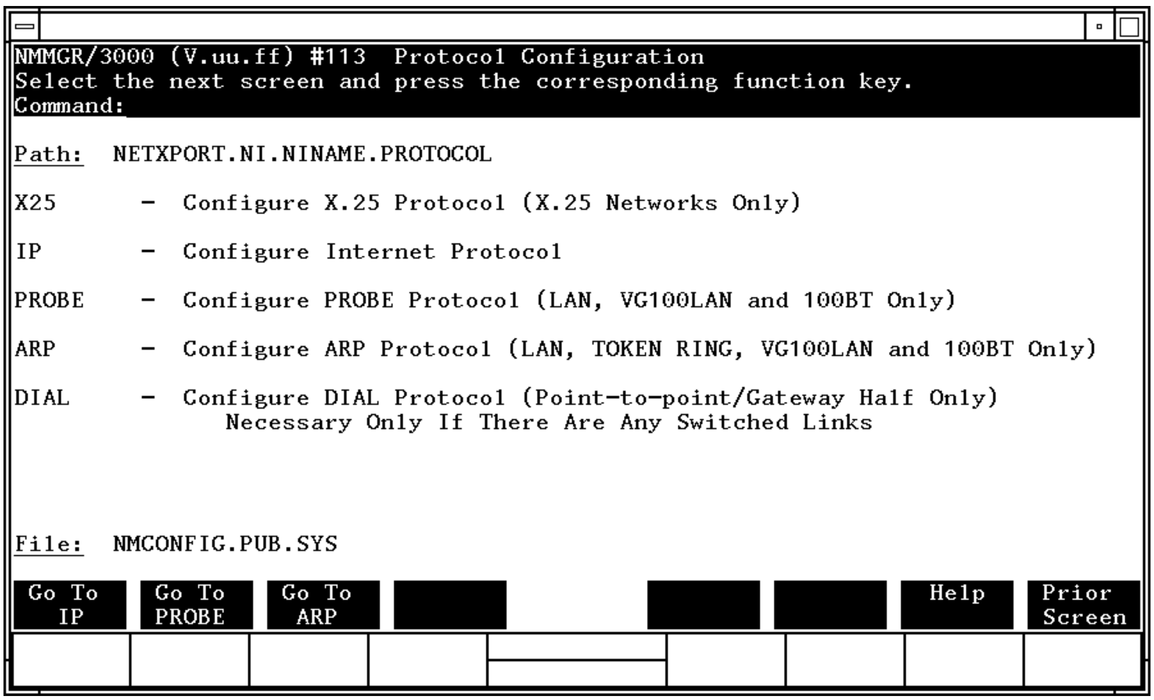
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 10-4 is displayed when you press the **[Go To PROTOCOL]** function key at the VG100LAN Network Interface Configuration screen (Figure 10-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI.

Figure 10-4 Protocol Configuration Screen



For the VG100LAN NI, you configure the IP, probe, and ARP protocols. Choose the protocol to configure, and press the corresponding function key.

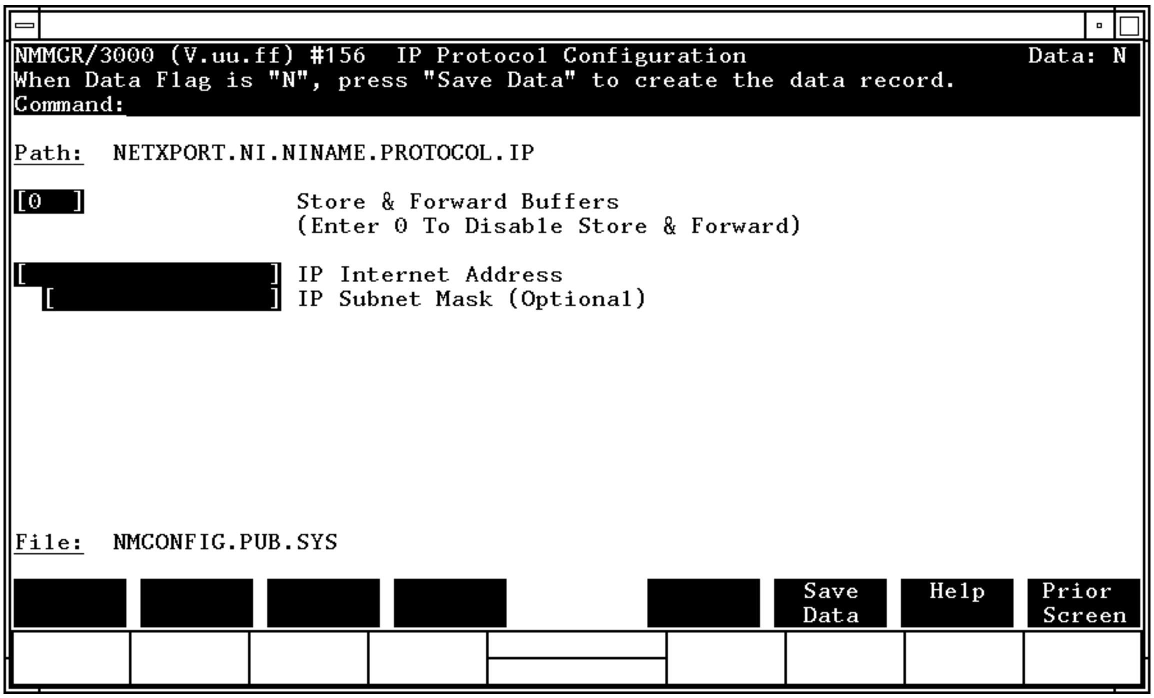
Internet Protocol Configuration

The IP Protocol Configuration screen (#156) in Figure 10-5 is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 10-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI.

Figure 10-5 IP Protocol Configuration Screen



This screen is used to supply IP protocol information for the network being configured. Each NI has an IP address. The IP address field is a key element in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI named in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

This field allocates buffers to support store-and-forward over the network interface being configured. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface. You can modify the number of store-and-forward buffers to allow performance tuning for different network types. HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

You do not need to allocate store-and-forward buffers if you are configuring a non-gateway node on this network. Leave the default (0) in this field to indicate that this is a non-gateway node.

Default value: 0

Range: 0–50

NOTE If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

`Class C:      C nnn.nnn.nnn xxx`

```
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and where *xxx* is a value ranging from 000 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:     001–126
```

Network and node values of all zeroes or all ones are not allowed. These are special values.

Default value: No default, but a value *must* be supplied.

`IP subnet mask (optional)` An IP subnet mask is used when configuring subnetworks. The mask identifies which bits of an IP address will be used to define a subnetwork. An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. For example, a mask for a Class A network with the subnet field being the first eight bits of the node part would be expressed as 255 255.000.000. The default is no IP subnet mask.

Refer to the *HP 3000/iX Network Planning and Configuration Guide* for more details on subnets.

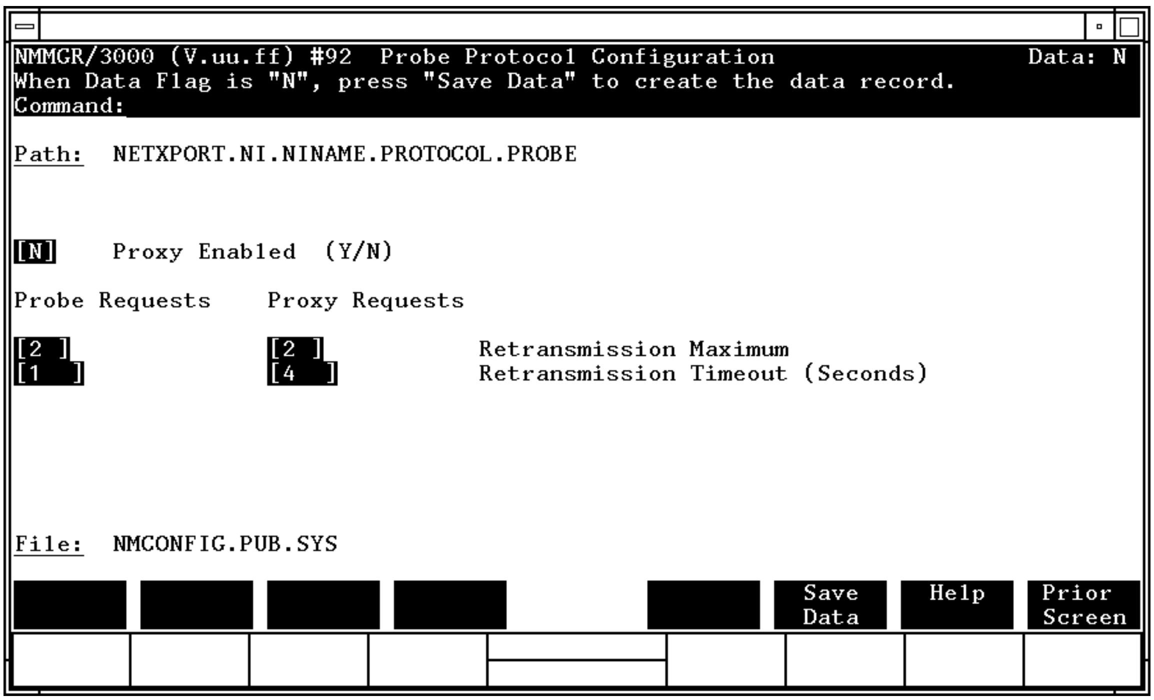
Probe Protocol Configuration

The Probe Protocol Configuration screen (#92) in Figure 10-6 is displayed when you press the **[Go To PROBE]** function at the Protocol Configuration screen (Figure 10-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.PROBE`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI.

Figure 10-6 Probe Protocol Configuration Screen



This screen allows you to configure the information required for the probe protocol. The probe protocol exists on a 100VG-AnyLAN network using the IEEE 802.3 protocol network to provide a means of exchanging addressing and naming information between nodes. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Proxy enabled (Y/N)`

Proxy nodes exist on networks to provide node name and address mapping facilities for nodes that do not have local network directories. Proxy requests are multicast on the network to request information about a third-party node from a proxy node.

`Y` means this node may be a proxy server and to answer all proxy requests on the network. `N` means this node will ignore all proxy requests on the network.

Default value: N

Range: Y or N

`Probe requests retransmission maximum`

This is the maximum number of transmissions of probe requests (name requests and address requests) before a probe failure is reported. Because it is unlikely that probe-request data is lost, HP recommends that you keep the maximum number of retransmissions low.

Default value: 2

Range: 1–10

`Probe requests retransmission timeout (seconds)`

This field is for specifying the time limit between retransmissions of probe requests. This is the time interval in seconds 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: 1

Range: 1–10

`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 lost, HP recommends that you keep the maximum number of retransmissions low.

Default value: 2

Range: 1–10

`Proxy requests retransmission timeout (seconds)`

The time interval in seconds 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: 4

Range: 1–10

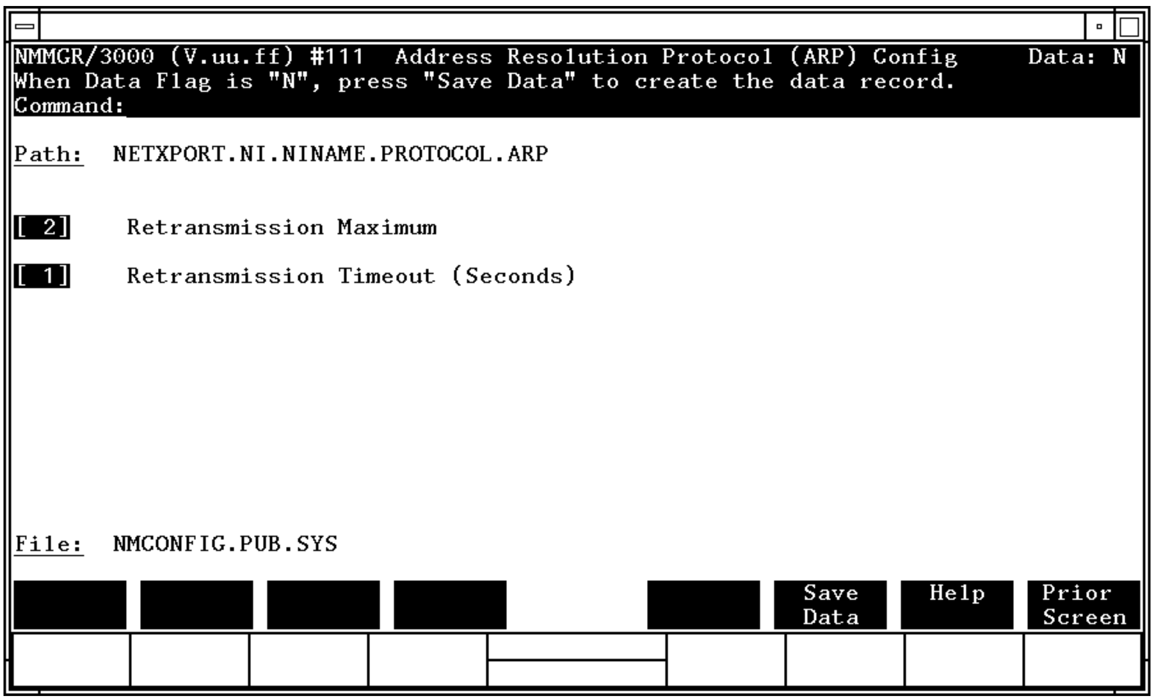
Address Resolution Protocol (ARP) Configuration

The Address Resolution Protocol (ARP) Configuration screen (#111) in Figure 10-7 is displayed when you press the **[Go To ARP]** function key at the Protocol configuration screen (Figure 10-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.ARP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI.

Figure 10-7 Address Resolution Protocol (ARP) Configuration Screen



This screen allows you to configure the information required for the address resolution protocol (ARP). The ARP protocol exists on a 100VG-AnyLAN network using the Ethernet protocol to provide a means of exchanging addressing information between Ethernet nodes. With the concurrent configuration of IEEE 802.3 and Ethernet, both the probe and ARP protocols broadcast requests to all nodes on the network to resolve the station address of a given remote node.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Retransmission maximum`

This is the maximum number of times that an ARP request packet will be retransmitted. If an ARP reply packet for this request is not received after this number of retransmissions, the attempted address resolution is considered to have failed. This value is bound closely to the retransmission timeout value as described. Taken together, they represent the total time to report an address resolution failure.

In general, the value of this field should be kept low.

Default value: 2

Range: 1–10

`Retransmission timeout (seconds)`

This is the time interval (in seconds) between ARP retransmissions. The value should be set large enough to avoid retransmissions in a temporarily overloaded environment, yet the value should be small enough to receive a timely failure report when a failure is inevitable.

Default value: 1

Range: 1–10

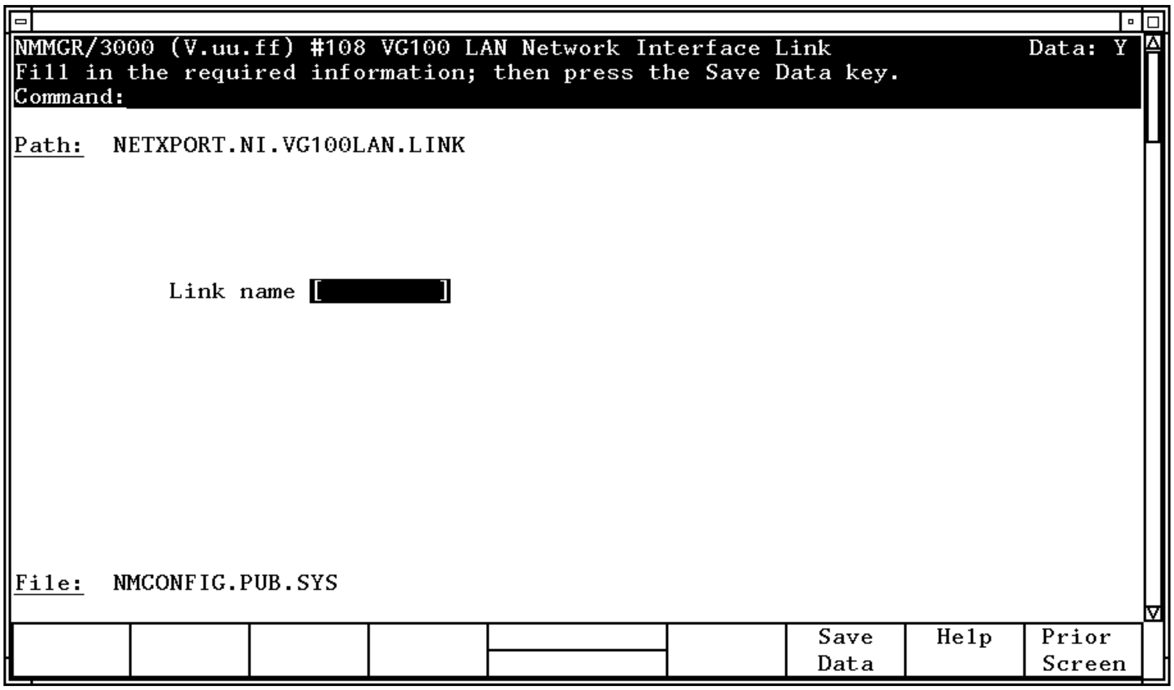
100VG-AnyLAN Network Interface Link

The 100VG-AnyLAN Network Interface Link screen (#108) in Figure 10-8 is displayed when you press the **[Go To LINK]** function key at the VG100LAN Network Interface Configuration screen (Figure 10-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI.

Figure 10-8 VG100LAN Network Interface Link Screen



Use this screen to specify the link name for the NI. The link name is used by the network transport when establishing connections.

Fields

`Link name` Make sure this is the same link name configured at the LAN Link Configuration screen (path name `LINK`). Press the **[Save Data]** function key to save the link name in the configuration file. Verify that the link name has been configured by checking that the Data flag is set to Y.

This screen associates the link data with the VG100LAN network interface data. The link name is used by the network transport when establishing connections. The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

To change an existing link name, enter the new name in the `Link name` field and press the **[Save Data]** function key.

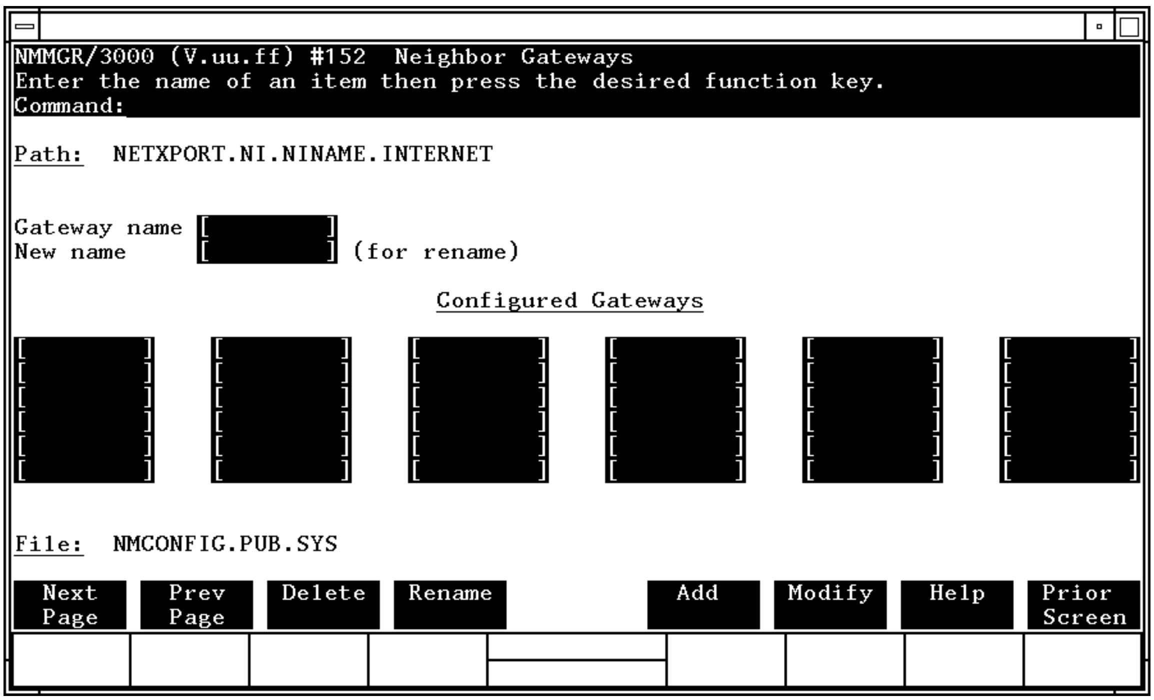
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 10-9 is displayed when you press the **[Go To INTERNET]** function key at the VG100LAN Network Interface Configuration screen (Figure 10-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI.

Figure 10-9 Neighbor Gateway Screen



Use this screen, and the screens that follow it, to identify the gateways on this network. Use the fields and the function keys of this select screen to perform the desired action as follows:

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**
- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway, specify the gateway name and a new name; then press the **[Rename]** function key. 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, specify the gateway name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. 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 network numbers of all networks reachable from this gateway node.

Fields

`Gateway name` Enter a name to represent a gateway on this 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 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.

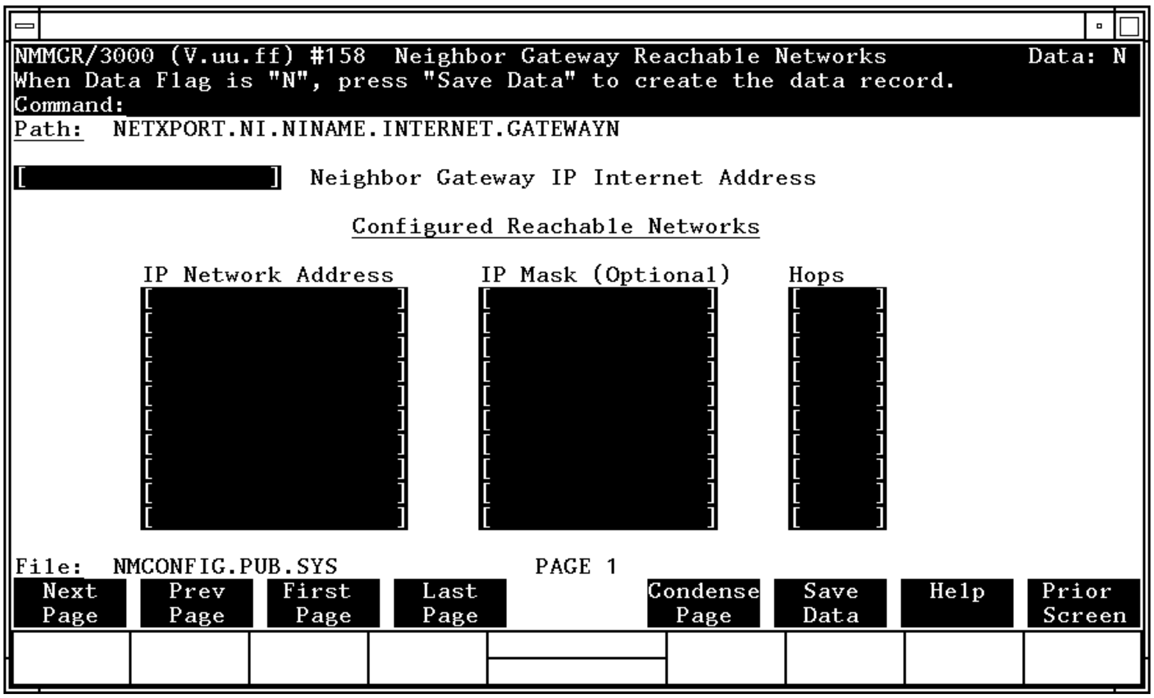
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 10-10 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 10-9) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.gatewayn`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured VG100LAN NI, and *gatewayn* is the configured VG100LAN NI gateway name.

Figure 10-10 Neighbor Gateway Reachable Networks Screen



After you have entered all the required data, press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 configured reachable networks. 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 internetwork 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; however, the node portion need not match.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The possible classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx

Class B:     B nnn.nnn xxx.xxx

Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and xxx is a value ranging from 000 to 255, representing the node portion of the address. Note that network and node values of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:     192–223`

`Class B:     128–191`

`Class A:     001–126`

The network address (network portion of the IP address) configured in `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` must match the neighbor gateway IP internet address configured in the current screen.

Default value: None

`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.

You can also designate this gateway as a default gateway by entering an “at” sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask entered in the IP Protocol Configuration screen (Figure 10-5) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnetting.

Related screen:

- `NETXPORT.NI.`*`NIname`*`.INTERNET`

  This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask`

The IP mask identifies a portion of the IP address for subnets. The subnet is specified in the same format as an IP address; that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the *node* portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, the network transport will choose internally from among the routes with equal hop counts.

