NETMANAGE®

Configuration Guide

Standards Based IntraNet Solutions

Version 6.0

NetManage, Inc.
10725 North De Anza Blvd.
Cupertino, CA 95014, USA
Fax: (408) 973-8272
Internet: sales@netmanage.com, intl_sales@netmanage.com
support@netmanage.com, intl_support@netmanage.com

West Coast	East Coast	International
Sales: (408) 973-7171	Sales: (603) 888-2800	Phone: +972-4-8550234
Support: (408) 973-8181	Support: (603) 888-3500	Fax: +972-4-8550122

NetManage Configuration Guide, Version 6.0

June 1996

Part number 5000-60-0696

Notice

Disclaimer

NetManage makes no representation or warranties other than the standard warranty with regard to the contents of this manual or the suitability of this software product for any particular purpose. Therefore, NetManage assumes no liability for damages incurred directly or indirectly from errors, omissions or discrepancies between the software and this manual.

Important: You should carefully read the license terms and conditions included in this package before you open or use the product. If you do not agree with the terms and conditions, you should promptly return the product unopened.

Disclosure: Permission to use, copy modify, and distribute portions of this program are granted by M.I.T. and Carnegie Mellon. Such rights are granted provided that the names M.I.T. and Carnegie Mellon are not used in any advertising or publicity pertaining to the distribution of this program or portions thereof. M.I.T. and Carnegie Mellon make no representations about the suitability of this software, or portions thereof for any purpose. It is provided "AS IS" without expressed or implied warranty.

Trademarks

NetManage and the NetManage Logo are registered trademarks of NetManage, Inc. Automatic Internet, Chameleon, ChameleonNFS, and NEWT are trademarks of NetManage, Inc.

Contents

Chapter 1. Overview 1
NEWT Applications 2
Product Features 2
Other Products 3
Using This Manual 4
Finding Help 4
Starting Applications 4
Configuration Files 5
Status Bar 5
Toolbar 5
Smart Buttons 5
Changing Column Width and Order 6
License Violation Detection 6
Customer Support 6
Chapter 2. Protocol Extensions 9
Network Policy Management (NPM) 9
Weighted Fair Queuing (WFQ) 14
SOCKS 15
NetWareIP 16
Chapter 3. Setup 19
Hardware Requirements 19
Software Requirements 19
Preparing for Installation 19
Installing Your NetManage Product 20
Setting Up NEWT 20
Verifying Installation and Setup 26
Chapter 4. Customizing Your Setup 29
Setting Passwords 29
Modifying an Interface 29
Setting IP and Dynamic Configuration Options 32
Name Resolution 34
Setting Up Default and Alternate Gateways 37
Configuring Advanced Settings 38
Adding New Interfaces 40
Selecting an ISDN Interface 41
INETD Configuration 42
Chapter 5. Using Dialup Protocols 45
SLIP/CSLIP/PPP Setup 46

Connecting and Disconnecting the Interface 57
Verifying Setup....58
Using PAP and CHAP 59
SLIP/CSLIP/PPP Login Scripting 59
Multiple SLIP/CSLIP/PPP Interfaces 64
Chapter 6. Using Routing.... 65
Using Multiple Interfaces....65
Router Setup 67
Verifying Setup....68
Chapter 7. NEWT and SNMP 69
Network Statistics 69
Network Tables....70
Using the SNMP Protocol 70
Chapter 8. NEWTToolbar 75
Starting NEWTToolbar....75
Main Menu....75
Button Menu....76
Adding Applications to NEWTToolbar....77
Modifying NEWTToolbar Buttons 77
Starting an Application in NEWTToolbar....78
Exiting NEWTToolbar....78
Chapter 9. Ping - Network Testing.... 79
Ping Host....79
Ping Settings....79
Additional Online Information....80
Troubleshooting....80
Appendix A. Windows for Workgroups.... 81
Installing Windows for Workgroups....81
Over NDIS....81
Over NDIS with No Workgroups Networking Installed....85
With Novell and Workgroups Networking 87
With Novell with No Workgroups Networking Installed 92
New Installation Replacing Microsoft Stack with NetManage Stack....95
OEM Setup for WFW 95
Appendix B. Open Data-Link Interface (ODI) 99
About the Open Data-Link Interface (ODI) 99
Glossary
Index
Reader's Comment Form

Chapter 1. Overview

NEWT is a TCP/IP protocol stack for Microsoft Windows that NetManage includes with its products. NEWT provides Windows 95 or Windows 3.1 users a degree of network access previously available only to workstation and mainframe users. This level of connectivity is enhanced by the ease of use associated with Windows applications.

Note: This manual discusses setting up and customizing NEWT in the Windows 95 or Windows 3.1 environment. Windows NT users and users running the Microsoft TCP/IP stack in the Windows 95 or Windows 3.1 environment, need to configure the Microsoft TCP/IP stack as discussed in their Microsoft documentation.

Through the exclusive use of TCP/IP for all network communication, the user is guaranteed transparent access to a wide variety of systems that support these same protocols. Your Windows-based PCs can seamlessly integrate into existing network environments, or expand small networks into large ones, without the painful changes commonly associated with these transitions.

Most applications have both client and server capabilities. This permits building of peer-to-peer networks of PCs without the use of a centralized workstation or mainframe. This also eliminates the need for a proprietary protocol for PC-to-PC communication; it also means that TCP/IP no longer needs to be used only to provide host access.

The standard Network Device Interface Specification (NDIS) or Open Data-Link Interface (ODI) are used for all communication with the network adapter. This permits a single version of NEWT to work across a wide variety of industry-standard network adapters. Any network adapter that supports either the NDIS or ODI interface is compatible with NEWT, regardless of its manufacturer or type. This same standard also permits NEWT to run concurrently with a wide variety of existing network operating systems using the same network adapter.

In the past, PC users who wanted this level of connectivity were restricted by the capabilities of DOS and available hardware. Both Microsoft Windows 95 and workstation-class PC hardware require a new set of products to take advantage of their new capabilities. NetManage is the premier supplier of these products. Our products are not adaptations of previous DOS products. Instead, they are unique applications that take full advantage of Windows-based systems.

NEWT Applications

The following table describes the different NEWT applications and includes each application's icon:

Tool	Icon	Description
NetManage TCP/IP		
Custom		Lets you set up and configure your TCP/IP client. You can create LAN or dial-up interface profiles.
Dialer		Lets you establish dial-up connections to the Internet. You can also add and modify interfaces.
Desktop Management		
Ping		Checks your connection to a specified computer
NEWTToolbar		Maintains a list of applications that you can start without having to switch to another window

Product Features

NEWT incorporates a number of features not normally found in other networking products such as:

- Multiple windows running multiple TCP/IP sessions
- Implementation as Windows DLL (not a TSR)
- Use of a Windows point-and-click user interface
- Context-sensitive online help
- TCP and UDP protocol support
- Industry standard NDIS or ODI network adapters support
- Ethernet, token ring, SLIP, PPP, CSLIP, and ISDN interfaces
- Concurrent LAN and serial interfaces
- Integrated Serial dialing and gateway access
- Optional TCP/IP development kits

Other Products

NetManage is committed to expanding network capabilities in line with existing products. We will maintain our high standards for ease of use and integration with Windows.

Our current set of products includes:

- Chameleon: TCP/IP applications package for Windows
- ChameleonNFS ATX for Windows: TCP/IP applications package for Windows, including NFS client and server for Windows.
- ChameleonNFS ATX for Windows NT: TCP/IP applications package for Windows NT
- ChameleonNFS ATX for Windows 95: TCP/IP applications package for Windows 95
- Chameleon for Windows 95: TCP/IP applications package for Windows 95
- Chameleon/X: Chameleon bundled with Xoftware
- ChameleonNFS/X: ChameleonNFS bundled with Xoftware
- Internet Chameleon: Internet dialup access
- NEWTWatch: SNMP-based desktop management
- NEWT-SDK: Development kit for TCP/IP DLL, FTP DLL, SMTP DLL, SNMP DLL, and ONC RPC/XDR
- ECCO Lite™, ECCO Professional™: Personal information management and workgroup communications applications.
- NetManage IntraNet HostLink™: Full-featured terminal emulation solution for Windows PC users who need access to AS/400™ and IBM mainframe systems.

We also have native-language versions of some of our products in:

- Dutch
- French
- German
- Japanese
- Spanish

Using This Manual

Use this manual to configure NEWT on your computer in the Windows 95 or Windows 3.1 environment. You do not need to use this manual if you are using the Microsoft TCP/IP stack instead of NEWT. The following table indicates how to use this manual for the different environments in which you can run NetManage products:

Environment	Refer to
Windows NT	Chapter 2. Then refer to the user's guide for your NetManage product.
Windows 95 and using NEWT	Chapters 1 through 9. Then refer to the user's guide for your NetManage product.
Windows 95 and using the Microsoft TCP/IP stack	Chapter 2. Then refer to the user's guide for your NetManage product.
Windows 3.1 and using NEWT	Chapters 1 through 9 and appendices A and B. Then refer to the user's guide for your NetManage product.
Windows 3.1 and using the Microsoft TCP/IP stack	Chapter 2. Then refer to the user's guide for your NetManage product.