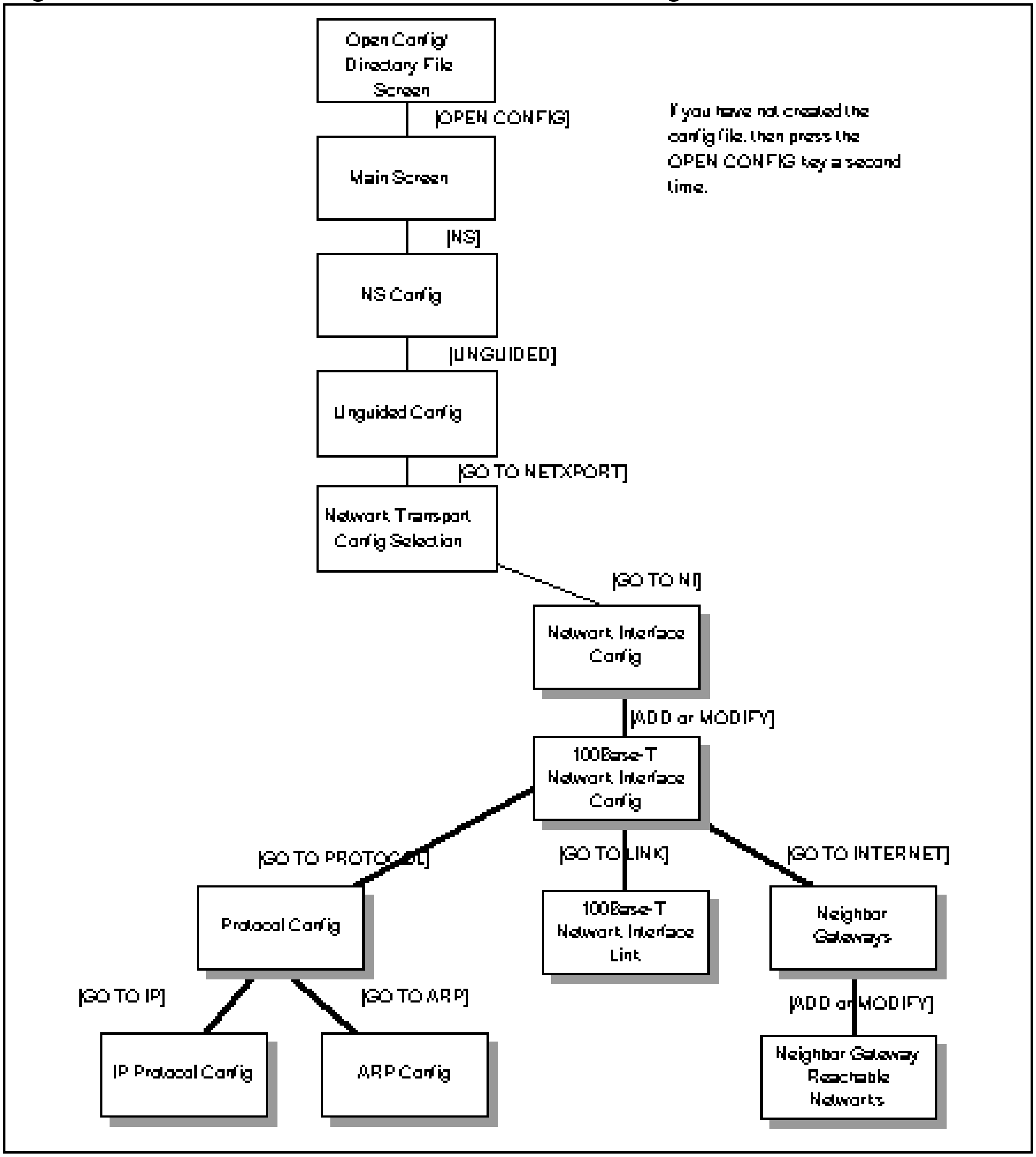
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

11 100Base-T Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring an I100Base-T network. Figure 11-1 shows the screen flow for configuring the 100Base-T screens. Screens unique to the 100Base-T network are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 11-1 100Base-T Network Interface Configuration Screen Flow



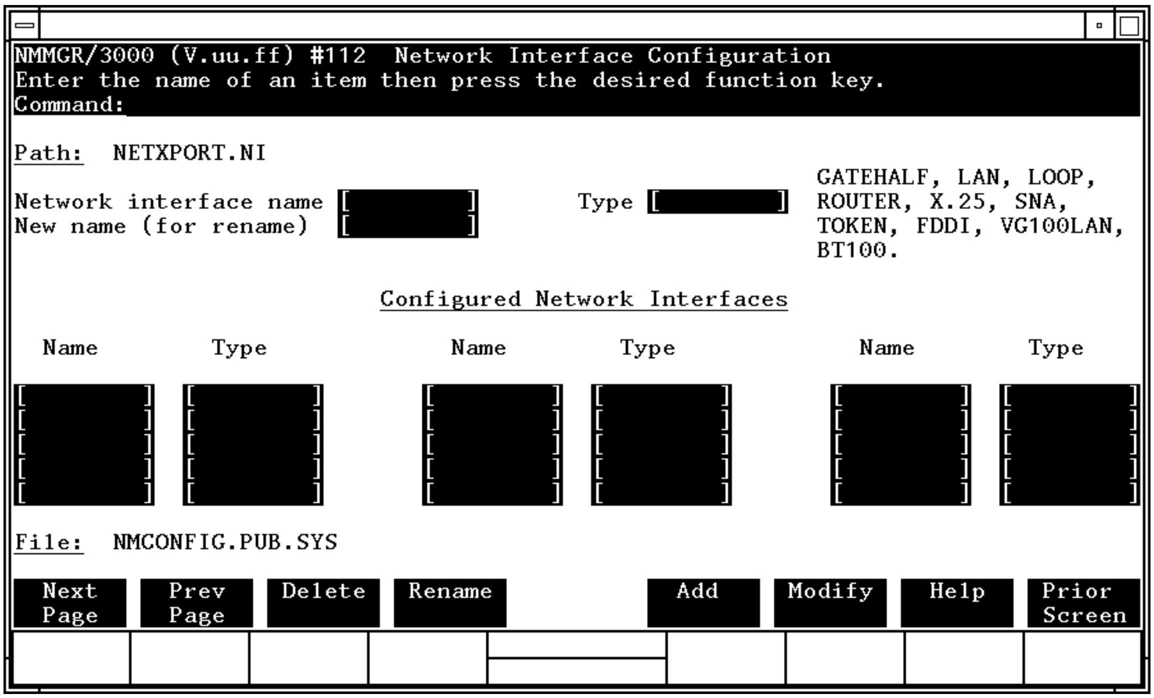
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 11-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration Selection screen (Figure 4-2). It is also displayed when you type the path name:

`@NETXPORT.NI`

in the command window of any screen and press the **[Enter]** key.

Figure 11-2 Network Interface Configuration Screen



Use the fields and the function keys of the select screen to perform the desired action:

- To define a new BT100 NI, specify the NI name and NI type `BY100`; then press the **[Add]** function key. The path for the selected NI name is added to the configuration file and the data screen on that path is displayed. **You can have a maximum of 12 NI's per system (one NI must be used for loopback). However, HP supports up to two active BT100 NI's per system.**
- To modify an existing NI configuration, specify the NI name; then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured NI name (and the associated data) 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.

Fields

`Network interface name` Enter the network interface name for the LAN interface. The network interface name can contain as many as eight alphanumeric characters; the first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, FDDI, VG100LAN, or BT100)` (Required only when adding an NI.) Enter `LAN` if you are configuring a local area network.

`New name` (Required only when renaming an NI.) 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.

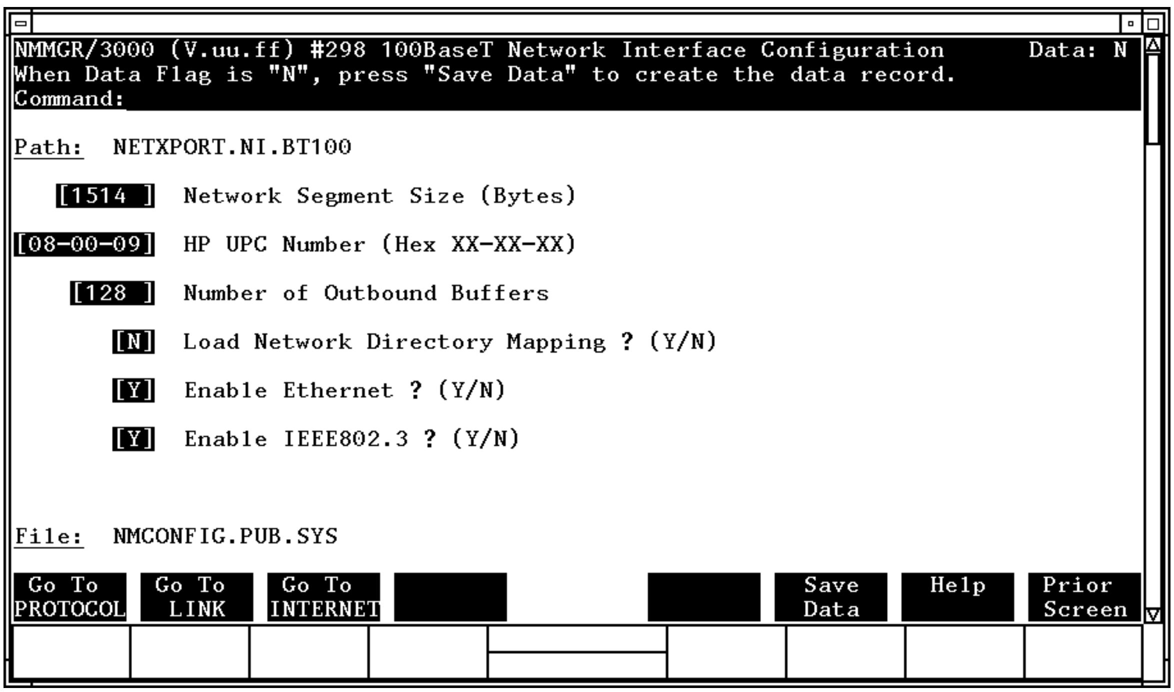
100Base-T Network Interface Configuration

The 100Base-T Network Interface Configuration screen (#298) in Figure 11-3 is displayed when you select an NI name and the NI type `BT100` at the Network Interface Configuration screen (Figure 11-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI name.

Figure 11-3 BT100 Network Interface Configuration Screen



The BT100 network interface (NI) module serves to interface the upper layers of the transport product to the 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.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. 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 BT100 link and internetwork routing.

Choose the item you wish to configure, and press the corresponding key.

Fields

`Network segment size (bytes)` **(HP modifiable.)** This field specifies the largest packet (including all data, protocol headers, and link level headers) that will be sent by the 100Base-T device. The only reason for entering a value smaller than 1514 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: 1514 bytes

Range: 300–1514

`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

Change the default only in rare circumstances. If all nodes on the LAN are not configured with identical HP UPC numbers, probe multicasts will not be universally recognized by nodes on the network.

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput. Overallocation may waste core memory.

Related screen:

- `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: 128

Range: 128–4096

`Load network directory mapping? (Y/N)`

If you have non-HP nodes on the network (nodes that do not support either ARP or probe protocols,) you must enter these nodes into the network directory and set load network directory mapping to Y.

HP recommends the default unless non-HP nodes are on the network and the network directory has been configured. Refer to Chapter 15, “Network Directory,” for information about the network directory.

Default value: N

Range: Y or N

`Enable Ethernet? (Y/N)`

This flag enables the Ethernet protocol to run either by itself or with the IEEE802.3 protocol. You can enable one or the other or both of these protocols simultaneously. One or the other *must* be enabled (you cannot disable both). Ethernet is enabled by default. Disabling Ethernet has the effect of disabling the ARP protocol as well.

Default value: Y

Range: Y or N

`Enable IEEE802.3? (Y/N)`

This flag enables the IEEE 802.3 protocol to run either by itself or with the Ethernet protocol. You can enable one or the other or both of these protocols simultaneously. One or the other must be enabled (you cannot disable both). IEEE 802.3 is enabled by default. Disabling IEEE 802.3 has the effect of disabling the probe protocol as well.

Default value: Y

Range: Y or N

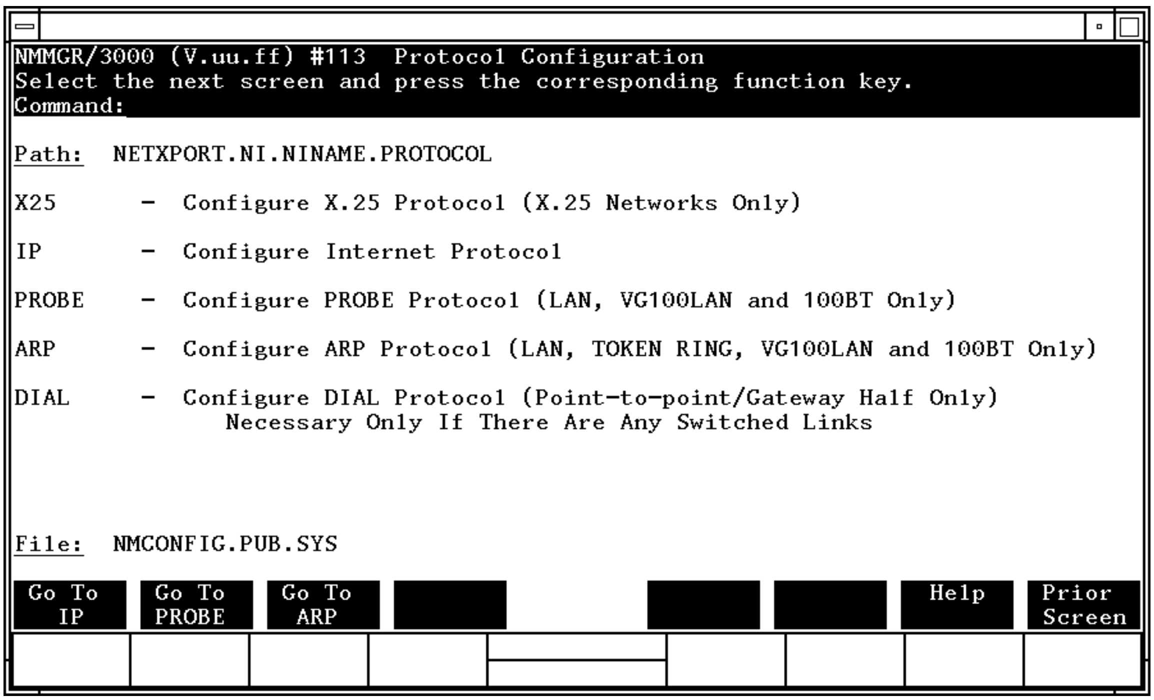
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 11-4 is displayed when you press the **[Go To PROTOCOL]** function key at the BT100 Network Interface Configuration screen (Figure 11-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BY100 NI.

Figure 11-4 Protocol Configuration Screen



For the BT100 NI, you configure the IP, probe, and ARP protocols. Choose the protocol to configure, and press the corresponding function key.

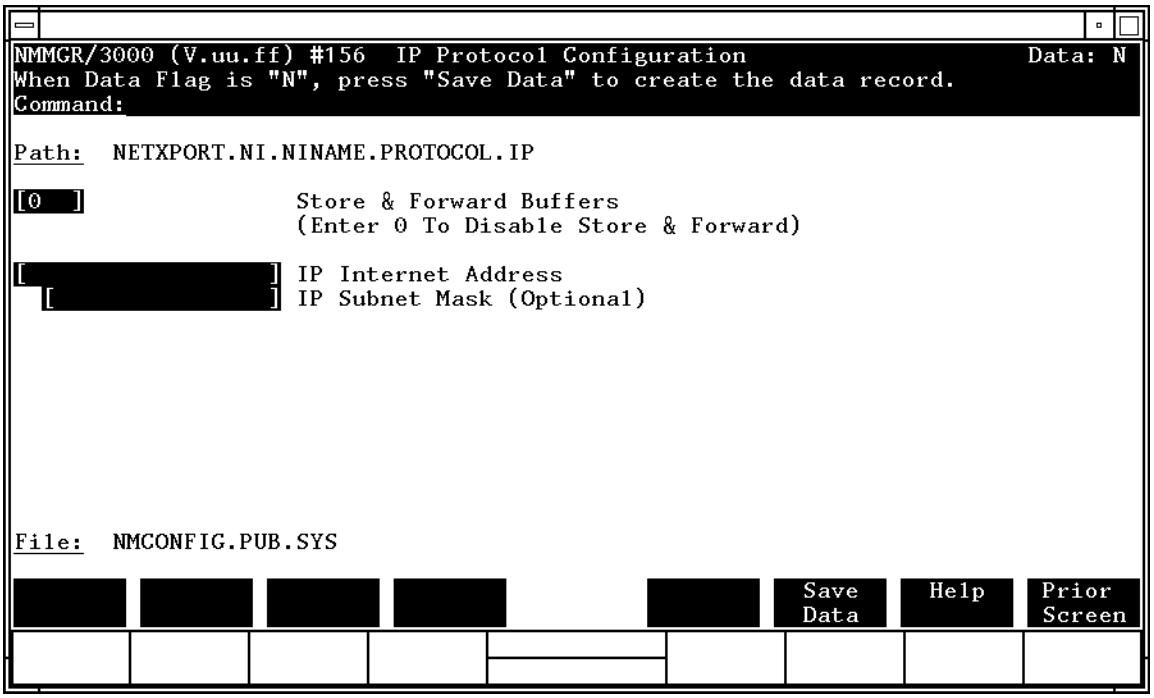
Internet Protocol Configuration

The IP Protocol Configuration screen (#156) in Figure 11-5 is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 11-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI.

Figure 11-5 IP Protocol Configuration Screen



This screen is used to supply IP protocol information for the network being configured. Each NI has an IP address. The IP address field is a key element in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI named in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

This field allocates buffers to support store-and-forward over the network interface being configured. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface. You can modify the number of store-and-forward buffers to allow performance tuning for different network types. HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

You do not need to allocate store-and-forward buffers if you are configuring a non-gateway node on this network. Leave the default (0) in this field to indicate that this is a non-gateway node.

Default value: 0

Range: 0–50

NOTE If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`IP internet address`

Enter the internet protocol (IP) address for the network interface being configured.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx
Class B:     B nnn.nnn xxx.xxx
Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and where *xxx* is a value ranging from 000 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:     001–126
```

Network and node values of all zeroes or all ones are not allowed. These are special values.

Default value: No default, but a value *must* be supplied.

`IP subnet mask (optional)`

An IP subnet mask is used when configuring subnetworks. The mask identifies which bits of an IP address will be used to define a subnetwork. An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. For example, a mask for a Class A network with the subnet field being the first eight bits of the node part would be expressed as 255 255.000.000. The default is no IP subnet mask.

Refer to the *HP 3000/iX Network Planning and Configuration Guide* for more details on subnets.

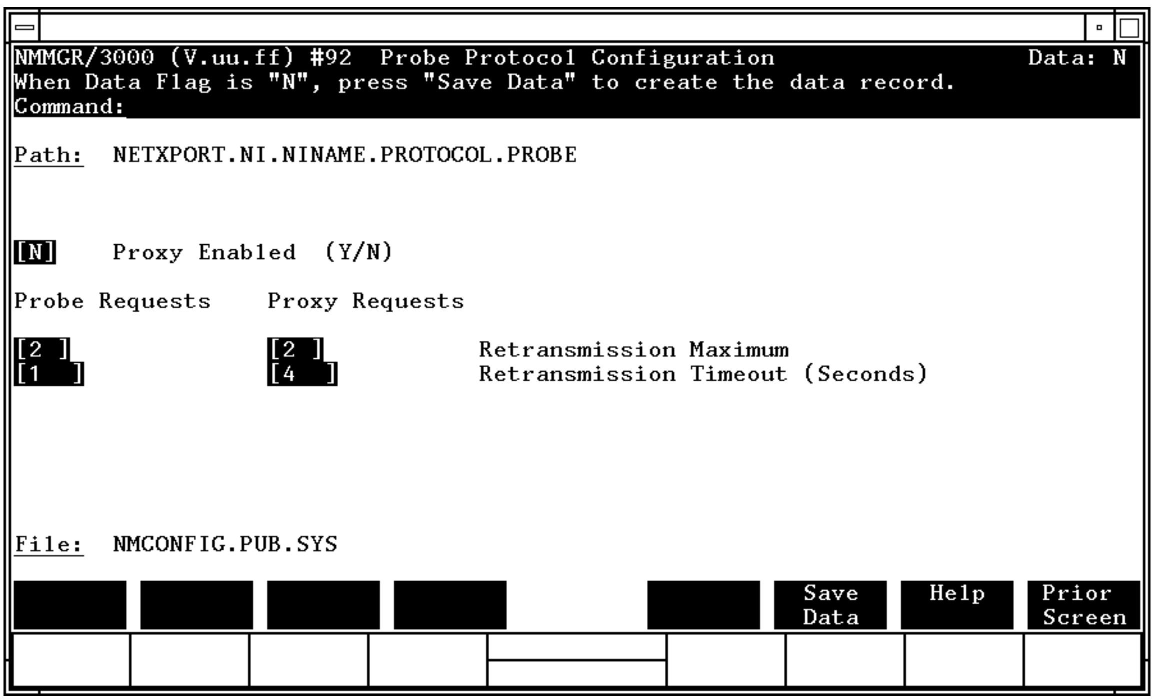
Probe Protocol Configuration

The Probe Protocol Configuration screen (#92) in Figure 11-6 is displayed when you press the **[Go To PROBE]** function at the Protocol Configuration screen (Figure 11-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.PROBE`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI.

Figure 11-6 Probe Protocol Configuration Screen



This screen allows you to configure the information required for the probe protocol. The probe protocol exists on a 100Base-T network using the IEEE 802.3 protocol to provide a means of exchanging addressing and naming information between nodes. Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Proxy enabled (Y/N)`

Proxy nodes exist on networks to provide node name and address mapping facilities for nodes that do not have local network directories. Proxy requests are multicast on the network to request information about a third-party node from a proxy node.

`Y` means this node may be a proxy server and to answer all proxy requests on the network. `N` means this node will ignore all proxy requests on the network.

Default value: N

Range: Y or N

`Probe requests retransmission maximum`

This is the maximum number of transmissions of probe requests (name requests and address requests) before a probe failure is reported. Because it is unlikely that probe-request data is lost, HP recommends that you keep the maximum number of retransmissions low.

Default value: 2

Range: 1–10

`Probe requests retransmission timeout (seconds)`

This field is for specifying the time limit between retransmissions of probe requests. This is the time interval in seconds 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: 1

Range: 1–10

`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 lost, HP recommends that you keep the maximum number of retransmissions low.

Default value: 2

Range: 1–10

`Proxy requests retransmission timeout (seconds)`

The time interval in seconds 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: 4

Range: 1–10

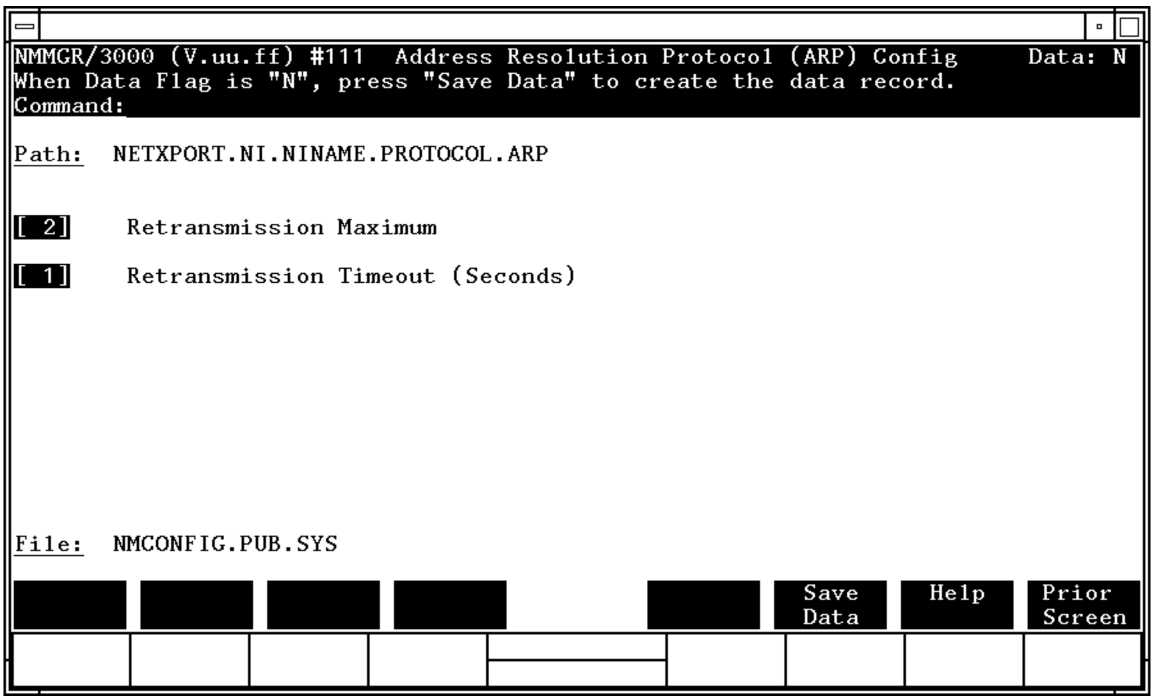
Address Resolution Protocol (ARP) Configuration

The Address Resolution Protocol (ARP) Configuration screen (#111) in Figure 11-7 is displayed when you press the **[Go To ARP]** function key at the Protocol configuration screen (Figure 11-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.ARP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI.

Figure 11-7 Address Resolution Protocol (ARP) Configuration Screen



This screen allows you to configure the information required for the address resolution protocol (ARP). The ARP protocol exists on an 100Base-T network using the Ethernet protocol to provide a means of exchanging addressing information between Ethernet nodes. With the concurrent configuration of IEEE 802.3 and Ethernet, both the probe and ARP protocols broadcast requests to all nodes on the network to resolve the LAN station address of a given remote node.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or modifying. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Retransmission maximum`

This is the maximum number of times that an ARP request packet will be retransmitted. If an ARP reply packet for this request is not received after this number of retransmissions, the attempted address resolution is considered to have failed. This value is bound closely to the retransmission timeout value as described. Taken together, they represent the total time to report an address resolution failure.

In general, the value of this field should be kept low.

Default value: 2

Range: 1–10

`Retransmission timeout (seconds)`

This is the time interval (in seconds) between ARP retransmissions. The value should be set large enough to avoid retransmissions in a temporarily overloaded environment, yet the value should be small enough to receive a timely failure report when a failure is inevitable.

Default value: 1

Range: 1–10

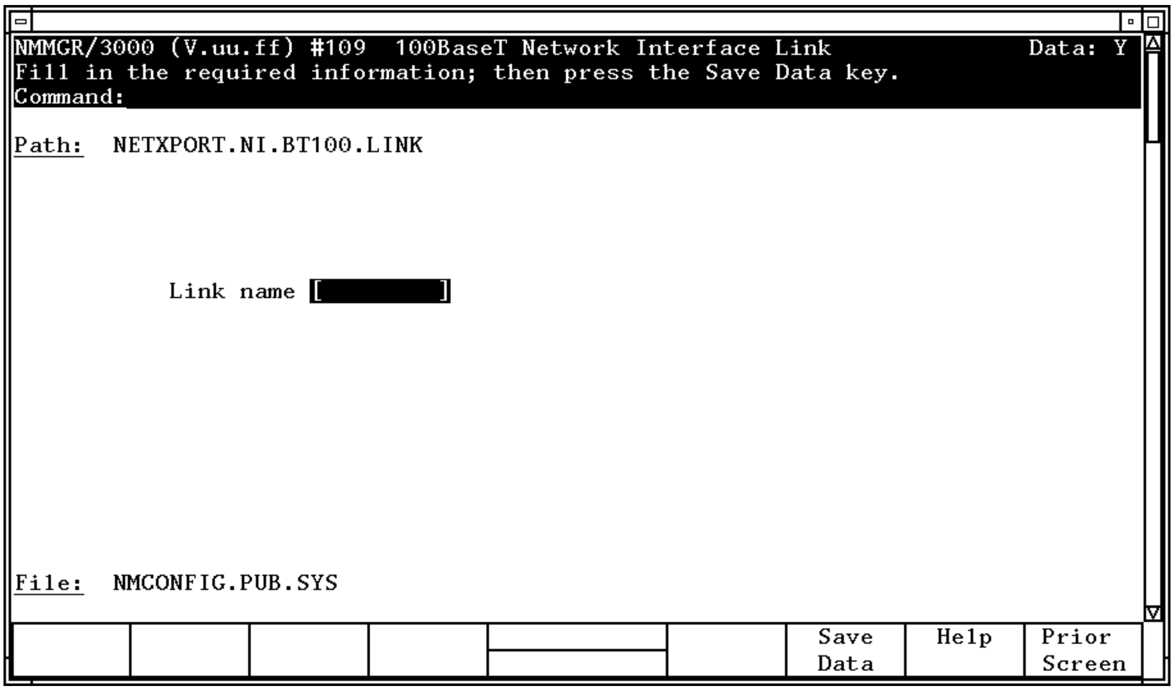
100Base-T Network Interface Link

The 100Base-T Network Interface Link screen (#109) in Figure 11-8 is displayed when you press the **[Go To LINK]** function key at the BT100 Network Interface Configuration screen (Figure 11-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI.

Figure 11-8 BT100 Network Interface Link Screen



Use this screen to specify the link name for the NI. The link name is used by the network transport when establishing connections.

Fields

`Link name` Make sure this is the same link name configured at the LAN Link Configuration screen (path name `LINK`). Press the **[Save Data]** function key to save the link name in the configuration file. Verify that the link name has been configured by checking that the Data flag is set to `Y`.

This screen associates the link data with the BT100 network interface data. The link name is used by the network transport when establishing connections. The link name can contain as many as eight alphanumeric characters, and the first character must be alphabetic.

To change an existing link name, enter the new name in the `Link name` field and press the **[Save Data]** function key.

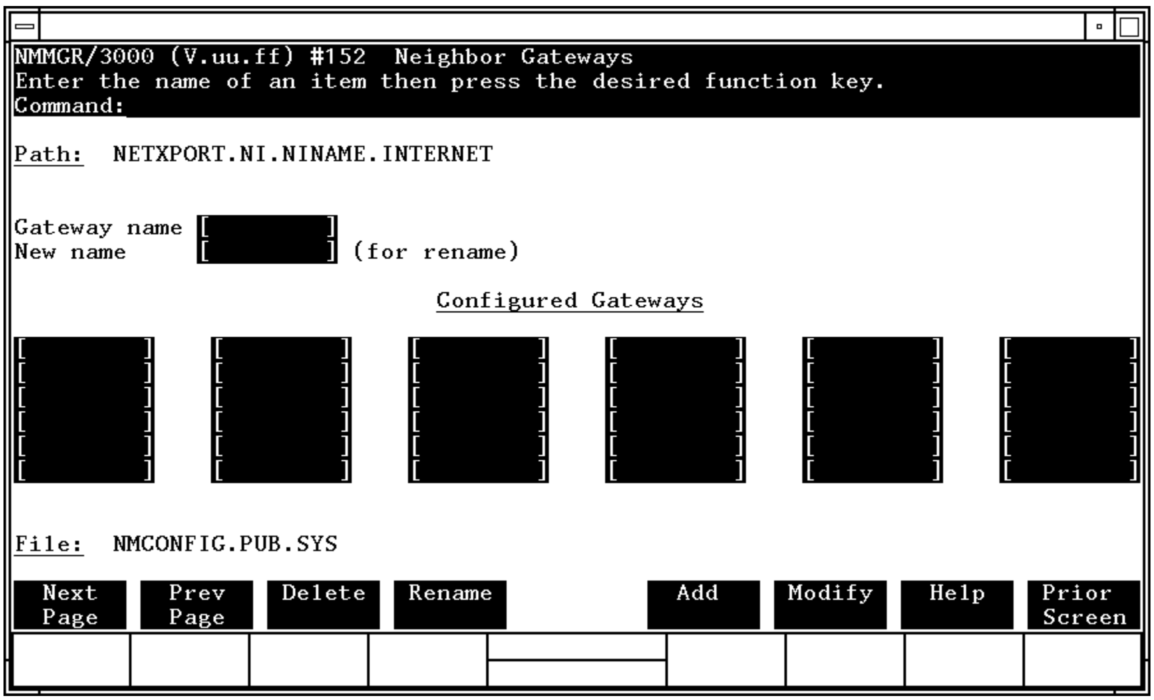
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 11-9 is displayed when you press the **[Go To INTERNET]** function key at the BT100 Network Interface Configuration screen (Figure 11-3). It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.INTERNET

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI.

Figure 11-9 Neighbor Gateways Screen



Use this screen, and the screens that follow it, to identify the gateways on this network. Use the fields and the function keys of this select screen to perform the desired action as follows:

- To identify a new gateway, specify the gateway name; then press the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**
- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. The data screen on the path for the specified gateway is displayed.

- To change the gateway name of an existing gateway, specify the gateway name and a new name; then press the **[Rename]** function key. 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, specify the gateway name; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. 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 network numbers of all networks reachable from this gateway node.

Fields

`Gateway name` Enter a name to represent a gateway on this 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 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.

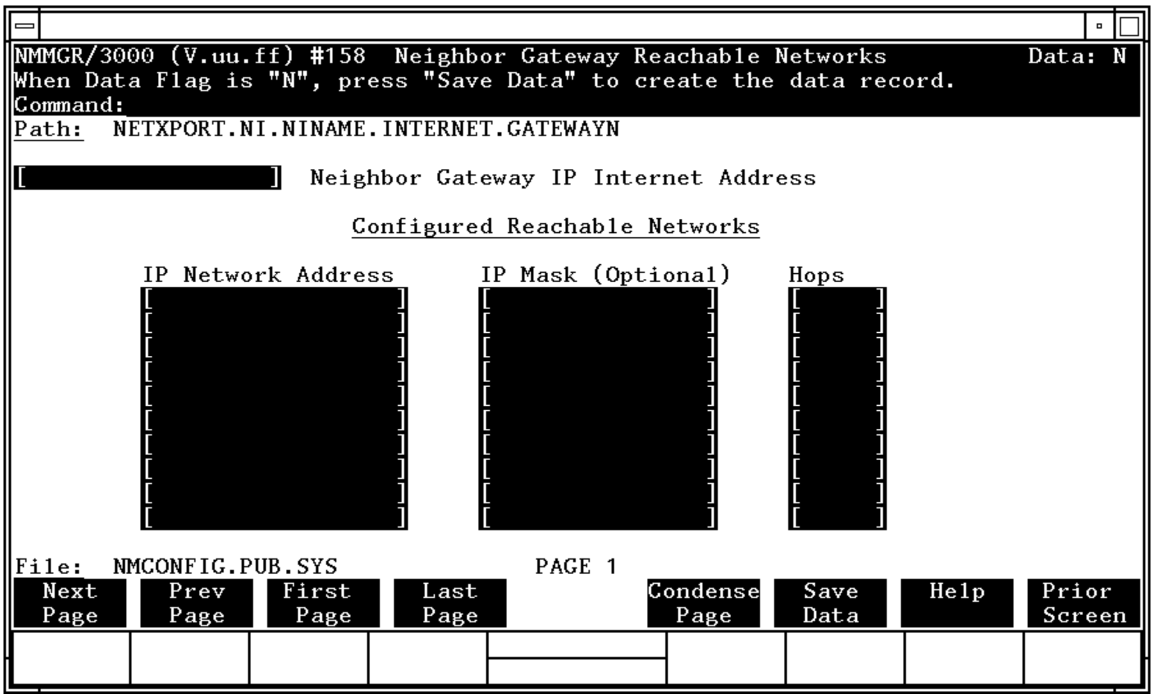
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 11-10 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 11-9) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.INTERNET.gatewayn

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured BT100 NI, and *gatewayn* is the configured BT100 NI gateway name.

Figure 11-10 Neighbor Gateway Reachable Networks Screen



After you have entered all the required data, press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 configured reachable networks. 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 internetwork 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; however, the node portion need not match.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The possible classes of network addresses have the following forms:

```
Class C:     C nnn.nnn.nnn xxx

Class B:     B nnn.nnn xxx.xxx

Class A:     A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and xxx is a value ranging from 000 to 255, representing the node portion of the address. Note that network and node values of all zeros or all ones are not allowed. These are special values.

The leftmost group of *nnn* has the following ranges for each address class:

`Class C:     192–223`

`Class B:     128–191`

`Class A:     001–126`

The network address (network portion of the IP address) configured in `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP` must match the neighbor gateway IP internet address configured in the current screen.

Default value: None

`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.

You can also designate this gateway as a default gateway by entering an “at” sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP mask entered in the IP Protocol Configuration screen (Figure 11-5) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnetting.

Related screen:

- `NETXPORT.NI.`*`NIname`*`.INTERNET`

  This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask` The IP mask identifies a portion of the IP address for subnets. The subnet is specified in the same format as an IP address; that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the *node* portion would be expressed as 255 255.000.000. The default is no IP mask.

`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, the network transport will choose internally from among the routes with equal hop counts.

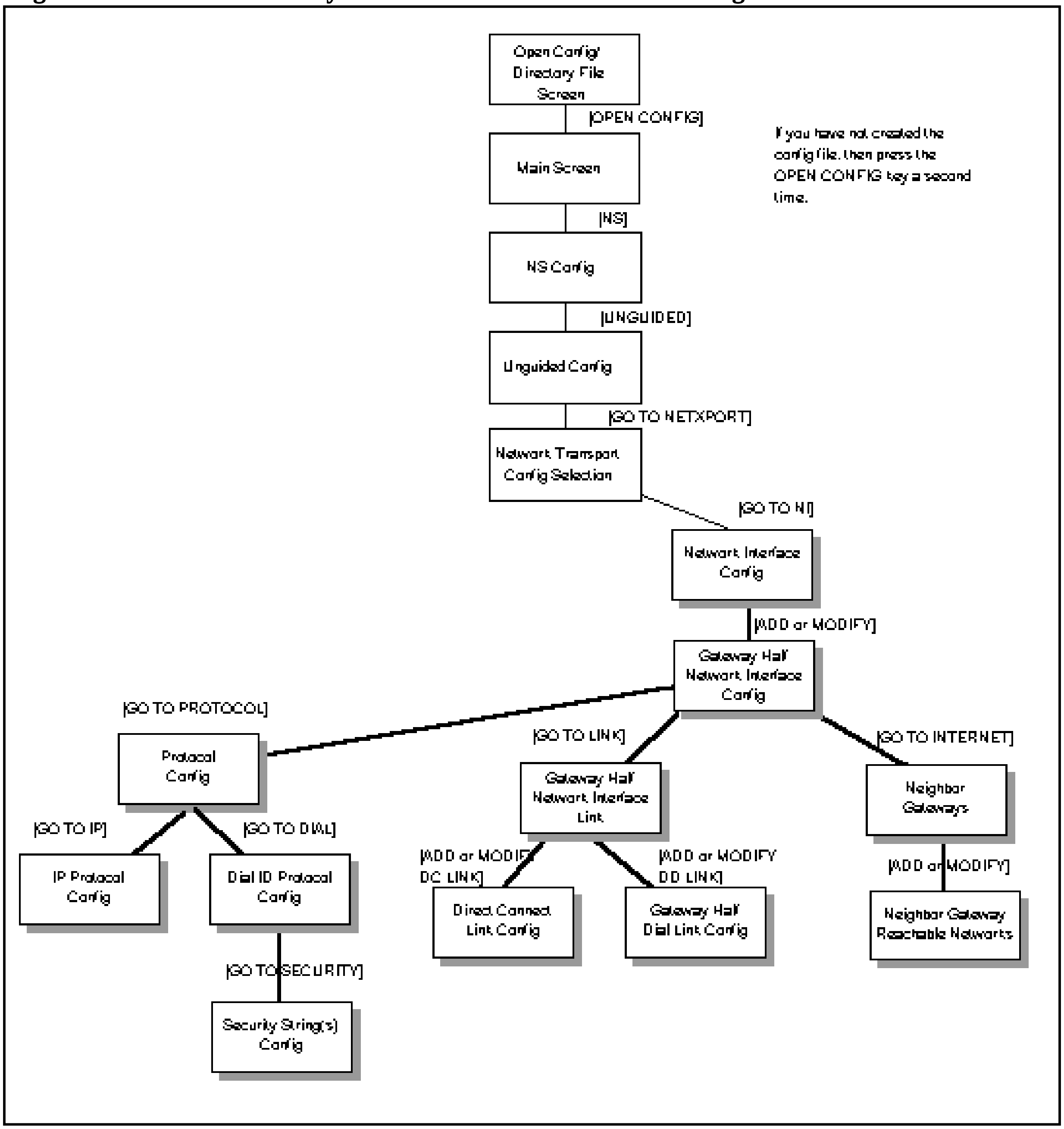
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

12 Gateway Half Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring a Gateway Half network. The Gateway Half Network Interface Configuration branch of NMMGR begins with a screen called the Network Interface Configuration screen. Figure 12-1 shows the screen flow for configuring the Gateway Half screens. Screens unique to Gateway Half are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 12-1 Gateway Half Network Interface Configuration Screen Flow



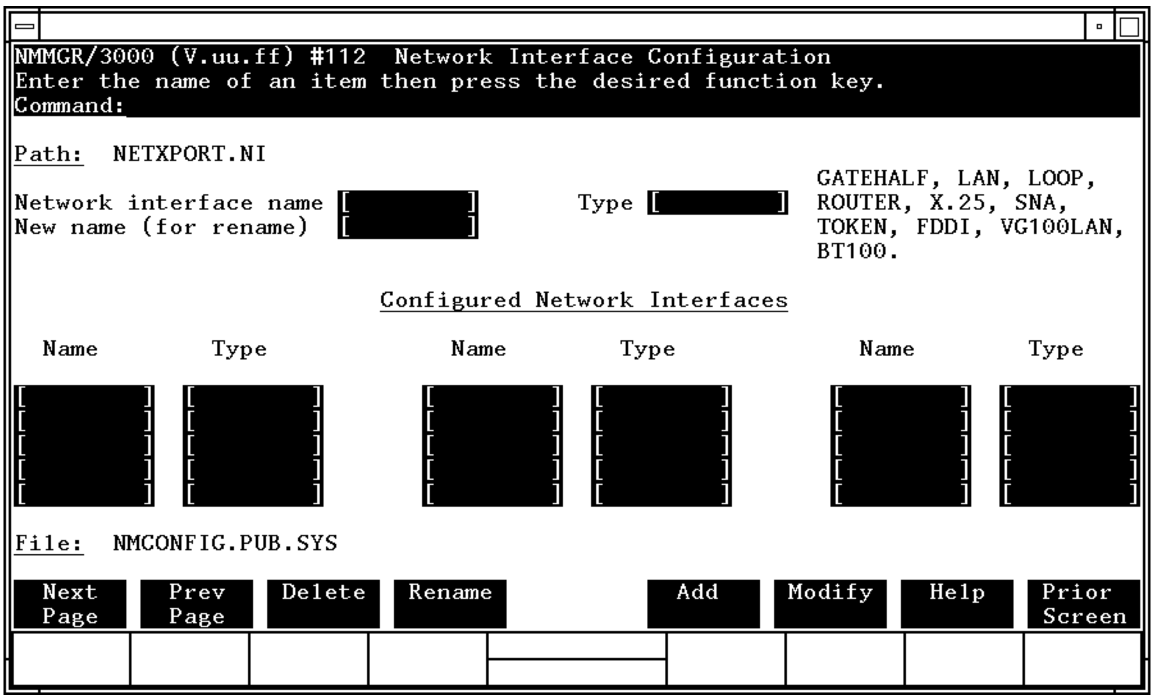
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 12-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration screen (Figure 4-2). It is also displayed when you type the path name:

```
@NETXPORT.NI
```

in the Command window of any screen and press the **[Enter]** key.

Figure 12-2 Network Interface Configuration Screen



Use the fields and function keys of the select screen to perform the desired action.

- To define a new gateway, specify the NI name and the NI type `GATEWAY`; then press the **[Add]** function key. The path for the new NI name is added to the configuration file, and the next screen for configuring a gateway NI is displayed. **Up to 12 NI's are supported per system (one NI must be used for loopback).**
- To modify an existing gateway NI, specify the NI name and press the **[Modify]** function key. The next screen is displayed with the data for that gateway NI.

- To change the name of an existing gateway NI, specify the NI name and a new name and press the **[Rename]** function key. The old 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 gateway NI, specify the NI name and press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The gateway NI (and the associated data) is deleted from the configuration file and is no longer displayed in a display field under the label Configured Network Interfaces.

The network interface provides the interface between network transport protocols and link protocols. It also provides the software loopback capability.

Fields

`Network interface name` Enter the network interface name for the gateway NI. The NI name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, or FDDI,VG100LAN, or BT100)` This field is required if you are adding a network interface. If you are configuring a gateway half, select `GATEHALF`.

`New name` **(Required only when renaming an existing gateway half.)** Enter the current NI name in the network interface name field. Enter a new NI name in the new name field. Press the **[Rename]** function key.

The new name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

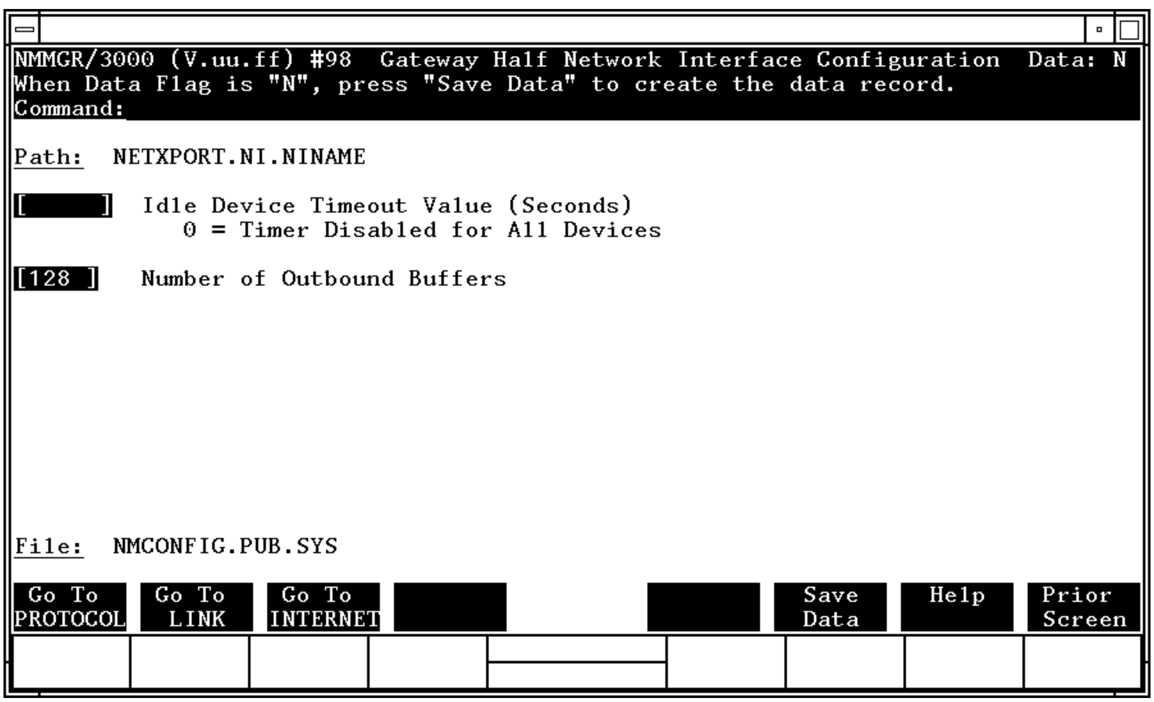
Gateway Half Network Interface Configuration

The gateway half network interface (NI) interfaces the upper layers of the transport protocol to the data link layer. The Gateway Half Network Interface Configuration screen (#98) shown in Figure 12-3 supplies the information required for that interface. The screen is displayed when you select an NI name of type `GATEHALF` at the Network Interface Configuration screen (Figure 12-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the command window of any screen and press the **[Enter]** key, where the *NIname* is a configured gateway half NI.

Figure 12-3 Gateway Half Network Interface Configuration Screen



Press the **[Save Data]** function key 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.

Fields

`Idle device timeout value (seconds)`

If the idle device timer has been enabled (see related screens), and if there is no activity during this time interval, the device is considered to be inactive and will be closed. 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.

Default value: None

Range: 0–32400

`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 they are acknowledged by the destination node. Underallocation may adversely affect TCP throughput.

Related screen:

- `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: 128

Range: 32–1024

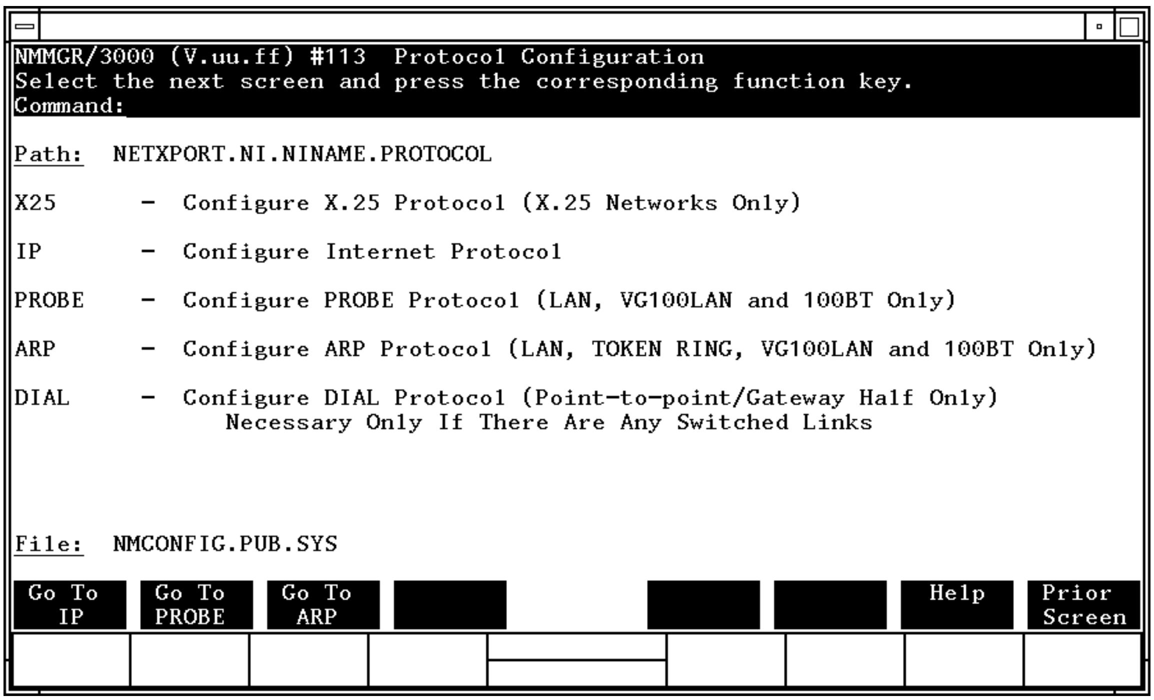
Protocol Configuration

The Protocol Configuration screen (#113) in Figure 12-4 is displayed when you press the **[Go To PROTOCOL]** function key at the Gateway Half Network Interface Configuration screen (Figure 12-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL`

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway half NI.

Figure 12-4 Protocol Configuration Screen



For the gateway half NI, you must configure the IP protocol. The dial protocol must be configured only if you have any switched lines.

Choose the protocol to configure and press the corresponding function key.