To use this document, you are assumed to be familiar with Windows 95 or Windows 3.1, DOS, and basic TCP/IP terminology. The troubleshooting sections of chapters provide a simple way to quickly diagnose problems you may encounter. The Glossary at the end of the manual defines basic terminology.

Finding Help

Most applications include online help, which you should use as your primary source for information about those applications. The Additional Online Information sections in this manual list many of the help topics available for an application.

To access online help from any application, choose the Contents command from the Help menu. You can navigate through a variety of topics by choosing the buttons along the top of the window, as well as by clicking on underlined text. Hypertext links are provided to cross-reference information.

You may obtain printed information by selecting Print Topic from the File menu; you may also copy text, using the Edit menu.

Starting Applications

How you start applications depends on the Windows environment in which your NetManage product is installed.

There is no need to quit a particular application to start another. Each application is totally independent of the others. You may minimize an application to help conserve screen space, if the desktop becomes too cluttered.

Separate discussions on starting applications in the different environments follow.

Starting Applications in Windows 95

To start an application in Windows 95, do the following:

1. Choose the Start button to open the Start menu. Then choose the Programs command.
2. From the menu that appears, choose the program group that contains the application you want to start.
3. From the menu that appears, choose the application you want to start.

Starting Applications in Windows 3.1

To start an application in Windows 3.1, choose (double-click) the corresponding icon. To start another copy of the same application, double-click the icon again. Some applications may be opened multiple times.

Configuration Files

Every application uses a configuration file to maintain its settings. This file is automatically loaded every time the application is started. Use the File menu to create a new default configuration (New), save the current settings (Save or Save As...), open another configuration file (Open...), or exit the application (Exit). If you quit an application without explicitly saving changes, the application displays a dialog box asking if changes should be saved.

Status Bar

All applications provide you the option of showing or hiding the application's status bar. The status bar is displayed at the bottom of the application window, where it shows messages and provides status and statistics about the current application.

Toolbar

The Toolbar menu item allows you to display or hide an application's toolbar. The toolbar gives you quick mouse access to several of the application's common functions.

Smart Buttons

The option to display toolbar icons, including each icon's description, is available in all applications.

Changing Column Width and Order

In some applications you can change the width of each column or field. You can also rearrange fields if you want to view them in a different order. To change the width of a column:

1. Position the mouse pointer at the right side of the column border for the column you want to resize.

2. Drag the column border to the desired size.

To move a column, select the column you want to move and drag it to its new position.

License Violation Detection

A license violation occurs when multiple copies of a single licensed copy of the product are present on a network. Under the license agreement, each copy of the product is for a single user only and must not be shared.

NEWT is not copy-protected and may be freely installed on any type of disk. Although you can make as many copies of the product as you like, the software notifies all illegal copies of a license violation.

Each copy of the software must have a unique serial number and key code. When the software detects a duplicate serial number on the network, a message is displayed on all duplicate serial numbered copies. This message interrupts all work in progress on the computers involved.

Note: All network activity is disabled after the license violation has been detected. The NetManage applications appear to run normally, but communication over the network is disabled.

Customer Support

Before you use NEWT, complete the enclosed registration card and mail it to NetManage. This will ensure that you will be provided with customer support. It will also allow us to keep you up-to-date on new products as they are introduced.

NetManage provides world-wide support for its customers. We can be reached at the following:

West Coast

- ❏ Sales Phone (408) 973-7171
- ❏ Sales Fax (408) 257-6405
- ❏ Support Phone (408) 973-8181
- ❏ Support Fax (408) 973-8272

❑ NetManage, Inc.
10725 N. DeAnza Blvd.
Cupertino, CA 95014 USA

East Coast

❑ Sales Phone	(603) 888-2800
❑ Support Phone	(603) 888-3500
❑ Fax	(603) 888-0304

Internet

❑ Sales	sales@netmanage.com
❑ Support	support@netmanage.com
❑ Compuserve	70640, 1074
❑ BBS	(408) 257-3794, 8-N-1

International

Internet	intl_sales@netmanage.com intl_support@netmanage.com

France

❑ Phone	+33-1-47720808
❑ Fax	+33-1-42046599

Germany

❑ Phone	+49 (0)8165/9470-0
❑ Fax	+49 (0)8165/9470-147

Israel

❑ Phone	+972-(0)4-8550234
❑ Fax	+972-(0)4-8550122

Japan

❑ Phone	+81-(0)332218400
❑ Fax	+81-(0)332218484

UK

❑ Phone	+44-(0)1483-881800
❑ Fax	+44-(0)1483-881818

Chapter 2. Protocol Extensions

NEWT includes the following protocol extensions. This chapter discusses each of these extensions.