Internet Protocol Configuration

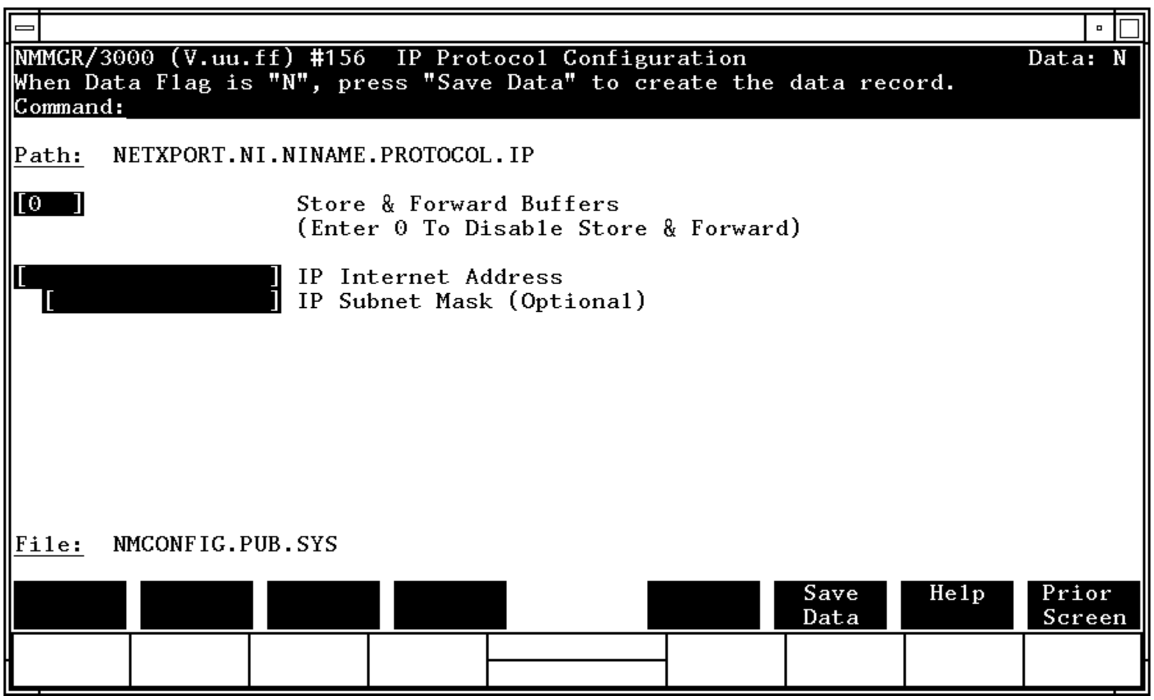
Internet Protocol information must be supplied for each configured NI. The key field in the IP Protocol Configuration screen (#156) shown in Figure 12-5 is the IP internet address, which is used in IP routing and datagram delivery algorithms. The IP subnet mask field allows you to identify an IP subnet mask for the NI named in the path. The store and forward buffers field is useful for internal resource allocation and performance tuning.

The IP Protocol Configuration screen is displayed when you press the **[Go To IP]** function key at the Protocol Configuration screen (Figure 12-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured gateway half NI name.

Figure 12-5 IP Protocol Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Store & forward buffers`

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 you are configuring a non-gateway node on this network. You must allocate store and forward buffers if you are configuring an internet gateway and packets from another network will be forwarded over this network interface. You can modify the number of store-and-forward buffers to allow performance tuning for different network types. However, HP recommends that you use 20 as the store-and-forward buffers. Consult your HP representative before modifying this value.

If store-and-forward is to be disallowed, set this number to 0.

Default value: 0

Range: 0–50

NOTE If this node is a gateway node, HP recommends that you use 20 as the store-and-forward buffers.

`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 home network for which the partner serves as a gateway half.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

`Class C:`	`C nnn.nnn.nnn xxx`
`Class B:`	`B nnn.nnn xxx.xxx`
`Class A:`	`A nnn xxx.xxx.xxx`

where *nnn* is a value ranging from 000 to 255, representing eight bit of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node 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:`	`001–126x`

Default value: None

`IP mask` The IP mask masks a portion of the IP address for subnets. The subnet is specified in the same format as an IP address, that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the *node* portion would be expressed as 255 255.000.000. The default is no IP mask.

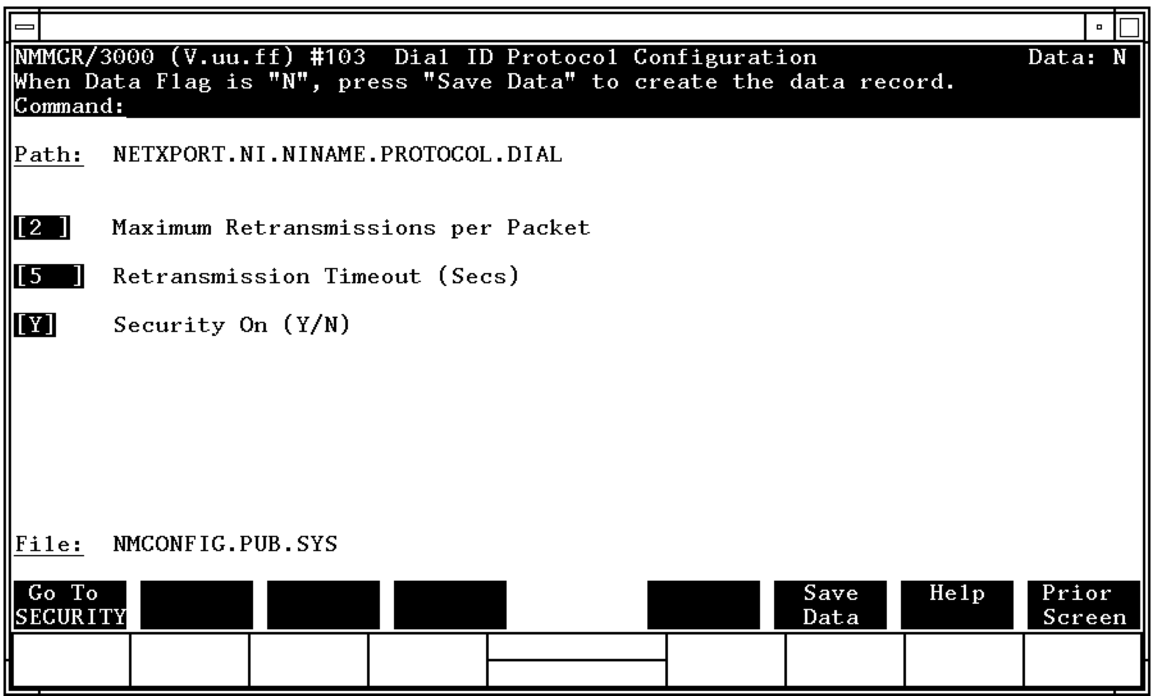
Dial ID Protocol Configuration

Along with other protocol information, the Dial ID Protocol Configuration screen (#103) 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 12-6, is displayed when you press the **[Go To DIAL]** function key at the Protocol Configuration screen (Figure 12-4). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.DIAL`

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway half NI name.

Figure 12-6 Dial ID Protocol Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

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.

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). 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, indicates the path name of the screen in which you can configure security strings.) If security validation fails, an error message is logged. (Refer to the *NS 3000/iX Error Messages Reference 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

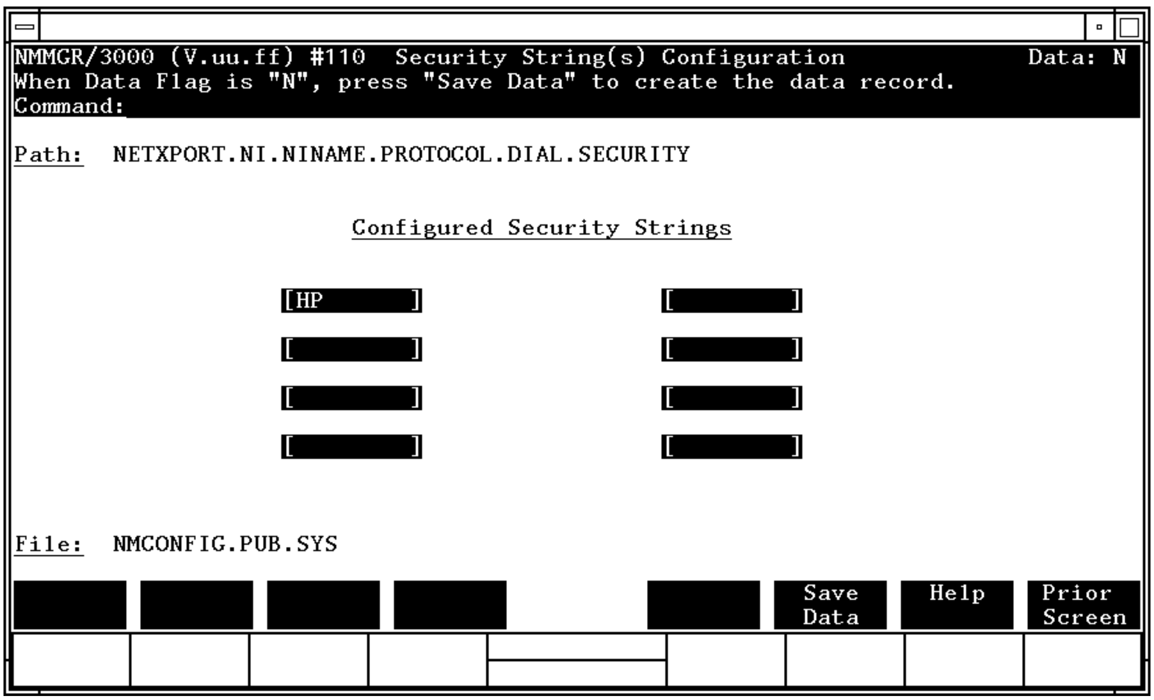
Security String(s) Configuration

The Security String(s) Configuration screen (#110) 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 12-7, is displayed if you press the **[Go to SECURITY]** function key at the preceding Dial ID Protocol Configuration screen (Figure 12-6). It is also displayed when you type:

`@NETXPORT.NI.`*`NIname`*`.PROTOCOL.DIAL.SECURITY`

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway half NI.

Figure 12-7 Security String(s) Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

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.`*`linkname`*

  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 **[Save Data]**.

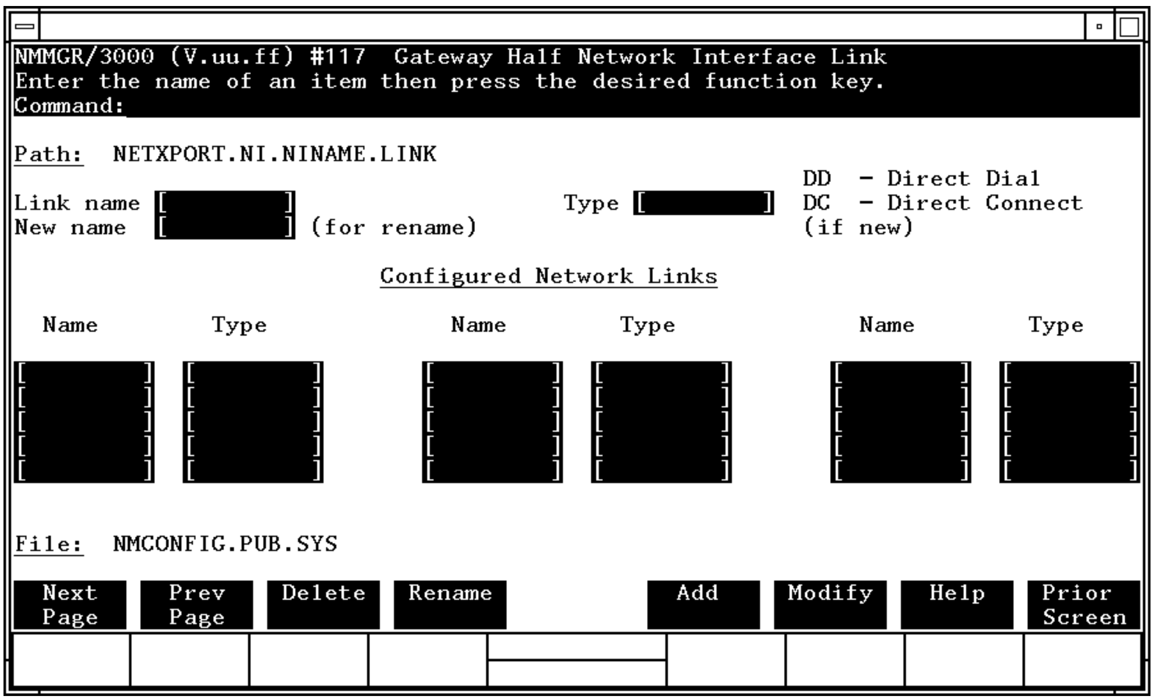
Gateway Half Network Interface Link

The Gateway Half Network Interface Link screen (#117) in Figure 12-8 is displayed when you press the **[Go To LINK]** function key at the Gateway Half Network Interface Configuration screen (Figure 12-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK`

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway half link network interface name.

Figure 12-8 Gateway Half Network Interface Link Screen



Use the fields of this select screen in combination with the function keys to perform the desired action.

- To define a new NI link configuration, specify the link name and link type, then press the **[Add]** function key. The path for the selected link name is added to the configuration file, and the data screen on the path is displayed. **You may configure only one network link per gateway half NI.**
- To modify an existing NI link configuration, specify the link name, then press the **[Modify]** function key. The next screen for the specified link is displayed.

- To change the link name of an existing NI link configuration, specify the link name and a new name, then press the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured name is deleted and is no longer displayed under the label Configured Network Links.

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.

Related Screen:

- `LINK`

  The link name configured in the `NETXPORT.NI.`*`NIname`*`.LINK.`*`linkname`* screen must be the same as a link name of type LAP-B configured in the `LINK` screen.

`Type` Enter `DD` for a direct dial link, or `DC` if the link is direct connect (leased line, private line, or other non-switched link).

`New name` **(Required only when renaming an existing gateway link.)** 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.

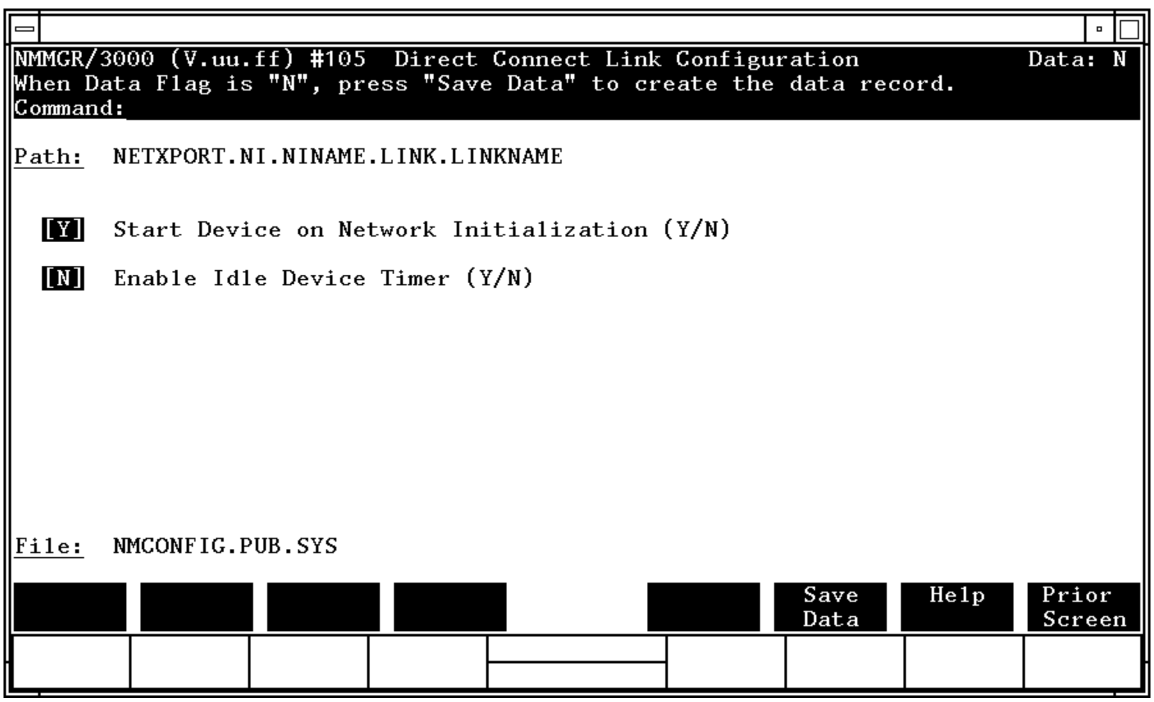
Direct Connect Link Configuration

The Direct Connect Link Configuration screen (#105) 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 12-9, is displayed when you select an NI link name and the link type DC at the Gateway Half Network Interface Link screen (Figure 12-8) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

@NETXPORT.NI.*NIname*.LINK.*linkname*

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway half NI, and *linkname* is the configured gateway half NI link.

Figure 12-9 Direct Connect Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

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 (Y/N)`

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 (see Related screens).

Related screens:

- `NETXPORT.NI.`*`NIname`*

  The idle device timeout value is configured on this screen.

Default value: N

Range: Y or N

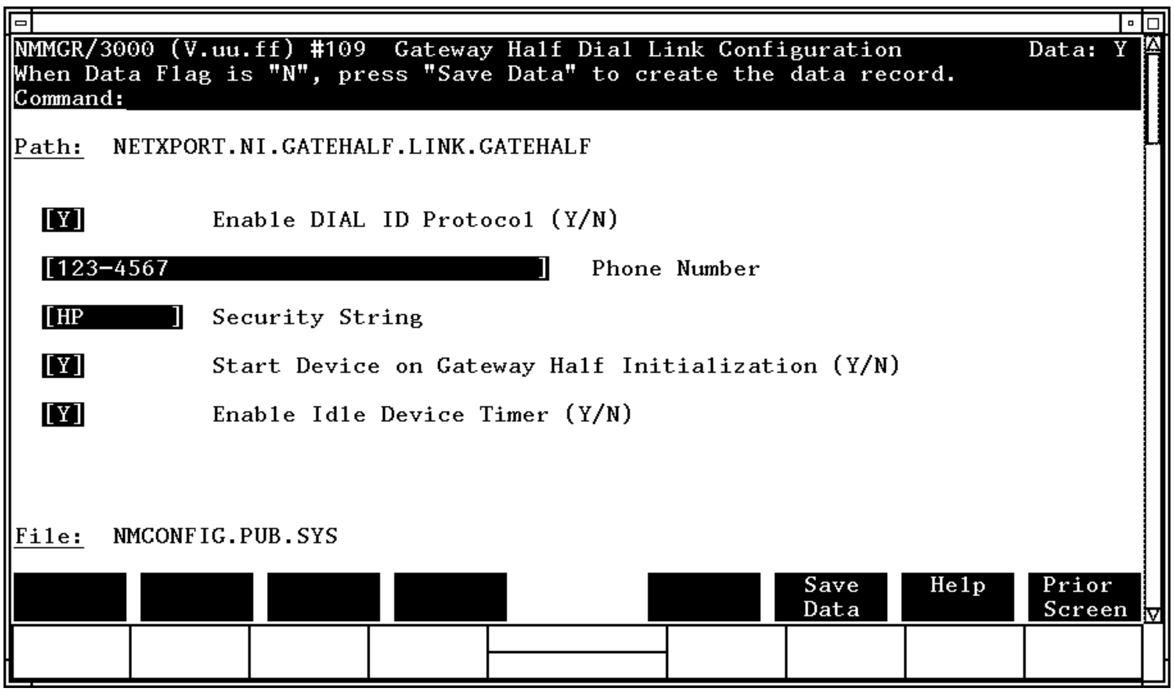
Gateway Half Dial Link Configuration

Dial link configuration provides the information necessary to interface the gateway-half NI to a dial link. The Gateway Half Dial Link Configuration screen (#109), shown in Figure 12-10, is displayed when you select an NI link name and link type DD at the Gateway Half Network Interface Link screen (Figure 12-8) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.LINK.`*`linkname`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway-half NI, and *linkname* is the configured gateway half NI link.

Figure 12-10 Gateway Half Dial Link Configuration Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Enable dial ID protocol (Y/N)`

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 `N`) 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.

- `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 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.`*`NIname`*`.LINK`

  Dial ID protocol is enabled/disabled here

- `NETXPORT.NI.`*`NIname`*`.PROTOCOL.DIAL`

  Security validation is enabled/disabled here.

Default value: HP

`Start device on gateway half 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. 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 (Y/N)`

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).

Related screen:

- `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

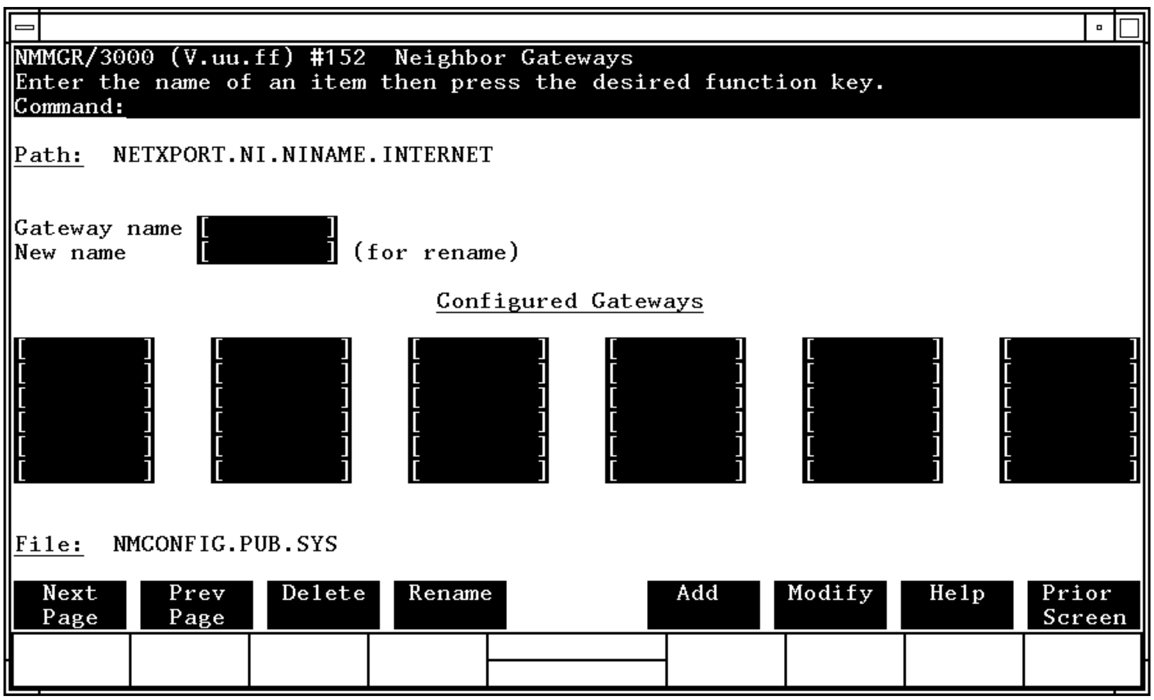
Neighbor Gateways

The Neighbor Gateways screen (#152) in Figure 12-11 is displayed when you press the **[Go To INTERNET]** function key at the Gateway Half Network Interface Configuration screen (Figure 12-3). It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET`

in the command window of any screen and press the **[Enter]** key, where the *NIname* is the configured gateway-half NI name.

Figure 12-11 Neighbor Gateways Screen



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 the **[Add]** function key. The path for the selected gateway name is added to the configuration file, and the data screen on the path is displayed. **You may configure up to 14 gateways under an NI.**
- To modify an existing gateway configuration, specify the gateway name; then press the **[Modify]** function key. 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 the **[Rename]** function key. 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 the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion. The previously configured name is deleted and is no longer displayed in a display field under the label Configured Gateways.

Fields

`Gateway name` Enter a name to represent this node's partner gateway half, through which one or more remote networks can be reached. Using the remote node's node name may help you keep track of gateways.

A gateway name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

`New name` **(Required only when renaming an existing gateway half.)** Enter the name of an existing gateway in the gateway name field and enter a new gateway name in this field. Press the **[Rename]** function key. 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.

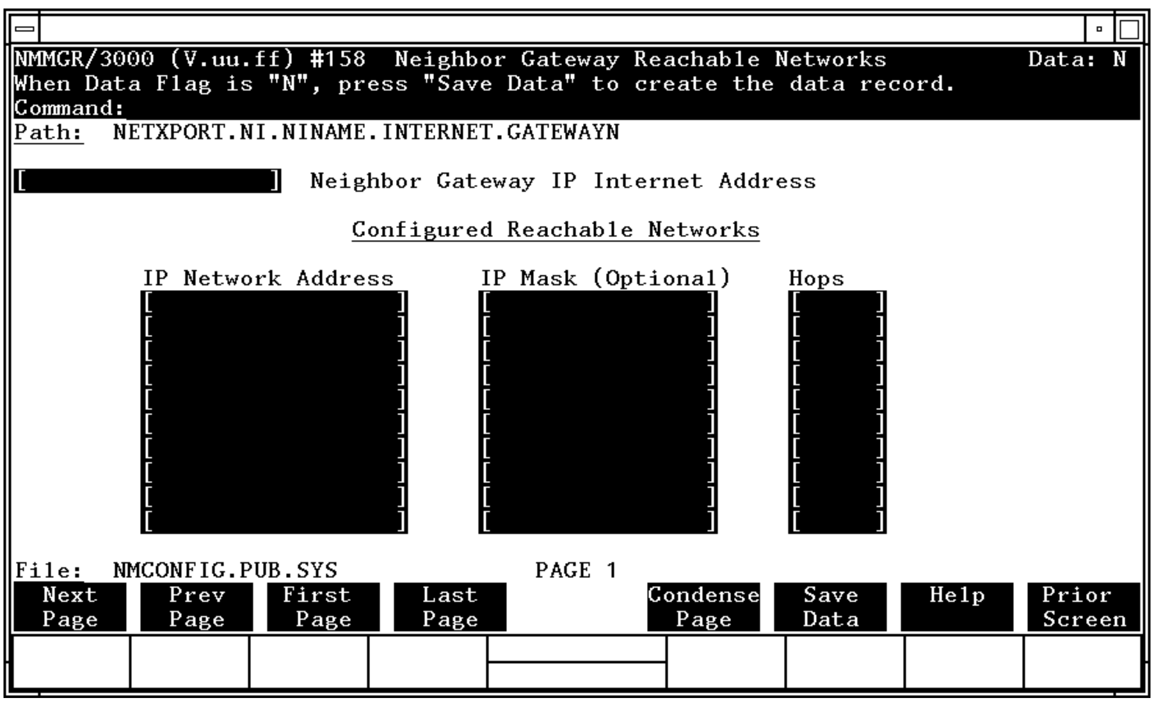
Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) is used to enter internet routing information. It supplies the internet address of a neighbor internet gateway, lists addresses of remote networks which are reachable through that gateway, and gives the distances to those remote networks. For the gateway half NI there is only one neighbor gateway: the partner gateway half. The screen in Figure 12-12 is displayed when you select a gateway name at the Neighbor Gateways screen (Figure 12-11) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*`.INTERNET.`*`gatewayn`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is the configured gateway-half NI, and *gatewayn* is the configured gateway.

Figure 12-12 Neighbor Gateway Reachable Networks Screen



Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

NOTE The information configured in this screen can extend to more than 1 page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). 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 Page]**.

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.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009)

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

   You need not enter the following items as NMMGR will fill these in:

   – Class A, B, C

   – Leading zeros for the network and node portion of the IP address.

Addresses are made up of a **network** portion and a **node** portion. The supported classes of network addresses have the following forms:

```
Class C:    C nnn.nnn.nnn xxx

Class B:    B nnn.nnn xxx.xxx

Class A:    A nnn xxx.xxx.xxx
```

where *nnn* is a value ranging from 000 to 255, representing eight bits of the network portion of an address and *xxx* is a value ranging from 000 to 255, representing the node 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:     001–126`

Default value: None

Related screen:

- `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.

You can also designate this gateway as a default gateway by entering an “at” sign (@) in one of the `Configured reachable networks IP network address` fields. The network will route messages to the default gateway if it is unable to locate their destination by any other means. The default gateway will then attempt to locate the destination.

When specifying reachable networks, entering only the network portions, and optionally the subnet, of the IP address (setting the node portion to all zeros) allows this node to communicate with any other node on the remote network.

If the remote network is subnetted, you can restrict communication of this node to particular subnets by entering the decimal equivalent of those subnets and including the IP mask in the IP mask field.

To allow this node to communicate with other subnets on the local network, enter the decimal equivalent of the subnet in the IP network address field and enter the subnet mask in the IP mask field. If you do not enter a subnet mask one of the following occurs:

- If the IP address is the same as the node you are configuring, the IP Mask configured in the IP Protocol Configuration screen (Figure 6-4) is used.
- If the IP address is different from the node you are configuring, NMMGR assumes no subnets.

Related screen:

- `NETXPORT.NI.`*`NIname`*`.INTERNET`

  This path name corresponds to the Neighbor Gateways screen. A Neighbor Gateway Reachable Networks screen must be configured for each gateway configured in the Neighbor Gateways screen.

`IP mask` The IP mask masks a portion of the IP address for subnets. The subnet is specified in the same format as an IP address, that is, the 32-bit mask is grouped in octets expressed as decimal integers and delimited by a "." or a space. For example, a mask for a class A address with the subnet field being the first 8 bits of the **node** portion would be expressed as 255 255.000.000. The default is no IP mask.

`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

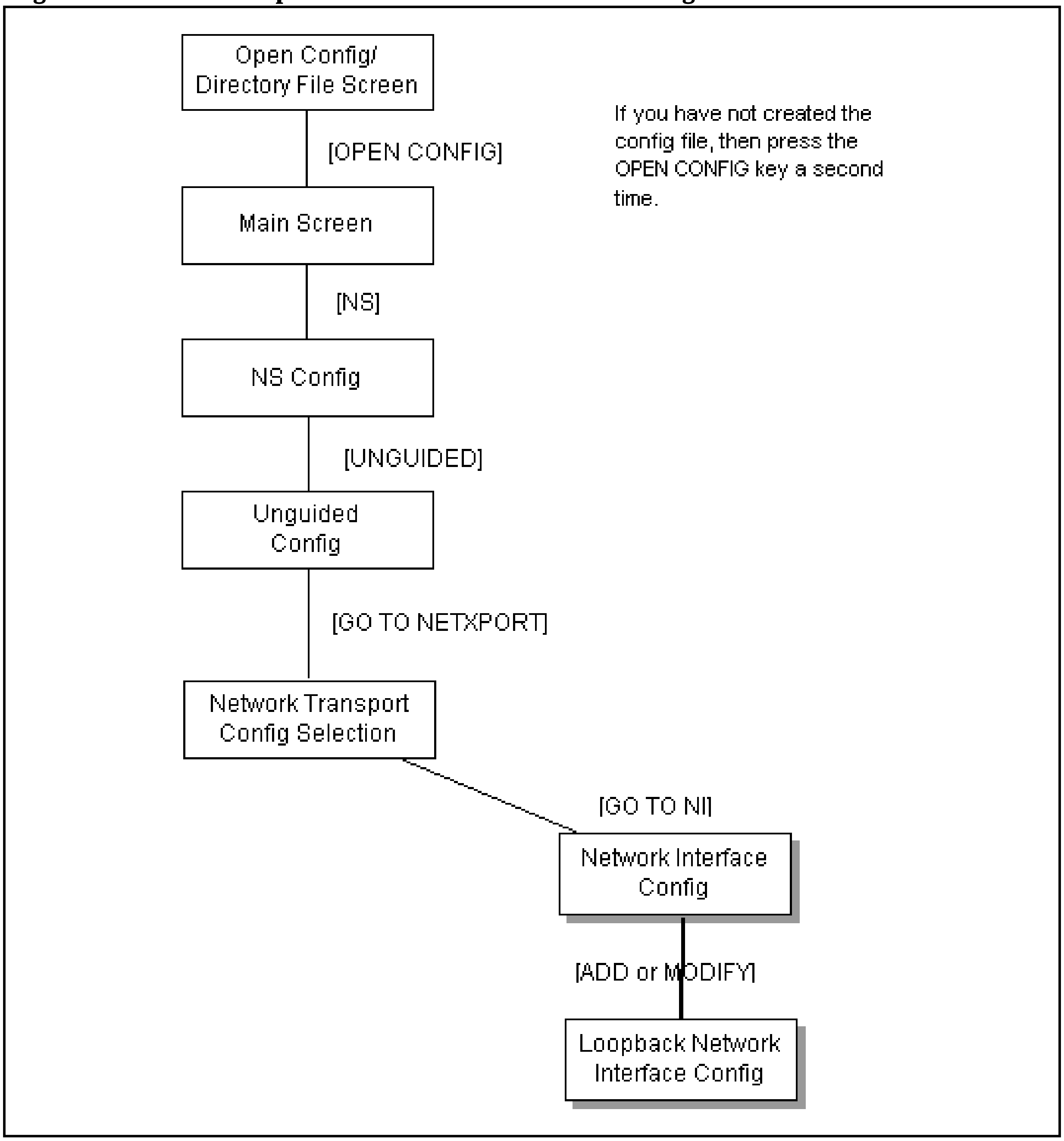
Range: 1–32767

NOTE To delete a reachable network entry, fill the field to be deleted with blanks and press the **[Save Data]** function key.

13 Loopback Network Interface Configuration Screens

The screens in this chapter are those you would see when configuring a Loopback network. The Loopback Network Interface Configuration branch of NMMGR begins with a screen called the Loopback Network Interface Configuration screen. Figure 13-1 shows the screen flow for configuring the Loopback screens. Screens unique to Loopback are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 13-1 Loopback Network Interface Configuration Screen Flow



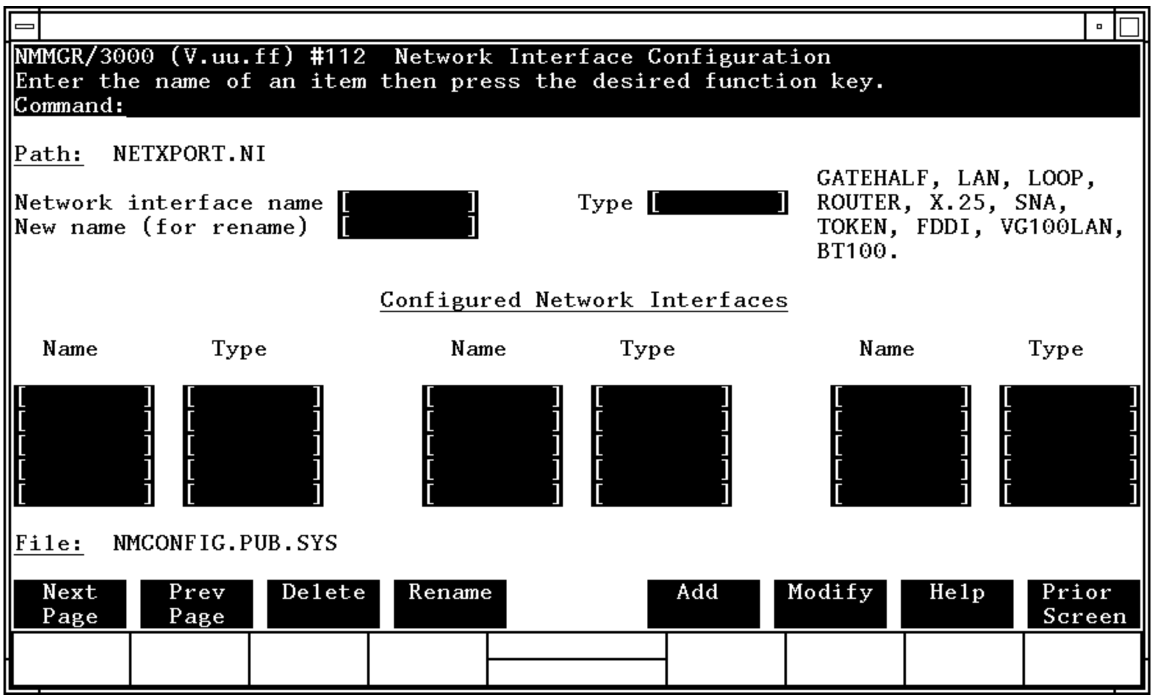
Network Interface Configuration

The Network Interface Configuration screen (#112) in Figure 13-2 is displayed when you press the **[Go To NI]** function key at the Network Transport Configuration screen (Figure 4-2). It is also displayed when you type the path name:

`@NETXPORT.NI`

in the Command window and press the **[Enter]** key.

Figure 13-2 Network Interface Configuration



To configure a loopback interface, enter a network interface name of type LOOP and press the **[Add]** function key. (Note that loopback is configured automatically when you use guided configuration.) **You may configure up to 12 NI's per system (one NI must be used for loopback.)**

Fields

`Network interface name` **(Required.)** This is the name of the network interface you want to configure or modify. The name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

`Type (GATEHALF, LAN, LOOP, ROUTER, X.25, SNA, TOKEN, FDDI, VG100LAN, or BT100)` This field is required if you are adding a network interface. If you are configuring a loopback NI, select `LOOP`.

`New name` **(Required only when you are renaming an existing network interface.)** Type the current name in the network interface name field. Type the new name in the new name field. Press the **[Rename]** function key.

The name can contain as many as eight alphanumeric characters. The first character must be alphabetic.

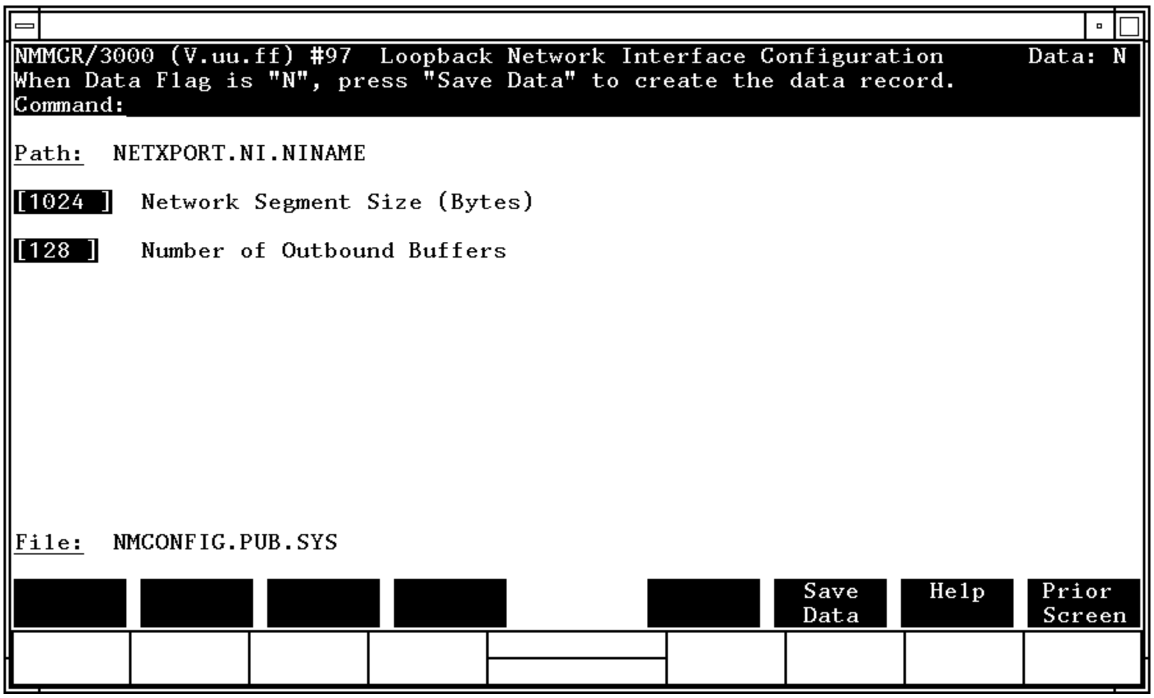
Loopback Network Interface Configuration

The Loopback Network Interface Configuration screen (#97) in Figure 13-3 is displayed when you select an NI name and the NI type LOOP at the Network Interface Configuration screen (Figure 13-2) and press the **[Add]** or **[Modify]** function key. It is also displayed when you type the path name:

`@NETXPORT.NI.`*`NIname`*

in the command window of any screen and press the **[Enter]** key, where *NIname* is a configured loopback NI.

Figure 13-3 Loopback Network Interface Configuration Screen



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.

Press the **[Save Data]** function key to transfer the data displayed on the screen to the configuration file you are creating or updating. Verify that the data record has been created by checking that the Data flag is set to Y.

Fields

`Network segment size (bytes)`

(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: 1024–4032

`Number of outbound buffers`

This field specifies the number of outbound buffers to be allocated for loopback. The default 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 loopback NI. Therefore, the default is 128. If you change the number of TCP connections from the default value, you should reconsider the number of inbound buffers for all NIs.

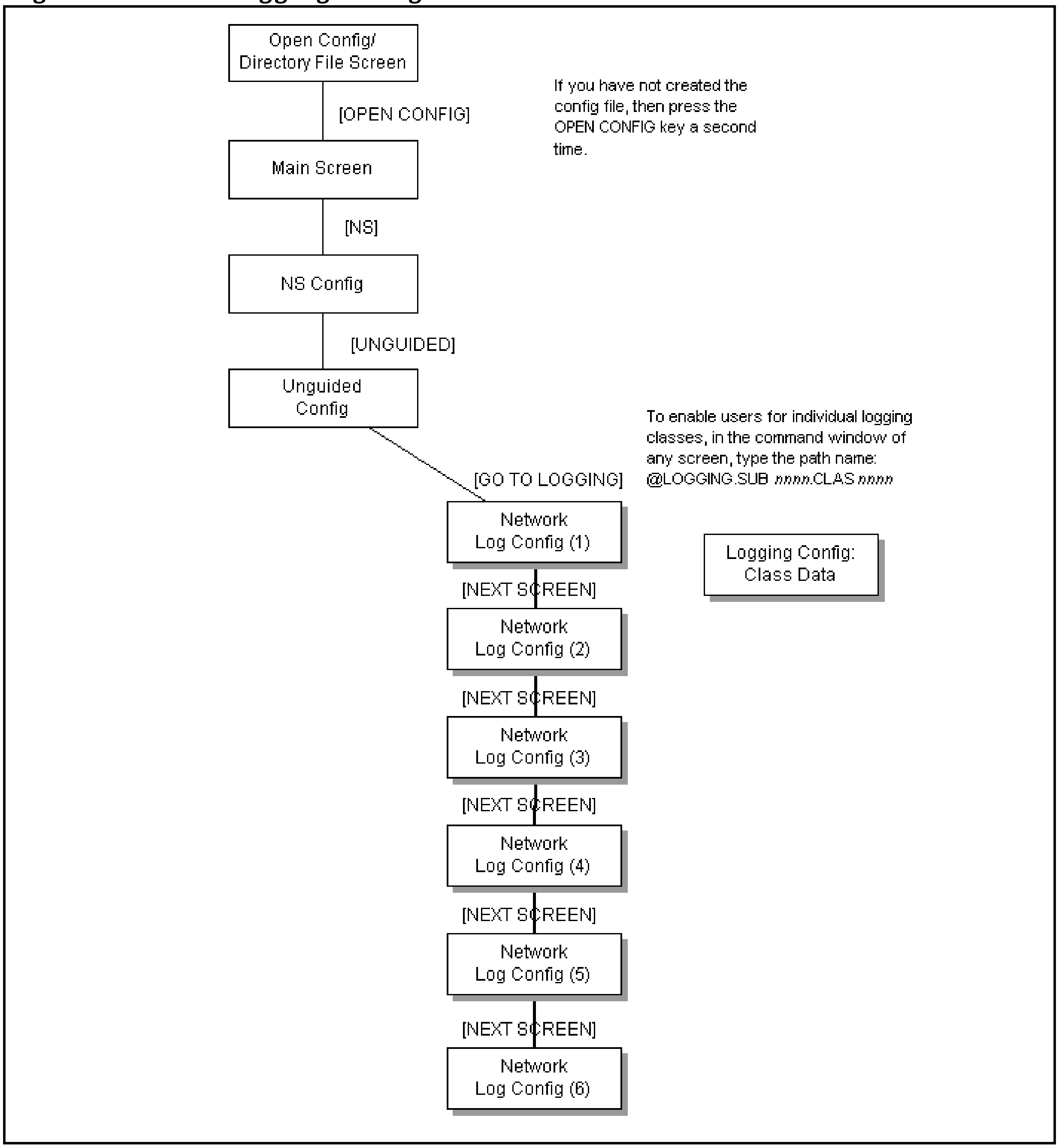
Default value: 128

Range: 128–1024

14 Logging Configuration Screens

The screens in this chapter are those you would see when configuring logging. The Logging Configuration branch of NMMGR begins with a screen called the Netxport Log Configuration screen. Figure 14-1 shows the screen flow for configuring the logging screens. Screens unique to logging are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 14-1 Logging Configuration Screen Flow



Logging is configured for the purpose of recording events such as errors and console commands. You configure logging for each of the network subsystems and links. Each subsystem includes different **classes** of events (such as internal errors).

You can record logging to a disk file for later analysis, to the system console so that the system operator receives the messages, or both. You can also display logging events at individual users' list devices. This may be valuable to allow the network manager to monitor NS console activity from an alternate terminal. 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*. (Take care if you enable users for logging; doing so can place a strain on system resources.)

The guided configuration process, described in the *HP 3000/iX Network Planning and Configuration Guide*, configures logging for you using defaults. You can also configure or modify the logging subsystem using either guided or unguided configuration.

Perform the following steps to reach the logging configuration screens for manual configuration:

Step 1. **Run NMMGR.** The Open Configuration/Directry File screen is displayed

Step 2. Enter the configuration file name (NMCONFIG.PUB.SYS) and password, if a password is needed, and press the **[Open Config]** function key. The Main screen is displayed.

Step 3. Press the **[NS]** function key. The NS Configuration screen is displayed.

Step 4. Press the **[Unguided Config]** function key to display the Unguided Configuration screen.

Step 5. Press the **[Go To Logging]** function key. The first of six logging configuration screens is displayed.

NOTE HP recommends that you use the default logging configuration values unless your HP representative tells you otherwise. Not using the recommended default values may result in the degration of system performance.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual*.

Activating Logging

NetIPC logging is automatically activated at system startup. Network Services logging is activated when the Network Services are initiated (i.e., when the **NSCONTROL START** command is issued). Link manager logging and network transport logging are activated when you initiate the network transport (**NETCONTROL START**).

When you are changing a logging configuration for a specific subsystem, the changes will normally take effect when you perform a **SWITCHNMLOG UPDATE** command. In some cases, however, such as when no logging is currently active, the subsystem may need to be deactivated and restarted. The steps that must be taken for each subsystem are shown in Table 14-1.

Table 14-1 Subsystem Activation/Deactivation

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 already active) **SNACONTROL STOP;NODE=nodename** (repeat until all SNA nodes are stopped; refer to the *SNA Link/iX Node Manager's Guide*) **SNACONTROL START;NODE=nodename** **NETCONTROL START**

How to use the log messages for troubleshooting is described in the *NS 3000/iX Error Messages Reference Manual*. How to format the log file for examination is described in *Using the Node Management Services (NMS) Utilities*.

NETXPORT Log Configuration

The Netxport Log Configuration (1) screen (#61) in Figure 14-2 is displayed when you press the function key for **[Go To Logging]** at the Unguided Configuration screen (#80) shown in Figure 2-6.

Figure 14-2 Netxport Log Configuration (1) Screen

```
NMMGR/3000 (V.uu.ff) #61  Netxport Log Configuration (1)              Data: Y
Fill in the required information; then press the Save Data key.
Command:

           Class     Console Disk
Subsystem  Name      Logging Logging  Event

SUB0000    CLAS0000   [Y]     [Y]     Informative messages


SUB0003    CLAS0001   [Y]     [Y]     Serious internal error
Network    CLAS0002   [Y]     [Y]     Internal error/operator attention
Transport  CLAS0003   [N]     [Y]     Non-critical errors
           CLAS0004   [Y]     [Y]     Nodal messages (start/stop)
           CLAS0005   [N]     [N]     Informative messages
           CLAS0006   [N]     [Y]     Statistical information

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.

To see more logging class options, press the Next Screen key.


File:  NMCONFIG.PUB.SYS
  Next  |        |        |  Exit  |            |Validate| Save  | Help  | Prior
 Screen |        |        |Logging |            |Netxport| Data  |       | Screen
```

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on the first screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual*.

Fields

`Console logging`
: The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk logging`
: The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *nnnn* is a number from 0000 to 9999. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.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`.

The Netxport Log Configuration (2) screen (#60) in Figure 14-3 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (1) screen.

Figure 14-3 Netxport Log Configuration (2) Screen

```
NMMGR/3000 (V.uu.ff) #60  Netxport Log Configuration (2)          Data: Y
Fill in the required information; then press the Save Data key.
Command:

               Class     Console Disk
Subsystem      Name      Logging Logging    Event

SUB0004        CLAS0000   [Y]     [Y]       Notable events
DC/LDM

SUB0005        CLAS0000   [Y]     [Y]       Internal errors
Network        CLAS0001   [N]     [Y]       Resource errors
IPC            CLAS0002   [N]     [N]       Informative messages

SUB0006        CLAS0002   [N]     [Y]       Resource errors
Network        CLAS0003   [N]     [Y]       Internal errors
Services       CLAS0004   [N]     [Y]       Detailed events (enable with NSCONTROL LOG)
               CLAS0005   [N]     [Y]       NetIPC internal errors

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and presss ENTER.

To see more logging class options, press the Next Screen key.
File:  NMCONFIG.PUB.SYS
  Next  |      |      | Exit  |          |Validate| Save  | Help  | Prior
 Screen |      |      |Logging|          |Netxport| Data  |       | Screen
```

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual*.

Fields

`Console logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *nnnn* is a number from 0000 to 9999. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.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`.

The Netxport Log Configuration (3) screen (#70) in Figure 14-4 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (2) screen.

Figure 14-4 Netxport Log Configuration (3) Screen

```
NMMGR/3000 (V.uu.ff) #70  Netxport Log Configuration (3)           Data: Y
Fill in the required information; then press the Save Data key.
Command:

             Class     Console Disk
Subsystem    Name      Logging Logging   Event

SUB0008      CLAS0000   [N]     [Y]      Internal errors
Link Mgr

SUB0018      CLAS0000   [N]     [N]      Errors
Trace Mgr

SUB0024      CLAS0001   [N]     [N]      Informational messages
NMMGR


To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.

To see more logging class options, press the Next Screen key.

File:  NMCONFIG.PUB.SYS

  Next   |        |        |  Exit   |               |Validate| Save   | Help   | Prior
 Screen  |        |        |Logging  |               |Netxport| Data   |        | Screen
```

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual*.

Fields

`Console Logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file.

The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *nnnn* is a number from 0000 to 9999. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.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`.

The Netxport Log Configuration (4) screen (#68) in Figure 14-5 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (3) screen.

Figure 14-5 Netxport Log Configuration (4) Screen

```
NMMGR/3000 (V.uu.ff) #68  Netxport Log Configuration (4)          Data: Y
Fill in the required information; then press the Save Data key.
Command:

           Class     Console Disk
Subsystem  Name      Logging Logging   Event

SUB0025    CLAS0001   [N]     [Y]      Errors
LAN driver CLAS0002   [N]     [Y]      Warnings
           CLAS0003   [N]     [Y]      Informational messages

SUB0028    CLAS0010   [N]     [Y]      Errors
Lap B Link CLAS0012   [N]     [Y]      Informational messages

SUB0040    CLAS0001   [N]     [Y]      Catastrophic errors
Remote     CLAS0002   [N]     [Y]      Serious errors
Link Mgr   CLAS0003   [N]     [Y]      Notable errors
           CLAS0004   [N]     [Y]      Nodal messages (start/stop)
           CLAS0005   [N]     [Y]      Informative messages

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.
To see more logging class options, press the Next Screen key.
File:  NMCONFIG.PUB.SYS
  Next  |        |        |  Exit   |            |Validate| Save  | Help  | Prior
 Screen |        |        |Logging  |            |Netxport| Data  |       | Screen
```

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Press the **[Exit Logging]** function key when you have finished modifying the logging configuration.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual*.

Fields

`Console logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *nnnn* is a number from 0000 to 9999. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.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`.