- NetManage Policy Management (NPM), which controls the bandwidth available to specified network traffic.
- Weighted Fair Queuing, which guarantees bandwidth through routers for specified IP traffic.
- SOCKS, which restores functions that may be lost when you set up a firewall. This feature is available only for NetManage products running in Windows 3.1.
- NetWareIP, which lets you access Novell servers using the Internet Protocol (IP). This feature is available only for NetManage products running in the Windows 3.1 ODI environment.

Network Policy Management (NPM)

Network Policy Management lets you manage the bandwidth allocated to specified network traffic. It uses packet filters to identify outbound traffic, then either limits the speed at which the traffic is transmitted using the NPM Enforcer, or requests that a router guarantee a certain amount of bandwidth for the traffic using NPM Weighted Fair Queuing (WFQ) support. Speed limits are enforced for any type of traffic (IP, IPX, SNA, and so on) and apply to traffic leaving an individual workstation. Bandwidth guarantees are available to routed traffic for routers that support WFQ.

The following are examples of typical NPM usage:

- When you start an FTP file transfer, your other network applications slow down. Use NPM to limit the speed of the FTP traffic, and your other applications will perform as usual.
- Network games are overloading your network. Use NPM to limit the speed at which network game traffic is transmitted.
- You want to run an internet telephony application across your network. Use NPM Weighted Fair Queuing support to ensure router bandwidth for the telephony application. You could also simultaneously limit the bandwidth available to other applications on the system so that your conversation is not affected if you start an FTP file transfer while you are talking.

NPM is available to Windows NT, Windows 95, Windows 3.1 (ODI only), and Windows for Workgroup users.

About NPM Filters

NPM uses filters to recognize and regulate network traffic. A filter contains up to five criteria that specify the positions in a packet where you expect to find particular values. These five criteria are logically ANDed together and then compared to each outbound packet. All matching packets form a logical stream that is regulated according to the filter definition (any packets that do not match the criteria are simply passed through to the network). For example, filter criteria could isolate a stream of all packets with a particular IP destination address AND a particular destination port AND specified values in the packet. This stream would then be regulated by NPM, based on the filter's corresponding traffic setting.

You define filters in a text file as discussed in the Setting Up NPM section of this chapter.

Setting Up NPM

To set up NPM, do the following:

1. Use a text editor to create a filter input file based on the syntax described in the following table. For an example of such a file, see the Examples of an NPM Filter section in this chapter.

Field	Description
FILTER	Identifies the beginning of a filter for a Stream.
BANDWIDTH	Specifies number of bytes per second maximum for the stream, if you want to regulate the bandwidth. Omit this parameter if you do not want to regulate bandwidth for this stream. This field is optional.
IPPRECEDENCE	Specifies the IP precedence value to be placed in this streams packets if you want to set Weighted Fair Queuing for the stream. Omit this parameter if you do not want Weighted Fair Queuing for this stream. **Note:** No checking is done to ensure a packet is an IP packet. Be sure that you uniquely identify an IP packet in your filter's criteria if you set this optional field. If you set this field and your criteria match protocols other than IP, the bit positions of the non-IP protocols correspond to the IPPRECEDENCE field, which destroys the non-IP packet.
TOTAL:	Indicates the number of filter criteria for this stream.

Field	Description
CRITERIA	Consists of the OFFSET, LENGTH, and FILTER fields. You may have up to five sets of CRITERIA per stream, all of which must be matched to identify the stream. Enter the number of these sets in the TOTAL: field. Each set of CRITERIA begins with the word CRITERIA alone on a line and not preceded by any spaces or tabs. OFFSET: The offset (in decimal) into the packet for this filter. LENGTH: The number of bytes (in decimal) to match in this filter (from the offset position). FILTER: The bytes (as hex values) to match, separated by commas.