The Netxport Log Configuration (5) screen (#69) in Figure 14-6 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (4) screen.

Figure 14-6 Netxport Log Configuration (5) Screen

```
NMMGR/3000 (V.uu.ff) #69  Netxport Log Configuration (5)          Data: Y
Fill in the required information; then press the Save Data key.
Command:

             Class     Console Disk
Subsystem    Name      Logging Logging   Event

SUB0057      CLAS0001   [Y]     [Y]      Fatal errors
SNMP         CLAS0002   [N]     [Y]      Serious errors
             CLAS0003   [N]     [N]      Warnings
             CLAS0004   [N]     [N]      Informational messages

SUB0061      CLAS0001   [N]     [Y]      Errors
Token Ring   CLAS0002   [N]     [Y]      Warnings
Link         CLAS0003   [N]     [Y]      Informational messages

SUB0067      CLAS0001   [N]     [Y]      Errors
FDDI Lan

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.


File:  NMCONFIG.PUB.SYS
  Next   |         |         |  Exit   |               |Validate|  Save  |  Help  |  Prior
 Screen  |         |         |Logging  |               |Netxport|  Data  |        | Screen
```

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Press the **[Exit Logging]** function key when you have finished modifying the logging configuration.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual*.

Fields

`Console logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *nnnn* is a number from 0000 to 9999. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.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`.

The Netxport Log Configuration (6) screen (#316) in Figure 14-7 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (5) screen.

Figure 14-7 Netxport Log Configuration (6) Screen

```
NMMGR/3000 (V.uu.ff) #316 Netxport Log Configuration (6)            Data: Y
Fill in the required information; then press the Save Data key.
Command:

           Class     Console Disk
Subsystem  Name      Logging Logging  Event

SUB0074    CLAS0001  [Y]     [Y]      Errors
100VG802.3 CLAS0002  [N]     [Y]      Warnings
driver     CLAS0003  [N]     [Y]      Informational messages

SUB0077    CLAS0001  [Y]     [Y]      Errors
100BaseT   CLAS0002  [N]     [Y]      Warnings
driver     CLAS0003  [N]     [Y]      Informational messages




To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.
To see more logging class options, press the Next Screen key.
File:  NMCONFIG.PUB.SYS
  Next                        Exit                 Validate  Save     Help     Prior
 Screen                      Logging               Netxport  Data              Screen
```

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Press the **[Exit Logging]** function key when you have finished modifying the logging configuration.

For more information on logging classes and subsystems see the *NS 3000/iX Operations and Maintenance Reference Manual.*

Fields

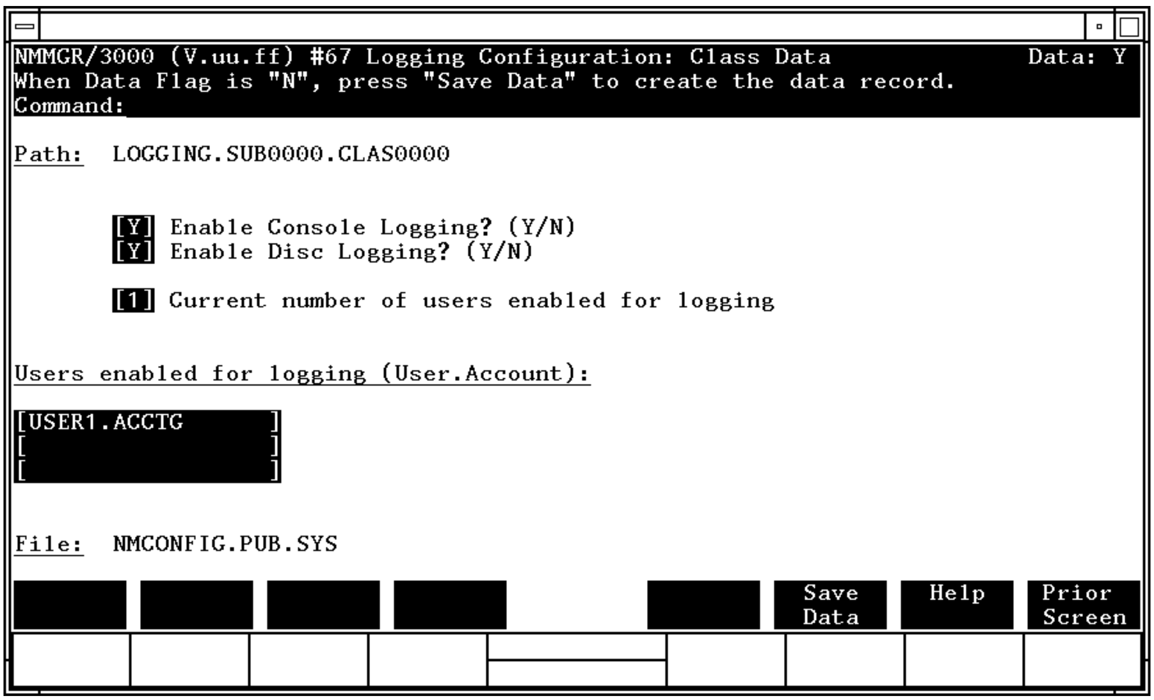
`Console logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *nnnn* is a number from 0000 to 9999. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.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`.

Enabling Users for Individual Logging Classes

The logging screens described in this chapter make it possible to completely configure logging for all subsystems by traversing only six screens. However, using these screens, it is not possible to configure logging so that messages generated by specific logging classes are sent to an individual user's list device. The Logging Configuration: Class Data screen (#67) is shown in Figure 14-8.

Figure 14-8 Logging Configuration: Class Data Screen



The following steps describe the method used to configuring users to receive logging messages. Using this method, you can create a configuration that allows messages from a single logging class, or a set of classes, to be sent to a user's list device.

To do so, you access and update the Logging Configuration Class Data screen according to the following steps:

Step 1. Type the path name:

`@LOGGING.SUB`*nnnn*`.CLAS`*nnnn*

in the command window of any screen and press the **[Enter]** key, where `SUB`*nnnn* is the subsystem ID and `CLAS`*nnnn* is the class name of the logging class you want directed to the user's list device. The Logging Configuration: Class Data screen shown in Figure 14-8 is displayed.

Step 2. To enable console logging for this subsystem logging class, enter a Y in the enable console logging field. To disable console logging, enter an N. **Be aware that changing the value in this field will override the previous setting for the logging class you are configuring.**

Step 3. To enable disk logging for this subsystem logging class, enter a Y in the enable disk logging field. To disable console logging, enter an N. **Be aware that changing the value in this field will override the previous setting for the logging class you are configuring.**

Step 4. Enter up to three names, in the form user.account, in the users enabled for logging fields. If these fields already contain names it is because user names were previously configured using this screen. If less than three user names are configured, type the new user name in an empty field. If all fields are used, type over one of the old user names to replace it with the new user name. (Note that the user name you type over will no longer be enabled to receive these logging messages.)

Step 5. Press the **[Save Data]** function key to modify the data record.

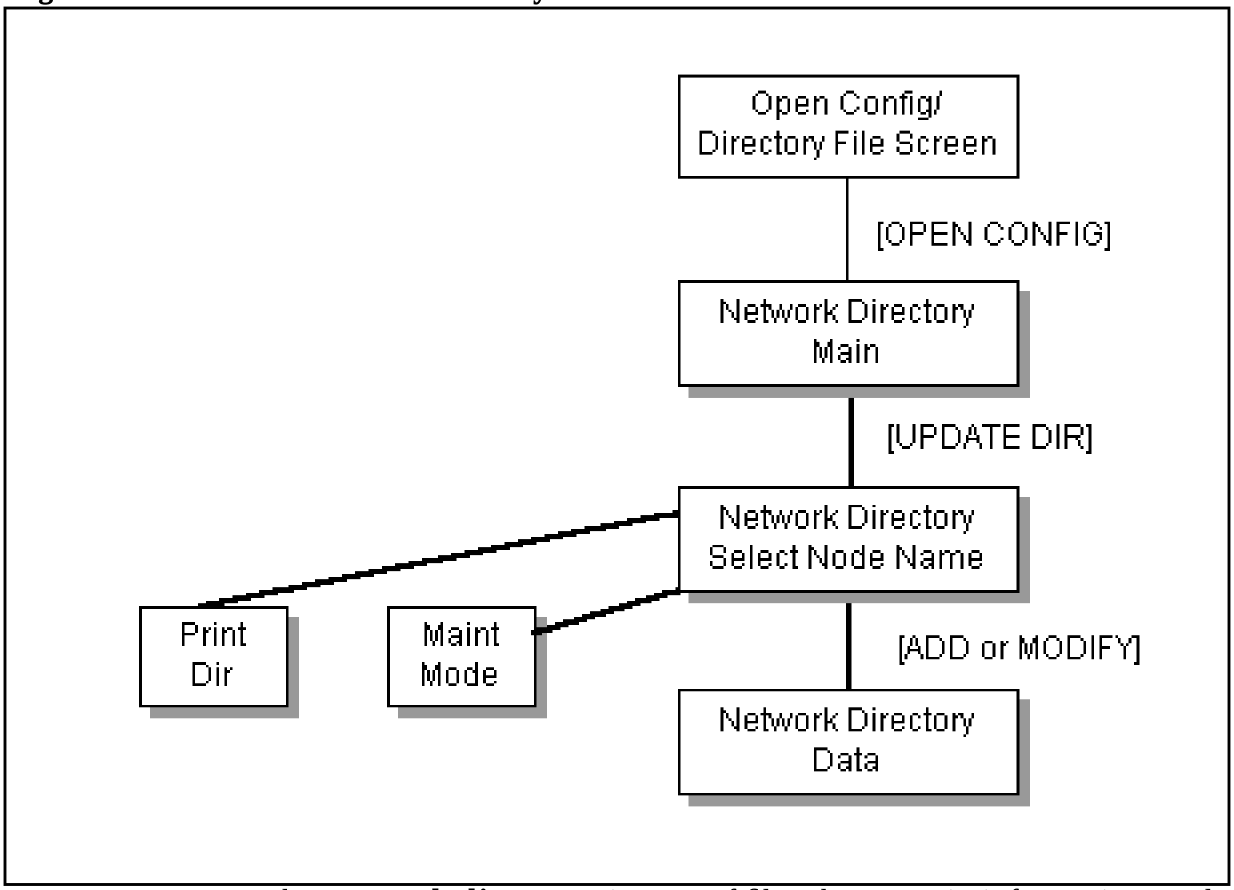
Step 6. Press the **[Prior Screen]** key to return to the screen from which you accessed the Logging Configuration: Class Data screen. Repeat the above procedure for each subsystem logging class for which you want to enable users.

CAUTION Enabling users to receive logging messages can strain system resources. Hewlett-Packard recommends that you use this capability sparingly and only for short periods of time.

15 Network Directory

The screens in this chapter are those you would see when configuring the Network Directory. The Network Directory branch of NMMGR begins with a screen called the Network Directory Main screen. Figure 15-1 shows the screen flow for configuring the Directory screens. Screens unique to the Network Directory are indicated by bold boxed screens. [FUNCTION] denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 15-1 Network Directory Main Screen Flow



The **network directory** is a set of files that contain information used by the node to communicate with other nodes in the internetwork. (An **internetwork** or **internet** is a collection of networks.)

The network directory is managed through two interfaces: NMMGR screens, and a command-driven interface called **maintenance mode**, to collect and merge directory information from remote nodes into the directory on the local node. This chapter describes the screen interface along with a general discussion of the functions of the network directory. The command-driven interface (maintenance mode) is described in detail in *Using the Node Management Services (NMS) Utilities*.

You use NMMGR to perform the following network directory functions:

- Add, modify, and delete entries in the directory.
- Review and inspect directory information.
- Merge a remote directory with a directory on the local node.
- 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 chapter.

What a Network Directory Provides

A network directory is used by the node for internetwork routing. Each entry in a network directory consists of a node name associated with an IP address, the network type, and an additional address, if necessary. The network directory uses the internet protocol (IP) address to transfer data between networks.

When a Network Directory is Required

A network directory must be configured on nodes with X.25 links. Point-to-Point nodes that do not use domain name services require network directory configuration. You must also configure a network directory when non-HP nodes are part of an HP LAN or token ring and you are not using domain name services. At least one node on LAN and token ring networks must have a network directory if any of the nodes on that network are to communicate with the internet and you are not using domain name services.

The network directory of a node in a point-to-point network must contain the IP address of all other nodes that you want the node to be able to reach. When configuring the network directory for a point-to-point network, make sure that the IP address you enter in the network directory matches the data in the mapping screens (path name `NETXPORT.NI.`*`NIname`*`.MAPPING.`*`mapentry`*).

For nodes on an X.25 network, the network directory maps the X.25 address key to an IP address to allow a node to communicate within the X.25 network. You must configure a network directory for nodes using X.25.

Probe and Proxy Servers

Because HP 3000s on an IEEE 802.3/Ethernet LAN use a proprietary HP protocol called **probe**, they are able to communicate on a LAN without a network directory. A node on an HP LAN can determine connection information about a node on the same LAN by sending a multicast probe request out on the LAN. The target node recognizes its address in the probe request and sends an individually addressed probe reply with the necessary connection information to the requesting node. The probe request/reply mechanism is sufficient to obtain connection requirements in an HP LAN environment.

However, at least one node on an HP LAN must have a network directory if the nodes on that LAN are to communicate with other networks and you are not using domain name services. The node with the network directory on a LAN is called a **proxy server**. By using the probe protocol, a LAN node without a network directory can multicast a request for an internet address from the proxy server. For backup purposes, you should designate at least two nodes on a LAN to be proxy servers.

A node is configured as a proxy server in the Probe Protocol Configuration screen, (path name `NETXPORT.NI.`*`NIname`*`.PROTOCOL.PROBE`).

Path Report Lists

A path report is an internal structure containing all configured paths to a given IP address in the internet. The **path report** list is a list of all path reports in a network directory. Each path report contains the protocol stacks that the data must pass through to get to a given IP address. An example of a path report where the protocol stack contains TCP with checksum error checking (level 4) over IP (level 3i) over IEEE 802.3 (level 2), is indicated in the following format:

```
TCP.IP.IEEE802.3
```

In the network directory, IP addresses must be unique so that a single path report can be identified.

Planning the Network Directory

There are two schools of thought on how network directories should be planned and configured on a network, as follows:

- Centralized network directories.
- Decentralized network directories.

The centralized school of thought requires each node on the internet to have the same network directory. This means that every node in the network must have an entry in the network directory. The advantage to this is that you update the network directory in one place, then copy it to the rest of the world. The disadvantage is that network directories for large internets are going to be large.

The recommended way to create and maintain your network directory using the centralized method is to assign a single node as the **central administrative node**. You configure the network directory on this node and then copy it to all other nodes on the network. When the network directory is updated, it is updated on the central administrative node, then copied to the other nodes. This procedure decreases the possibility of incompatible directories. You may want to assign a central administrative node for each network or for the entire internet.

The decentralized school of thought suggests that each network directory be configured individually on each node. The advantage to this is that you can customize the network directory on each node for security purposes using local and global entries. The network directory will also be smaller because it will only contain entries for that particular node. However, updates must be done manually on each node.

Copying and Merging Network Directory Files

The first time you configure the network directory, an entry for all remote IP addresses must be added manually using the NMMGR screens. After the first network directory is configured, you can use the MPE **STORE** and **RESTORE** commands to copy the network directory to other nodes. (This is assuming you have adopted the centralized method of network directory maintenance. If you use the decentralized method, you must always use NMMGR to create and maintain the network directory.)

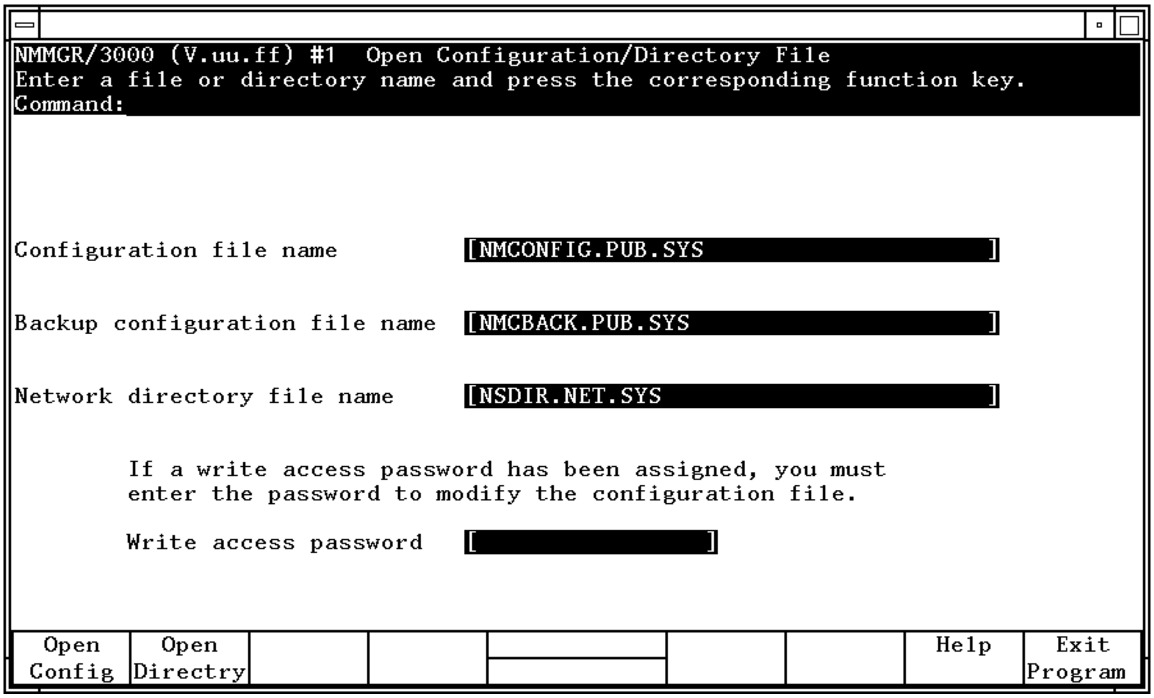
NOTE The network directory uses a KSAM file pair. Therefore, when copying a directory, be sure to copy both the data file and the key file.

Once a network directory has been established on each node in the internet, you can set up a job stream to automate network directory updates. The **MERGEDIR** command is part of a maintenance interface provided primarily to support the updating of directories using 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. Refer to the **MERGEDIR** and the **MAKESTREAM** commands in *Using the Node Management Services (NMS) Utilities*.

Open Configuration/Directory File

The Open Configuration/Directory File screen (#1) shown in Figure 15-2 is the first screen displayed when you run NMMGR.

Figure 15-2 Open Configuration/Directory File Screen

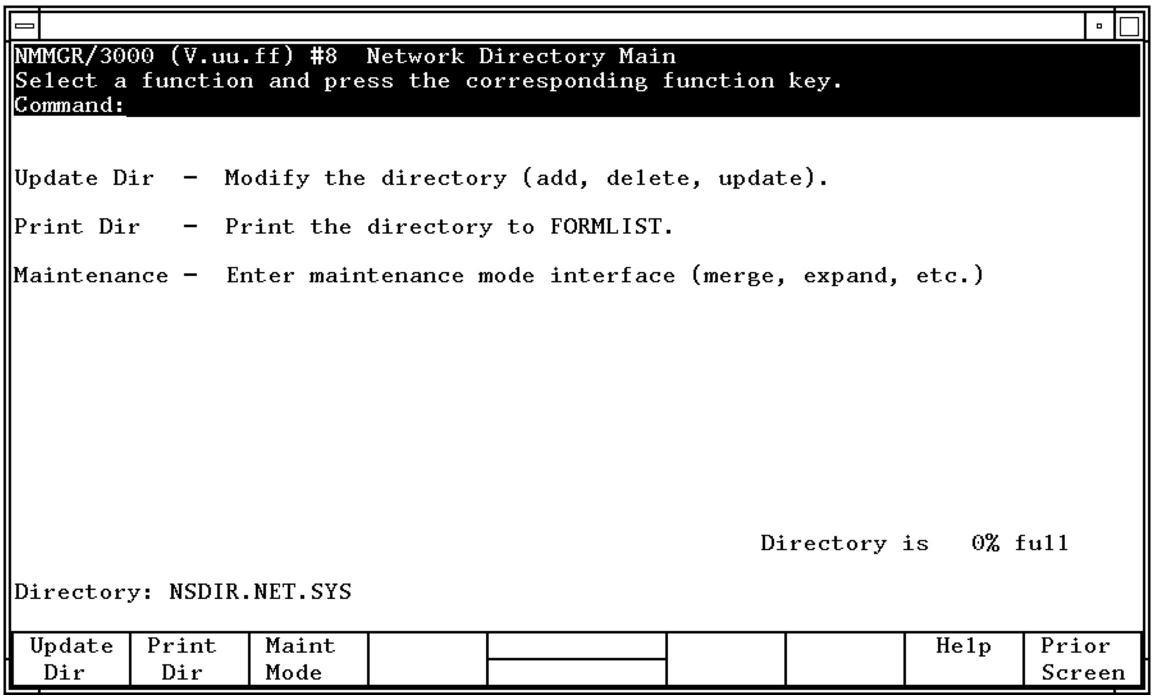


To create or modify a network directory, enter the network directory file name (and write access password, if one is required) and press the appropriate function key. The name `NSDIR.NET.SYS` is used by the network subsystems. If you create a network directory with a file name other than `NSDIR.NET.SYS`, it can be used to store network directory data, but the HP 3000 will not use it as a valid network directory until it is renamed to `NSDIR.NET.SYS`.

Network Directory Main

The Network Directory Main screen (#8) shown in Figure 15-3 is displayed when you press the **[Open Directry]** or the **[Create Directry]** function key at the Open Configuration/Directory File screen (#1) as shown in Figure 2-2. This screen is also displayed if a network directory has already been opened and you type **`NETDIR`** in the command window of any screen and press the **[Enter]** key.

Figure 15-3 Network Directory Main 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 all network directory screens. The percentage of the network directory that is full is shown in the lower right corner of the screen.

Press the **[Update Dir]** function key to modify the contents of the directory by adding, deleting and updating node names and path reports.

Press the **[Print Dir]** function key to print out a copy of the directory to formal designator `FORMLIST`, device class `LP`. You can use a file equation for `FORMLIST` to redirect the output to another device class or disk file. To set a file equation without leaving NMMGR, enter the appropriate MPE command, preceded by a colon (`:`), in the command window and press the **[Enter]** key.

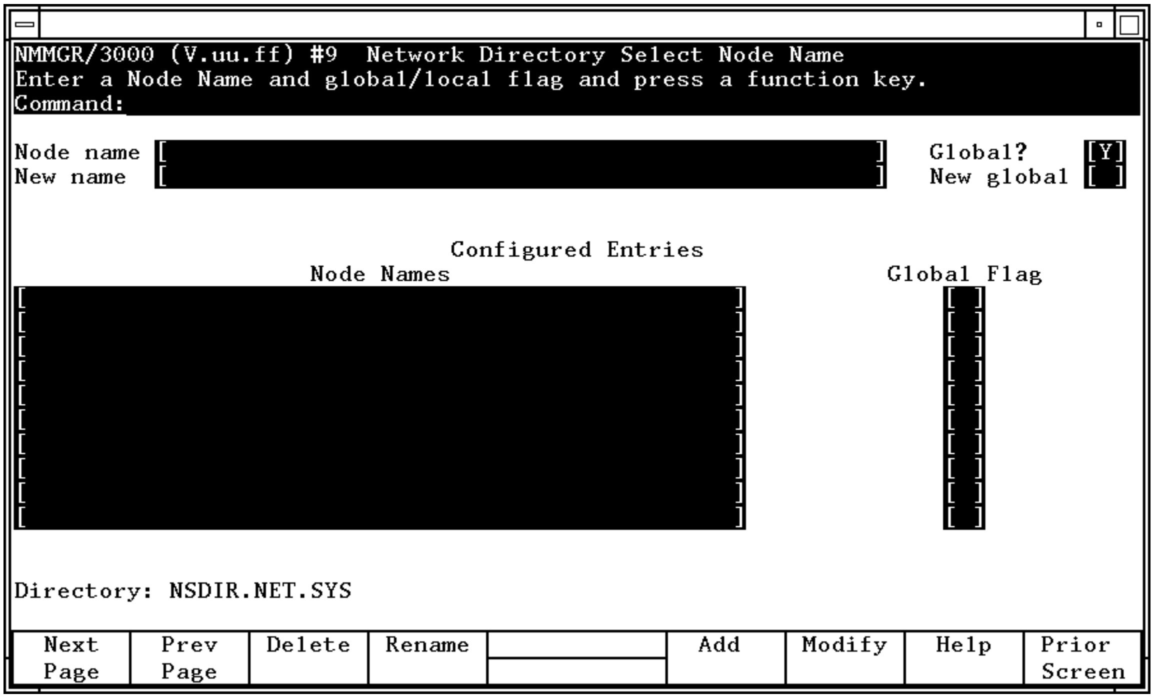
Press the **[Maint Mode]** function key to enter the command interface to perform directory merging or to expand the size of your directory. Refer to *Using the Node Management Services (NMS) Utilities* for details on maintenance mode.

Within the maintenance mode interface, command input is read from the formal designator `NMMGRCMD`, which defaults to `$STDINX`. Type `EXIT` and press the **[Return]** key to leave maintenance mode.

Network Directory Select Node Name

The Network Directory Select Node Name screen (#9) shown in Figure 15-4 is displayed when you press the function key for **[Update Dir]** at the Network Directory Main screen (Figure 15-3). The function of this screen is to display node names that are currently configured in the directory, and to allow you to delete, rename, add, or modify information about a node.

Figure 15-4 Network Directory Select Node Name Screen



Press the **[Next Page]** and **[Prev Page]** function keys to see additional nodes that have already been configured.

- To add a node to the directory, specify the node name and the global/local setting; then press the **[Add]** function key. You are taken to the Network Directory Data screen. You may add new entries as long as room remains in the file. If the file fills, you may use the Maintenance Mode command **EXPANDDIR** to expand the file.
- To modify path report data for a node in the directory, specify the node name; then press the **[Modify]** function key. This includes deleting part, but not all, of a node's path report list.
- To delete a node from the directory, specify the name of a node; then press the **[Delete]** function key. Press the **[Delete]** function key again to confirm the deletion.

- To change the name of a node in the directory, specify the node name and a new name; then press the **[Rename]** function key. The previously configured node name is replaced and the screen displays the new name in a display field under the label Configured Entries.

Fields

`Node name` The name of the node for which you want network directory information. The node name field must contain a fully qualified node name when used to add, modify, delete, or rename a node. The node name field is used with the **[Prev Page]** and **[Next Page]** function keys to browse through a specified part of the 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 `NIK`, and press the **[Next Page]** function key, the list of nodes will begin with the first matching node name, for example `NIKOLAI.FINANCE.IND`, and continue through the rest of the alphabet until all node names between the letters `NIK` and `Z` are listed.

`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 are displayed.

Entries can be configured as either global or local in the network directory. **Global** entries (the default) can be merged into other directories using the **`MERGEDIR`** command. Local entries are not merged into other network directories. The local entries are used for configuring localized network directory entries, thus providing a mechanism to restrict directory data from being propagated throughout the network.

A situation where this type of restriction could be useful is when you want to change the configuration for users on a single host, but not for everyone else. You 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 does not 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 contains information about the new link not included in the global entry configured for users on other nodes.

Other uses of local entries include restricting certain nodes from communicating with the internet, 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 for the same node, the network transport uses the local entry.

Default value: Y

Range: Y or N

`New name` **(Required only when renaming an existing node name.)** New name to be assigned to the node with the `Rename` function key.

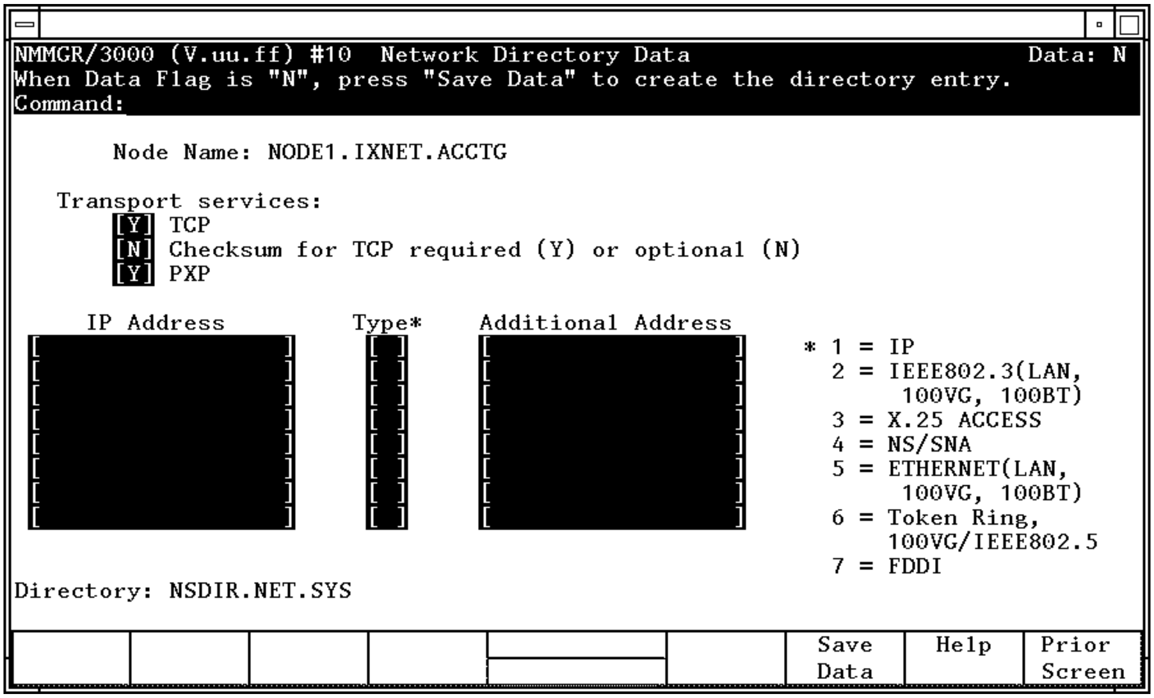
`New global` The global/local flag setting for the node named in the new name field. The acceptable values are `Y` or `N`. The only time this field is used is when you rename a node or when you change the global/local setting of a node. The new name field can be left blank if you wish to change only the global/local setting.

`Configured Entries (node names & global flag)` Display-only fields that show node names and their global/local flag settings that are already configured in the directory.

Network Directory Data

The Network Directory Data screen (#10) shown in Figure 15-5 is displayed when you press the **[Add]** or **[Modify]** function key at the Network Directory Select Node Name screen (Figure 15-4).

Figure 15-5 Network Directory Data Screen



The function of this screen is to configure path report data for the node name listed at the top of the screen. One path report is configured for each NI on a node.

To delete a path report, clear all three path report fields to blanks and press **[Save Data]**.

NOTE NS/SNA is no longer offered as a product and has been removed from the Corporate Price List. The product is obsolete with no plans for support.

Fields

`Transport services` These three fields describe the transport services that should be configured in each path.

`TCP` TCP must be Y (yes) for all nodes. The default is Y.

Checksum for TCP	The checksum setting indicates whether checksumming is optional (N) or required (Y) for TCP. If this field is set to `N`, then the use of checksums is not requested when communicating with this node. If this field is set to `Y` then checksums are used when communicating with this node. Checksumming is required for communication to non-HP systems. The default is `N`.
PXP	PXP must be `Y` (yes) for all nodes. The default is `Y`.

Note that the selection of transport services here must match the settings in the remote node's configuration file. If the checksum enabled field in the path `NETXPORT.GPROT.TCP` of this node is set to `Y`, then TCP checksum field in the network directory should also be set to `Y`.

`IP Address` One IP address should be entered for each network interface configured on the remote node that is directly reachable from this node. Each address must match an IP address configured in the remote node's configuration file. The path of the screen in the configuration file that contains IP addresses is `NETXPORT.NI.`*`NIname`*`.PROTOCOL.IP`.

`Type` A number indicating the type of path to configure is shown in Table 15-1:

1	Select this path type when the NI type is `ROUTER` (point-to-point); or when the NI type is `LAN` and the destination node supports probe or ARP; or when the NI type is `TOKEN` or `FDDI` and the destination node supports ARP.
2	Select this path type when the NI type is `LAN`, the destination node does not support probe, and 802.3 framing is used.
3	Select this path type when the NI type is `X25`.
4	NS/SNA is no longer offered as a product and has been removed from the Corporate Price List.

5 Select this path type when the NI type is `LAN`, the destination node does not support ARP, and Ethernet framing is to be used.

6 Select this path type when the NI type is `TOKEN` and the destination node does not support ARP.

7 Select this path type when the NI type is `FDDI` and the destination node does not support ARP.

Table 15-1 Path Type Configuration

NI Type	Framing	Protocols Supported by Remote Node	Type
Point-to-Point (Router)	N/A	N/A	1
LAN, VG100LAN, BT100	802.3 and Ethernet	Either Probe or ARP	1
		Neither Probe nor ARP	5
	802.3 only	Not Probe	2
	Ethernet only	Not ARP	5
X.25	N/A	N/A	3
SNA	N/A	N/A	4
Token Ring	N/A	ARP	1
	N/A	Not ARP	6
FDDI	N/A	ARP	1
	N/A	Not ARP	7

`Additional address` A lower-level address, which depends on the type.

Type 1 does not contain lower-level addressing information. You can leave the field blank, or enter the keyword `NONE`.

Types 2, 5, 6, and 7 require the destination node's station address, which is a string of six hexadecimal bytes, separated by dashes (*XX*-*XX*-*XX*-*XX*-*XX*-*XX*).

Type 3 requires an X.25 address key, which is an ASCII string of as many as eight characters. Each `NETXPORT.NI.`*`NIname`*`.X25.SVCPATH` screen may contain up to 2048 X.25 address keys. Each

`NETPORT.NI.`*`NIname`*`.X25.PVCPATH` screen may contain up to 128 X.25 address keys. No address key may be used more than once per system.

Type 4 requires the destination node's LU name. The LU name is taken from the host generation file of the IBM computer to which this HP 3000 is connected.

Glossary

A

access port A special interface card in the system cabinet through which the system console is connected.

address A numerical identifier defined and used by a particular protocol and associated software to distinguish one node from another.

address key *See* **X.25 address key**.

address resolution In NS networks, the mapping of node names to IP addresses and the mapping of IP addresses to link level addresses.

address resolution protocol (ARP) A protocol used by LAN links with Ethernet enabled that provides a means of exchanging addressing information between Ethernet nodes.

adjacent A node on a point-to-point network that is connected to another node by a single link with no intervening nodes.

ARP *See* **address resolution protocol**.

ASCII American National Standard Code for Information Interchange. A character set using 7-bit code used for information interchange among data processing and data communications systems. The American implementation of International Alphabet No. 5.

asynchronous A device's mode of operation in which a sequence of operations are executed irrespective of time coincidence with any event. Devices that are directly accessible by people (for example, terminal keyboards) operate in this manner.

Attachment Unit Interface

AUI. The cable that runs between each node (host, DTC, or other device) and the Medium Attachment Unit (MAU) that connects it to the LAN in a ThickLAN configuration.

AUI *See* **Attachment Unit Interface.**

autodial A dial link in which the remote node's telephone number is automatically dialed by a modem or other device with this capability.

B

backbone LAN A thick LAN cable conforming to the IEEE 802.3 Type 10 BASE 5 Standard.

back-to-back configuration A DTC configuration whereby MPE users connected to one DTC can communicate with a non-MPE/iX system connected to another DTC via the LAN. *See also* **local switching**.

backup configuration file A file that contains a copy of the information contained in the configuration file. The backup file, called NMCBACK.*group.account* by default, is updated each time the configuration file is successfully validated.

banner A welcome message displayed on your screen. On the local OpenView workstation a banner appears when a remote connection is established with the OpenView DTC Manager. A banner also can appear when you log on to MPE.

baud The measure of the speed at which information travels between devices, most commonly used in reference to terminal speed settings. Baud represents signal events per second. When one bit represents each signal change, baud is the same as “bits per second.”

binary mode A data-transfer scheme in which no special character processing is performed. All characters are considered to be data and are passed through with no control actions being taken.

bit Binary digit. A unit of information that designates one of two possible states, which are represented by either 1 or 0.

block mode A terminal processing mode in which groups, or “blocks,” of data are transmitted all at once.

BNC T-Connector A connector used to connect a computer or a component such as a DTC to the LAN in a ThinLAN configuration.

boundary *See* **network boundary**.

bps Bits per second. The number of bits passing a point per second.

broadcast Communication method of sending a message to all devices on a link simultaneously.

byte A sequence of eight consecutive bits operated on as a unit.

C

call In X.25, a call is an attempt to set up communication between two DTEs using a virtual circuit. Also known as a virtual call.

call collision A conflict that occurs at a DTE/DCE interface when there is a simultaneous attempt by the DTE and DCE to set up a call using the same logical channel identifier.

called address When a node sends out a call request packet, the packet contains the address of the destination node. The address of the destination node is the called address.

calling address When a node receives an incoming call packet, the packet contains the address of the sending node. The address of the sending node is the calling address.

carrier A continuous wave that is modulated by an information-bearing signal.

catenet *See* **internetwork**.

CCITT Consultative Committee for International Telephony and Telegraphy. An international organization of communication carriers, especially government telephone monopolies, responsible for developing telecommunication standards by making recommendations. The emphasis is on "recommendations"; no carrier is *required* to adhere to a CCITT recommendation, although most do so in their own interests.

CIB The channel input/output bus in the backplane of an HP 3000.

circuit-switching network A type of data communications network wherein a physical and exclusive link is maintained between two communicating devices for the call duration. An all-digital, circuit-switching network is often referred to as an X.21 network.

closed user group An X.25 user facility that allows communication to and from a pre-specified group of users and no one else.

compatibility mode A processing mode on HP 3000 Series 900 computers that allows applications written for MPE V/E-based systems to be ported and run without changes or recompilation.

computer network A group of computer systems connected in such a way that they can exchange information and share resources.

configuration 1) The way in which computer equipment is physically interconnected and set up to operate as a system.

2) The layout of the computer system, including the MPE table, memory, and buffer sizes, that tells which peripheral devices are (or can be) connected to the computer and how they can be accessed.

3) The process of defining the characteristics of a network in software. For MPE/iX-based computers, the operating systems are configured through use of the SYSGEN utility. Next, the Datacommunications and Terminal Subsystem (DTS) link is configured by using NMMGR (running on the host) and can, in addition, be configured using the OpenView DTC Manager software (running on the OpenView Windows Workstation) depending on the type of network management you use. A system that is to run network services (NS 3000/iX) is configured

through use of NMMGR. Access to X.25 is configured in two parts. The X.25 MPE/iX System Access software is configured on the host through use of NMMGR. The DTC/X.25 Network Access software residing on the DTC is configured at the OpenView Windows Workstation through use of the OpenView DTC Manager.

configuration file The configuration file contains the information that the network needs in order to operate. This file also contains information necessary for link- level and NetIPC logging. The only file name that the system recognizes is `NMCONFIG.PUB.SYS`

control-X echo Three exclamation marks (! ! !) output to the terminal screen when the cancel character (normally **[CTRL]-X**) is entered.

control-Y trap A user-written procedure to which control is passed when the subsystem break character (normally **[CTRL]-Y**) is entered during execution of a program with subsystem break enabled.

cross-validate The process of assuring that information contained in two locations is consistent where it is imperative that it be consistent. For example, an automatic cross-validation occurs when you enter SYSGEN to assure that information contained in `NMCONFIG.PUB.SYS` agrees with system configuration data.

CSMA/CD Carrier Sense Multiple Access with Collision Detect, transmission access method used by the LAN standard.

CSN *See* **circuit-switching network**.

CTB The cache transfer bus in the backplane of an HP 3000.

CUG *See* **closed user group**.

D

data Basic elements of information that can be processed or produced by a computer.

Datacommunications and Terminal Controller *See* **DTC**.

data overrun Transmitted data that is sent faster than the receiving equipment can receive it. The resultant overflow data is lost. *See also* **flow control**.

Datapac The national public PSN of Canada.

Datex-P The national public PSN of West Germany.

D bit Delivery confirmation bit. Used in the X.25 protocol, the setting of the D bit in DATA packets indicates whether delivery acknowledgment of the packet is required from the local DCE or from the remote DTE. It therefore allows the choice between local and end-to-end acknowledgment.

DCE Data circuit-terminating equipment. The interfacing equipment required in order to interface to data terminal equipment (DTE) and its transmission circuit. Synonyms: data communications equipment, dataset. A modem is an example of a DCE.

DDX The national public PSN of Japan.

dedicated printer A printer that can be used only by one host on the LAN—the one specified in the Destination Node Name in that printer's configuration screen.

default gateway A gateway accessible by a system may be designated as a default gateway. The network will then send any transmitted messages for which it is unable to locate a destination through normal means to the default gateway in a final effort to determine a transmission route.

demodulation The process by which the information-bearing signal is retrieved from a modulated carrier wave. The inverse of modulation.

destination node name In DTS configuration, it is either 1) the name of a host that a user can be connected to by default (if switching is not enabled for that user, or if automatic modem connection is enabled), or 2) the name of the only host that can access a dedicated printer.

device class A collection of devices that have some user-defined relation. Device classes are assigned through use of the NMMGR configuration program.

device-dependent characteristic A file specification for which modifications are restricted because of the type of device on which the file is opened. For example, data directed to terminals must have a blocking factor of one.

device driver A software module that controls a specific type of input/output device.

devicefile A file being input to or output from any peripheral device except a disk. MPE/iX allows operations to be performed on the device itself as if it were a file.

device independence A characteristic of the operating system that allows users to selectively redirect input/output from a program, session, or job without regard to the nature of the device.

device name *See* **PAD name**.

Dial ID protocol A proprietary Hewlett- Packard protocol that provides security checking and address exchange for dial links.

dial link A connection made through public telephone lines.

direct-connect device An asynchronous device that is connected directly to a DTC through an RS-232-C or RS-422 cable, with no intervening communications equipment. Also referred to as a "local connection."

direct connection A leased line, private line, or other non-switched link in a network.

direct dial A dial link through which only one remote node can be reached.

direct-path branching The process of directly accessing any screen in NMMGR by entering a path name in the `Command:` field. The path name must be preceded by an at sign (@).

domain name A name designated for a system in ARPANET standard format. This name can be used by other nodes on the network to access the host for which it is configured.

download The process of loading operating code and configuration files into the DTC's memory. The DTC is downloaded by the MPE/iX host for LANs using host-based network management, and by the PC for DTCs managed by the OpenView DTC Manager.

driver Software that controls input/output devices including NS 3000/iX links.

DTC Datacommunications and Terminal Controller. The DTC is a hardware device, configured as a node on a LAN, that enables asynchronous devices to access HP 3000 Series 900 computers. Terminals can either be directly connected to the DTC, or they can be remotely connected through a Packet Assembler Disassembler (PAD). The DTC can be configured with DTC/X.25 Network Access cards and DTC/X.25 Network Access software. A DTC/X.25 iX Network Link consists of two software modules: the X.25 iX System Access software (running on the host) and the DTC/X.25 Network Access software (running on the DTC).

DTCCNTRL A command file you can use to manage DTS configurations. Using DTCCNTRL, you can dynamically implement DTS changes, automatically add a new DTC, shutdown/restart DTS, and manage/dynamically configure host-based X.25 connections.

DTC identifier An identifier used only within NMMGR to define the branch of the configuration file containing information about a particular DTC. The identifier must begin with a letter and can be up to eight characters long.

DTC Manager *See* **OpenView DTC Manager**.

DTC node name A unique name used to identify a DTC on a LAN. The node name format is *nodename.domain.organization*, with each of the three parts having up to 16 characters. The name begins with either a letter or a digit.

DTC station address (802.3 address) A 12-digit hexadecimal number used to identify the DTC as a node belonging to the network configuration. Also called the LAN address or node address.

DTC switching A facility enabling terminal users to select any host system that they want to connect to. DTC switching is available only when the OpenView DTC Manager is used for network management.

DTC/X.25 Network Access The X.25 software that resides on the Datacommunications and Terminal Controller (DTC). To configure access to an X.25 network, you must configure two software components: the X.25 iX System Access (residing on the HP 3000 host), and the DTC/X.25 Network Access. DTC/X.25 Network Access is configured through use of the OpenView DTC Manager software for systems using PC-based network management or throughNMMGR for systems using host-based network management.

DTC/X.25 Network Access card The hardware card and channel adapter that provides X.25 Network Access. It resides in the Datacommunications and Terminal Controller (DTC).

DTC/X.25 iX Network Link

Software and hardware that provides MPE/iX access to private and public X.25 networks. The X.25 iX System Access software resides on an HP 3000 host and is configured through use of NMMGR. The DTC/X.25 Network Access software resides on the Datacommunications and Terminal Controller and is configured at the OpenView Windows Workstation for PC-based management and through NMMGR for host-based management.

DTE Data Terminal Equipment. Equipment that converts user information into data-transmission signals or reconverts received data signals into user information. Data terminal equipment operates in conjunction with data circuit-terminating equipment.

DTS Datacommunications and Terminal Subsystem. This consists of all of the Datacommunications and Terminal Controllers (DTCs) on a LAN, their LANIC cards (attached to the host), the LAN cable, and the host and DTC software that controls all related DTS hardware.

DTS restart The startup of the DTS subsystem using the DTCCNTRL command file after DTS has been shut down.

DTS shutdown The shutdown of the DTS subsystem, including the release of all TIO-related resources, using the DTCCNTRL command file.

duplex A transmission method that allows two-way communication. If both ends of the transmission link can transmit simultaneously, it is called full duplex. If only one end can transmit at a time, it is half-duplex transmission.

dynamic configuration The ability to make DTS configuration changes using NMMGR without rebooting the HP 3000 system.

E

entry priority In a point-to-point network, it is a ranking that identifies the most desirable route for data to travel from a given local node to a remote node.

environment A session that is established on a remote node.

escape from data transfer character A character that allows a user who is connected to a host system through the DTC, to break that connection and return to the DTC switching user interface. The default is **[CTRL]-K**. This character is used only on networks managed by the OpenView Windows Workstation.

escape sequence A sequence of characters beginning with the escape character and followed by one or more other characters, used to convey control directives to printers, plotters, or terminals.

Ethernet A Local Area Network system that uses baseband transmission at 10 Mbps over coaxial cable and unshielded twisted pair. Ethernet is a trademark of Xerox Corporation.

event log One of three circular files stored on the OpenView windows workstation. It contains lists of events that are reported by the DTCs for which it is responsible.

extended packet sequence numbering One of the optional Network Subscribed Facilities that provides packet sequence numbering using modulo 128. If not subscribed, modulo 8 is used.

F

facility An optional service offered by a packet switching network's administration and requested by the user either at the time of subscription for network access or at the time a call is made. Also known as user facility.

facility set A facility set defines the various X.25 connection parameters and X.25 facilities that can be negotiated for each virtual circuit on a per-call basis.

fast select An optional packet-switching network facility by which user data can be transmitted as part of the control packets that establish and clear a virtual connection.

FCS Frame Check Sequence. A sequence of bits generated by X.25 at Level 2 that forms part of the frame and guarantees the integrity of its frame's contents. The FCS is also used by the IEEE 802.3 protocol to check the validity of frames.

FDDI Fiber Distributed Data Interface. A set of ANSI standards that define a 100 Mb/s timed token passing protocol LAN that uses fiber optic cable as the transmission medium. FDDI is a specification for a high-speed fiber-optic ring network.

file equation An assignment statement used to associate a file with a specific device or type of device during execution of a program.

file number A unique number associated with a file when the file is opened. The file number is returned in the FOPEN or HPFOPEN call used to open the file. It can be used to access that file until the file is closed.

file specification The name and location of a file. The full specification for a file includes the file name, group, and account.

file system The part of the operating system that handles access to input/output devices (including those connected through the DTC), data blocking, buffering, data transfers, and deblocking.

flow control A means of regulating the rate at which data transfer takes place between devices to protect against data overruns.

flow control negotiation One of the network subscribed facilities selected at subscription time. This facility allows the Flow Control parameter to be negotiated at call set-up time, as opposed to having a predefined value.

formal file designator A name that can be used programmatically or in a file equation to refer to a file.

FOS Fundamental Operating System. The programs, utilities, and subsystems supplied on the Master Installation Tape that form the basic core of the operating system.

full gateway A full gateway is a node that belongs to more than one network and has one IP address for each network. It uses store and forward to transfer packets between each network that it belongs to.

G

gateway A node that connects two dissimilar network architectures. A gateway can be either a single node (full gateway) or two gateway halves.

gateway half A node that works in conjunction with another node on another network to form an internetwork. The only protocol used by gateway halves is the NS Point-to-Point 3000/iX Link. *See also* **full gateway**.

gateway-half link A link between the two nodes of a gateway-half pair. Each of the two nodes of a gateway-half pair has a configured link (hardware interface card) that is used for the gateway half network interface. The NS Point-to-Point 3000/iX Link is the only link that can be used as a gateway-half link.

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 the link.

guided configuration A method of configuring a node in which a subset of the complete NMMGR interface is presented, and defaults of configurable values are used automatically.

H

handshaking A communications protocol between devices or between a device and the CPU. Provides a method of determining that each end of a communications link is ready to transmit or receive data, and that transmission has occurred without error.

hop count *See* **internet hop count and intranet hop count**

host-based network management A method of managing asynchronous communications for HP 3000 Series 900 computers. All of the control software is configured on a single host and is downloaded to the DTCs that are managed by that host. With host-based management, a permanent relationship exists between each DTC and the host. Terminal users can access only the single system that owns the DTC their terminal is connected to.

host-based X.25 The management of X.25 network connections from a host computer. Host-based X.25 network connections are made through a DTC Network Access card installed in a DTC managed by the host. All configuration is accomplished using the NMMGR utility. It is not necessary for a PC to be part of the LAN when you are using host-based X.25.

host computer The primary or controlling computer on a network. The computer on which the network control software resides. For HP purposes, it can also be used to distinguish the HP 3000 Series 900 system (host) from the DTC.

HP block mode A block mode transmission method employed by HP computers where the system controls the block mode handshake. When HP block mode is used, the user program need not concern itself with data transfer protocol.

HP PPN Hewlett-Packard Private Packet Network. Hewlett-Packard's own packet-switching X.25 network, which gives users full control over the administration and security of their data communication.

HP TS8 A terminal server that can support up to eight asynchronous serial connections. When used in back-to-back configuration, users can access HP 3000 MPE/V systems on it through a DTC.

I

idle device timeout A timeout defined by the Configure: CPU command. When the timer lapses, a device connected to the DTC user interface that is still inactive will be disconnected.

IEEE 802.3 A standard for a broadcast local area network published by the Institute for Electrical and Electronics Engineers (IEEE). This standard is used for both the ThinLAN and ThickLAN implementations of the LAN.

IEEE 802.3 multicast address

A hexadecimal number that identifies a set of nodes. This address is used for multicast delivery.

IEEE 802.3 nodal address A unique hexadecimal number that identifies a node on an IEEE 802.3 LAN.

IEEE 802.5 A standard for a token ring network published by the Institute for Electrical and Electronics Engineers (IEEE). This standard is used for the Token Ring 3000/iX Network Link.

initialization string A sequence of control characters used to initialize a terminal, printer, or plotter when a connection is established from a host on the network.

interactive communications

Processing that allows users to enter commands and data at the terminal and receive an immediate response. Interactive processing occurs in session mode on MPE/iX systems.

internet communication

Communication that occurs between networks.

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

internet protocol A protocol used to provide routing between different local networks in an internetwork, as well as among nodes in the same local network. The Internet Protocol corresponds to Layer 3, the Network Layer, of the OSI model. *See also* **IP address**.

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.

internetwork Two or more networks joined by gateways.

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 point-to-point network.

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.

intrinsic A system routine accessible by user programs. It provides an interface to operating system resources and functions. Intrinsics perform common tasks such as file access and device control.

IP *See* **internet protocol**.

IP address Internet Protocol address. An address used by the Internet Protocol to perform internet routing. A complete IP address consists of a network portion and a node portion. The network portion of the IP address identifies a network, and the node portion identifies a node within the network.

IP router A node in an IP network that connects two or more networks and provides address mapping between them. The router selects messages from incoming buffers and places them into the appropriate outgoing message queues.

IP subnet mask. *See* **subnet mask.**

ISO International Organization of Standards. An international federation of national standards organizations involved in developing international standards, including communication standards.

LAP-B must also be used over direct-connect NS Point-to-Point 3000/iX Links.

L

LAN Local Area Network. A collection of data communication systems sharing a common cable whereby each system can communicate directly with another

LAN address *See* **station address**.

LANIC *See* **Local Area Network Interface Controller**

LANIC physical path The physical location (slot number) of the LANIC within the SPU.

LANIC Self-Test A ROM-based program on a LANIC card that tests and reports the status of the LANIC hardware.

LAP Link Access Protocol. The data link protocol specified by older versions (prior to 1980) of X.25 at Level 2 but still permitted and therefore usable. All new implementations of X.25 must use LAP-B, and all old implementations must migrate to LAP-B at a future date.

LAP-B Link Access Protocol-Balanced. The data link protocol specified by the 1980 version of X.25 at Level 2 that determines the frame exchange procedures.

LCI Logical Channel Identifier. Local value on a network node which identifies the channel used to establish a virtual circuit (SVC or PVC) through an X.25 network.

ldev *See* **logical device number**.

leased line A data-grade telephone line leased directly to a subscriber and allocated specifically for the subscriber's needs.

line speed The speed at which data is transferred over a specific physical link (usually measured in bits or kilobits per second).

link name A name that represents a hardware interface card. The link name can contain as many as eight characters. All characters except the first can be alphanumeric; the first character must be alphabetic.

Local Area Network Interface Controller (LANIC) A hardware card that fits into the backplane of the HP 3000 Series 900 computer and provides a physical layer interface for IEEE 802.3 local area networks.

local connection *See* **direct connection**.

local node The computer that you are configuring or that you are logged on to.

local switching A feature of the DTC which permits back-to-back configuration (for connections to an HP 3000 MPE/V host), using two ports of the same DTC. *See also* **closed user group.**

local user group A list defined for a particular DTC and card that specifies which *remote* nodes this DTC can send data to and also which *remote* nodes this DTC can receive data from.

logging The process of recording the usage of network resources. Events can be logged to both the OpenView workstation and to the MPE host.

logging class A number defining the severity of any given event logged. An operator uses the logging classes to specify which events are to be logged. Class 1 (catastrophic event) is always logged.

logical device number (ldev)

A value by which operating system recognizes a specific device. All DTC devices that are configured as nailed devices through the NMMGR configuration have ldev numbers permanently assigned. The DTC devices can then be accessed programmatically through use of their ldev number. Non-nailed devices have ldev numbers that are assigned from a pool of available ldev numbers for the life of their connection to a system. Each nailed port configured in NMMGR must have a unique ldev number.

log off The termination of a job or session.

log on The process of initiating a job or session.

logon device *See* **session-accepting device**.

loopback The routing of messages from a node back to itself.

LUG Local User Group. A list defined for a particular DTC and card that specifies which *remote* nodes this DTC can send data to and also which *remote* nodes this DTC can receive data from. *See also* **local user group**.

M

maintenance mode An NMMGR character mode interface used to manage both network directory and configuration files. It can be used interactively, from within the screen mode interface, or as a set of commands entered via a batch job.

map, network A drawing that shows the topology of the network. For networks managed by the OpenView DTC Manager a network map must be created through use of the OVDraw capability provided with the management software. A network map is also a hardcopy drawing used when planning a network. It shows network topology, node and network names, addresses, network boundaries (for an internetwork 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 point-to-point network. One mapping is configured at each node for every other node on the network to which messages will be sent.

MAU Medium Attachment Unit. A device attached to a ThickLAN coaxial cable that provides the physical and electrical connection from the AUI cable to the coaxial cable.

M bit More data bit. Setting this bit in a DATA packet indicates that at least one more DATA packet is required to complete a message of contiguous data.

medium attachment unit A device attached to a ThickLAN coaxial cable that provides the physical and electrical connection from the AUI cable to the coaxial cable.

MIT Master Installation Tape. A magnetic tape containing the Fundamental Operating System for an HP 3000 Series 900 computer.

modem modulator/demodulator. A device that modulates and demodulates signals. Primarily used for modulating digital signals onto carriers for transmission and for performing the inverse function at the receiving end. Modems are essential for transmitting and receiving digital signals over telephone lines.

modulo Value used as the counting cycle for determining the send sequence number (N(S)) of frames sent across an X.25 network.

modulation The process in which certain characteristics of a carrier signal are altered in accordance with the changes of an information-bearing signal.

MPE/iX MultiProgramming Executive POSIX. The operating system of the HP 3000 Series 900 computers. The NS 3000/iX network services operate in conjunction with the MPE/iX operating system.

multiplexer MUX. A device that allows multiple communication links to use a single channel.

N

nailed device A device with a permanently assigned ldev. The assignment is established through the system configuration of the MPE/iX host system. Nailed devices can be accessed programmatically through their ldev number. Nailed devices can also be assigned to more than one host.

native mode The run-time environment of MPE/iX. In Native Mode, source code has been compiled into the native instruction set of the HP 3000 Series 900 computer.

neighbor gateway A gateway that is in the same network as a given node.

NetIPC Network Interprocess Communication. Software that enables programs to access network transport protocols.

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

network address This can be either 1) the network portion of an IP address as opposed to the node portion, or 2) when referring to X.25 networks, it is a node's X.25 address.

network boundary The logical division between networks in an internetwork.

network directory A file containing information required for one node to communicate with other nodes in 1) an internetwork, 2) an X.25 network, or 3) a network that contains non-HP nodes. The active network directory on a node must be named `NSDIR.NET.SYS`.

network interface NI. The collective software that enables data communication between a system and a network. A node possesses one or more network interfaces for each of the networks to which it belongs. Network interface types are LAN, router (point-to-point), X.25, token ring, FDDI, VG100LAN, BT100, SNA, loopback, and gateway half. The maximum number of supported NIs per system is 12, one of which is reserved for loopback.

network management The collective tasks required to design, install, configure, maintain, and if necessary, change a network.

network map A drawing that shows the topology of the network. For networks managed by the OpenView DTC Manager, a network map must be created using the OVDraw capability provided with the management software. A network map is also a hardcopy drawing used when planning a network. It shows network topology, node and network names, addresses, network boundaries (for an internetwork map), and link types.

Network Services NS. Software application products that can be used to access data, initiate processes, and exchange information among nodes in the network. The HP 3000/iX Network Services include RPM, VT, RFA, RDBA, and NFT.

network subscribed facilities

A set of parameters that the user chooses when he subscribes to the X.25 network; they include flow control negotiation, use of D-bit, throughput class negotiation and extended packet sequence numbering.

network transport Software that corresponds to layers 4 and 3 of the OSI network architecture model. The function of this software is to send data out over the appropriate communications link, to receive incoming data, and to route incoming or outgoing data to the appropriate destination node.

NFT Network File Transfer. The network service that transfers disk files between nodes on a network.

NI *See* **network interface**.

NMCBACK.PUB.SYS The default file name for the file that contains a copy of the information contained in the configuration file (`NMCONFIG.PUB.SYS`). The backup file is updated each time the configuration file is successfully validated.

NMCONFIG.PUB.SYS The file that contains all of the network configuration data for the HP 3000 Series 900 computer on which it resides. It includes information about the DTCs that can access the system as well as information about any Network Service (NS) products running on the system. This is the only file name allowed.

NMDUMP Node management services trace/log file analyzer. A utility used to format log and trace files.

NMMAINT Node management services maintenance utility. A utility that lists the software module version numbers for all HP AdvanceNet products, including NS 3000/iX. It detects missing or invalid software modules.

NMMGR Node management services configuration manager. A software subsystem that enables you to configure DTC connectivity and network access parameters for an HP 3000 Series 900 computer.

NMMGRVER Node management services conversion utility. A conversion program that converts configuration files created with NMMGR from an earlier version to the latest format.

NMSAMP1.PUB.SYS A sample configuration file supplied with FOS that can be used as a template for DTS configuration.

NMSTART.PUB.SYS The file which contains maintenance mode commands executed during NMMGR startup.

node A computer that is part of a network. The DTC is also considered to be a node and has its own address.

node address The node portion of an IP address. The IP address consists of a node portion and a network portion.

node management services configuration manager *See* **NMMGR**.

node name A character string that uniquely identifies each system in a network or internetwork. Each node name in a network or internetwork must be unique; however, a single node can be identified by more than one node name.

node names list A list defined on the OpenView workstation and subsequently downloaded to all DTCs for which it is the "owner." The list specifies all of the HP 3000 Series 900 hosts on the LAN that are accessible from the DTCs.

non-adjacent Describes a node on an NS Point-to-Point 3000/iX network that is separated from a given node by intervening or intermediate node.

non-nailed device A session accepting device that is not permanently associated with an ldev number at configuration time. When the user at such a device logs on to an HP 3000 Series 900 system, an ldev is assigned from a pool of ldevs set aside for this purpose at configuration time. The association between a non-nailed device and this temporarily assigned ldev exists only for the duration of the session. One advantage of the use of non-nailed device connections is that configuration is simplified, since it is not required that each non-nailed device be individually configured.

NS 3000/iX A Hewlett-Packard data communication product that provides networking capabilities for HP 3000 Series 900 minicomputers. NS 3000/iX consists of a link and network services.

NS 3000/iX Link Software and hardware that provides the connection between nodes on a network. Some of the NS 3000/iX links available are the ThinLAN 3000/iX Link and its ThickLAN option, the DTC/X.25 iX Network Link, the NS Point-to-Point 3000/iX Link, and the Token Ring 3000/iX network link.

NS 3000/iX Network Services

Software applications that can be used to access data, initiate processes, and exchange information among nodes in a network. The services are RPM, VT, RFA, RDBA, and NFT.

NS Point-to-Point 3000/iX Link Hardware and software necessary to create networks in which data is transmitted from node to node over a defined route until it reaches it destination. This technique is referred to as store and forward. Systems in a point-to-point network are connected by means of leased or dial-up telephone lines. HP 3000 systems attach to the point-to-point network via HP 3000 Programmable Serial Interface (PSI) cards that fit into the back of each system's SPU.

NSDIR.NET.SYS Name of the active network directory file. *See also* **network directory**.

O

octet An eight-bit byte operated upon as an entity.

OpenView HP OpenView Windows is HP's network management environment. It provides the basic services for accessing and managing networks used by the DTC Manager, and other applications, such as Switch/PAD Manager, Hub Manager, etc.

OpenView Admin An OpenView Windows program that enables you to configure how your OpenView Windows applications will function. For example, it enables you to set a default map for the OpenView DTC Manager.

OpenView Draw An OpenView windows program that is used to draw the network map and to label the components on it.

OpenView DTC Manager An OpenView Windows application that enables you to configure, control, monitor, and troubleshoot the operation of the datacommunications terminal subsystems on the LAN.

OpenView Run An OpenView windows program that covers most of the control features used by the DTC Manager, including monitoring and diagnostic functions.

OpenView Windows The set of three programs: OV Admin, OV Draw and OV Run, running on the OpenView workstation under MS Windows, that acts as the platform for all OpenView applications, such as DTC Manager.

OpenView Windows Workstation The personal computer that provides software downloads to enable operation of the Datacommunications and Terminal Controller (DTC). The configuration software that runs on this workstation is called the OpenView DTC Manager software.

OSI model Open Systems Interconnection model. A model of network architecture devised by the International Standards Organization (ISO). The OSI model defines seven layers of a network architecture with each layer performing specified functions.

P

packet A block of data whose maximum length is fixed. The unit of information exchanged by X.25 at Level 3. The types of packets are DATA packets and various control packets. A packet type is identified by the encoding of its header.

packet exchange protocol

PXP. A transport layer protocol used in NS 3000/iX links to initially establish communication between nodes when NetIPC socket registry is used.

packet-switched network name The name of a data communication network adhering to the CCITT X.25 recommendation. This can be a PDN or a private network such as the HP PPN.

PAD (Packet Assembler/Disassembler A device that converts asynchronous character streams into packets that can be transmitted over a packet switching network (PSN).

PAD name A name of up to eight characters that is associated with a configured PAD device. The PAD name is known to both the DTC and the host systems that the device can access.

PAD profile A terminal or printer profile that specifies the configuration characteristics for PAD-connected devices.

partner gateway half When gateway halves are used, two gateway halves are required in order to provide communication between two networks. Each is the partner of the other.

path name When configuring with NMMGR, you can type a string in the `COMMAND:` field on a screen to branch to another screen. Each screen has a unique path name that corresponds to its location in the hierarchy of configuration screens presented by NMMGR.

PDN Public data network. A data communication network whose services are available to any user willing to pay for them. Most PDNs use packet switching techniques.

point-to-point A link that connects either two nodes in a NS Point-to-Point 3000/iX network or two gateway halves.

port An outlet through which a device can be connected to a computer, consisting of a physical connection point and controlling hardware, controlling software, and configurable port characteristics. Ports can be thought of as data paths through which a device communicates with the computer.

Precision Architecture The hardware design structure for the HP 3000 Series 900 computer family.

printer name A character string of up to 16 characters specified in the DTC Manager configuration (for networks using OpenView Network Management) to define a printer by name. Can be shared by several printers (port pool).

printer profile A set of configuration characteristics that can be associated with one or more printers through the NMMGR configuration. Printer profile specifications include the printer type, line speed, device class assignment, and other values relevant to printers connected through a DTC.

printer type A collection of characteristics that cause a printer connected to an HP 3000 Series 900 system to act and react in a specified manner. You can configure a printer to use one of the system-supplied printer types, or you can create custom printer types using workstation configurator.

privileged mode A capability assigned to accounts, groups, or users allowing unrestricted memory access, access to privileged CPU instructions, and the ability to call privileged procedures

probe protocol An HP protocol used by NS 3000/iX 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. A probe proxy server can provide a node with information about other nodes on the same or other networks of an internetwork.

profile A method of grouping device connection specifications and characteristics so that the set of characteristics can be easily associated with groups of like devices. *See also* **printer profile, terminal profile**.

program captive device *See* **programmatic device**.

Programmable Serial Interface PSI. A hardware card that fits into the backplane of the HP 3000 Series 900 computer. It provides a physical layer interface for NS Point-to-Point 3000/iX Links.

programmatic device A device operating under control of a program running on a computer. Programmatic devices can be used for input, output, or both, depending on the device and how it is opened by the controlling program.

protocol A set of rules that enables two or more data processing entities to exchange information. In networks, protocols are the rules that govern each layer of network architecture. They define which functions are to be performed and how messages are to be exchanged.

PSN Packet-Switching Network. Any data communication network in which data is disassembled into packets at a source interface and reassembled into a data stream at a destination interface. A public PSN offers the service to any paying customer.

PSS Packet-Switching System. The national public PSN of the United Kingdom.

PVC Permanent Virtual Circuit. A permanent logical association between two physically separate DTEs that does not require call set-up or clearing procedures.

PXP *See* **packet exchange protocol**.

Q

Q bit Qualified bit. When set in DATA packets the Q bit signifies that the packet's user data is a control signal for the remote device, not a message for its user.

QuickVal A software program that tests whether Network Services are operating correctly between nodes.

R

RDBA Remote data base access. A 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 connect device An asynchronous device that is indirectly connected to a DTC through a modem and telephone hook-up or through a PAD.

remote node Any network node that is physically separate from the node you are currently using or referring to.

retransmission count (N2) The maximum number of times a frame will be retransmitted following the expiration of the Retransmission Timer, T1.

retransmission timer (T1) The length of time that a transmitter will wait for an acknowledgment from a destination address before attempting to retransmit a frame. When choosing this value, factors like the line speed and maximum frame size should be taken into account.

RFA Remote file access. A network service that allows users to access file and devices on remote nodes.

router network *See* **point-to-point.**

routing The path that packets or fragments of a message take through a network to reach a destination node.

RMP Remote Maintenance Protocol. HP proprietary protocol used in DTC management.

RPM Remote Process Management. A network service that allows a process to programmatically initiate and terminate other processes throughout a network from any node on the network.

RS-232-C The Electronic Industries Association (EIA) Level 1 protocol specification that defines electrical circuit functions for 25 connector pins. HP provides two implementations of this standard: a 3-pin version for direct connections up to a distance of 15 meters (50 feet), and a version which makes use of additional circuits and can be used for either modem or direct connections.

RS-422 The Electronic Industries Association (EIA) Level 1 protocol specification implemented by HP in a 5-pin version which can be used for direct device connection up to a distance of 1500 meters (4000 feet).

S

security string An alphanumeric character string that functions as a password for dial links. The security string is used by the dial IP protocol.

serial device Any device that is attached to and communicates with a computer by means of a serial transmission interface. Terminals, printers, and plotters are among the devices that communicate serially with HP 3000 Series 900 computers.

serial transmission A method of transferring data in which characters are transmitted one bit at a time and received one bit at a time in the order of transmission. This transmission scheme is employed by devices connected to the system via the DTC.

session-accepting device A terminal or personal computer running in terminal- emulation mode that is able to establish an interactive (conversational) session with an HP 3000 computer. Also referred to as a logon device.

shared dial A dial link that provides connection to more than one remote system, although to only one at a time.

shared-line access The feature that allows two or more HP 3000 Series 900 hosts to use the same DTC/X.25 Network Access card on a DTC to access an X.25 network.

SIC Serial Interface Card. A card installed in the front of the DTC that acts as an interface between a corresponding Connector Card (CC) and the DTC's processor.

slaved device A device that shares the same DTC port as another device and is connected, to the other device, referred to as its master, by a cable. The actions of the slaved device are controlled by the master device.

SNMP Simple Network Management Protocol. An industry standard for managing networked computers in a multi-vendor environment.

SNMP agent A network node, such as a DTC, that is able to respond to SNMP requests.

SNMP manager A network management platform that is running software which allows it to manage SNMP nodes.

SNP Synchronous Network Processor card; an alternative name for an X.25 board.

spooled device A printer that is accessed through the spooling facility. The spooling facility allows a nonsharable device to be shared among several users by temporarily storing output data on disk and managing the selection of output spool files destined for the spooled device.

start bit A data bit used to signal the start of a character being transmitted in an asynchronous communication mode.

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.

stop bit A data bit used to signal the end of a character being transmitted in an asynchronous communication mode.

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 an internetwork. The word subnet is also a synonym for intranet.

subnet mask Grouping of bits that determines which bits of the IP address will be used to define a subnetwork. The subnet mask is configured using the NMMGR utility and specified in the same format as an IP address.

SVC Switched Virtual Circuit. The path through an X.25 network that is established at call set-up time.

switching *See* **DTC switching**.

Switching user interface The user interface available when DTC switching is enabled that allows terminal users to choose the HP 3000 Series 900 computer with which they want to establish a communication link.

synchronous A mode of operation or transmission in which a continuous data stream is generated without intervals between characters. The data stream is synchronized by clock signals at the receiver and transmitter. As a result, fast transmission speeds (above 9600 bps) are attainable.

SYSGEN The software program that allows you to configure the operating system on HP 3000 Series 900 computers.

system configuration The method for telling the operating system what peripheral I/O devices are attached and what parameters are required for system operation.

T

TCP *See* **transmission control protocol**.

telenet A proprietary public data network in the USA.

TermDSM Terminal online diagnostic system manager. A utility that provides diagnostic services for DTC connections by means of a series of commands accessible through the SYSDIAG utility. TermDSM is used only when DTCs are managed by a host system.

terminal name A character string of up to 16 characters specified in the OpenView DTC Manager configuration (for networks using OpenView Network Management) to define a terminal by name. It can be shared by several terminals (pool port).

terminal profile A set of configuration characteristics that can be associated with one or more terminals through the NMMGR configuration. Terminal profile specifications include the terminal type, line speed, device class assignment, and other values relevant to terminals connected through a DTC.

terminal type A collection of characteristics that cause a terminal connected to an MPE system to act and react in a specified manner. You may configure a terminal to use one of the system-supplied terminal types, or you can create custom terminal types using the workstation configurator.

ThinLAN A LAN that conforms to the IEEE 802.3 Type 10 BASE 2 standard LAN.

ThinLAN 3000/iX Link

Hardware and software necessary to create a broadcast network, which uses the IEEE 802.3 LAN cable to transmit messages to all the nodes on the network. The messages are then accepted only by the node or nodes to which they are addressed. Also includes the ThickLAN and StarLAN 10 options.

throughput class A value assigned to a given virtual circuit that defines how many network resources should be assigned to a given call. It is determined by the access line speed, packet and window sizes, and the local network's internal mechanisms.

throughput class negotiation

One of the network subscribed facilities defined at subscription time. This allows the user to negotiate the throughput class at call set-up time.

timer (T3) The length of time that a link can remain in an idle state. After the expiration of the timer, the link is considered to be in a non-active, non-operational state and is automatically reset. The value should be chosen carefully. In particular, it must be sufficiently greater than the Retransmission Timer (T1) so that no doubt exists about the link's state.

token ring A collection of data communication systems sharing a common cable and communicating by means of the IEEE 802.5 protocol. In a token ring network, access is controlled by the passing of a token from node to node. Outgoing messages are attached to the token and passed with the token until they arrive at the node to which they are addressed.

Token Ring 3000/iX Network Link Hardware and software required to connect a HP 3000 Series 900 system to a token ring network.

topology The physical arrangement of nodes in a network. Some common topologies are bus, star, and ring.

Transpac The national public PSN of France.

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.

transparent mode A data transfer scheme in which only a limited number of special characters retain their meaning and are acted on by the system. All other characters are considered to be data and are passed through with no control actions being taken.

transport, network Software that corresponds to layers 4 and 3 of the OSI network architecture model. It sends data out over the communications link, receives incoming data, and routes incoming or outgoing data to the appropriate destination node.

TTUTIL Also known as the Workstation Configurator. A program, `TTUTIL.PUB.SYS`, on the HP 3000 that is used to create and modify terminal and printer type files.

Tymnet A proprietary public data network in the USA.

typeahead A facility that allows terminal users to enter data before a read is actually posted to the terminal.

U

UPS *See* **uninterruptible power supply**.

unacknowledged frame number (K) The number of frames that can be transmitted without receiving an acknowledgment from the destination address. When this number (K) frame is reached, the same K frames are retransmitted.

unedited mode *See* **transparent mode**.

uninterruptible power supply A hardware device that protects equipment from power failures and contains an internal storage battery to supply reserve power.

V

V.24 The CCITT recommendation that defines the function of the interchange circuits between a DTE and a DCE.

validation The process of ascertaining whether the network transport configuration file has been correctly configured. In guided NMMGR, you do this by pressing the Validate Netxport key.

VAN Value-Added Network. A data communication network that uses and pays for facilities belonging to another carrier. The value-added package is then sold to a user.

VC *See* **virtual circuit**.

virtual circuit A logical association between two physically separate DTEs.

virtual terminal A network service that allows a user to establish interactive sessions on a node.

VPLUS Software used to generate screens such as those displayed by NMMGR.

V-Series (V.##) CCITT A set of CCITT recommendations related to data communication over a voice-grade telephone network.

VT *See* **virtual terminal**.

W

WAN Wide Area Network. A data communications network of unlimited size, used for connecting localities, cities, and countries.

workstation configurator A utility (TTUTIL) that allows users to create customized terminal and printer types by entering data through a series of VPLUS screens.

X

X.3 Defines the user facilities that should be internationally available from a packet assembler/disassembler (PAD) facility, when this is offered by a public data network.

X.21 Defines the physical interface between a DTE and a DCE of a public data network where the access to the network is made over synchronous digital lines.

X.25 Defines the interface between a DTE and a DCE for packet mode operation on a public data network (PDN).

X.25 address The X.25 address provided by the network administration if you are connected to a public data network (PDN).

X.25 address key An X.25 address key is a label that maps a node's IP address to its X.25 address and its associated X.25 parameters. You have a combined maximum of 1024 X.25 address keys in the SVC and PVC path tables.

X.25 LUG address X.25 address of a node belonging to a LUG.

X.25 iX System Access The software that works in conjunction with the DTC/X.25 Network Access software to provide access to X.25. The software resides on an HP 3000 host and is configured through use of NMMGR. To configure access to an X.25 network, you must configure two software components: the X.25 iX System Access (residing on the HP 3000 host), and the DTC/X.25 Network Access. DTC/X.25 Network Access is configured through use of the OpenView DTC Manager software for systems using PC-based network management or through NMMGR for systems using host-based network management.

X.29 Defines the interface for data exchange between a packet-mode DTE and a remote packet assembly/disassembly (PAD) facility over a packet-switching network.

XON/XOFF protocol The flow control used by MPE/iX systems to protect against data overruns. XON/XOFF protocol is controlled by the data recipient who sends an XOFF character (ASCII DC3) to the sender if it is unable to continue to receive data. The sender suspends transmission until it receives an XON character (ASCII DC1).

X.Series (X.##) CCITT recommendations A set of recommendations for data communication networks governing their services, facilities, and terminal equipment operation and interfaces.

Index

Index

Index