2. For ODI environments, add the following to your AUTOEXEC.BAT file so that NPM is loaded:

   ```
   GKINIT
   ```

3. Run GKENCRYP to encrypt the filter input file. To run GKENCRYP, enter the following command at the DOS prompt:

   ```
   GKENCRYP <input filename>
   ```

   For example, suppose FILTER.TXT is the name of the file that defines the NPM filters. Encrypt that file by entering the following command:

   ```
   GKENCRYP FILTER.TXT
   ```

   GKENCRYP processes the filter input file to create an encrypted output file called GKFILTER.DAT, which NPM uses. You can use GKFILTER.DAT locally or distribute it to workstations on your network through NEWTWatch or a similar application.

   Note: The network adapter will not transmit data if the GKFILTER.DAT file is deleted or corrupted.

4. Copy the GKFILTER.DAT file to the directory containing the NPM driver (%WINDIR% for Windows 95, or %WINDIR\SYSTEM32\DRIVERS for Windows NT.)

5. Reboot your system.

NPM will now regulate stream bandwidth (if the BANDWIDTH parameter was specified) and/or reserve network bandwidth for a stream (if the IPPrecedence parameter was specified).

Examples of an NPM Filter

This section includes two example files of NPM filters.

NPM Filter File that Manages the Bandwidth of FTP Traffic

The following is an example file for using the NPM Enforcer to manage the bandwidth of FTP traffic. This file sets the bandwidth to a maximum of 1000 bytes per second.

```
##########################################################################
#
# This is a filter file for use with GKINIT.EXE/GKENCRYPT.EXE
#
# This filter file should be used as input to the GKENCRYP.EXE utility
# which will create an encrypted version of this file called GKCONFIG.DAT.
# This dat file should be placed in the same directory as GKINIT.EXE.
#
# To filter some stream, you must specify at least one filter.  The
# beginning of filter is indicating by the FILTER keyword by itself on a
# line, NOT preceded by any spaces or tabs.
#
# For details on the filter fields, see the Setting Up NPM section of your
# NetManage Configuration Guide.
#
#########################################################################
# Set outbound FTP (Data) traffic to 1000 bytes/sec
FILTER
BANDWIDTH: 1000
TOTAL: 2

CRITERIA
OFFSET: 0
LENGTH: 2
STRING: 45,00

CRITERIA
OFFSET: 22
LENGTH: 2
STRING: 00,14

########## Set outbound FTP traffic to 1000 bytes/sec
FILTER
BANDWIDTH: 1000
TOTAL: 2

CRITERIA
OFFSET: 0
LENGTH: 2
STRING: 45,00

CRITERIA
OFFSET: 22
LENGTH: 2
```

```
STRING: 00,15
```

NPM Filter File that Sets the IP Precedence

The following is an example file for using Weighted Fair Queuing. It sets the IP precedence to 7. For details on Weighted Fair Queuing and IP precedence, see the Weighted Fair Queuing section of this chapter.

```
###############################################################################
#
# This is a filter file for use with GKINIT.EXE/GKENCRYPT.EXE
#
# This filter file should be used as input to the GKENCRYP.EXE utility
# which will create an encrypted version of this file called GKCONFIG.DAT.
# This dat file should be placed in the same directory as GKINIT.EXE.
#
# To filter some stream, you must specify at least one filter.  The
# beginning of filter is indicating by the FILTER keyword by itself on a
# line, NOT preceded by any spaces or tabs.
#
# For details on the filter fields, see the Setting Up NPM section of your
# NetManage Configuration Guide.
#
#################################################################
########## Set outbound FTP (Data) to precedence 7
FILTER
IPPRECEDENCE:7
TOTAL: 2

CRITERIA
OFFSET: 0
LENGTH: 2
STRING: 45,00

CRITERIA
OFFSET: 22
LENGTH: 2
STRING: 00,14
########## Set outbound FTP to precedence 7
FILTER
IPPRECEDENCE:7
TOTAL: 2

CRITERIA
OFFSET: 0
LENGTH: 2
STRING: 45,00

CRITERIA
OFFSET: 22
LENGTH: 2
STRING: 00,15
```

Weighted Fair Queuing (WFQ)

Weighted Fair Queuing (WFQ), which is a feature provided by some major router manufacturers, can guarantee bandwidth to specified IP traffic. WFQ is particularly useful for applications that require real-time performance capabilities across routed networks. Applications for which WFQ is useful include video-conferencing programs (such as NetManage's InPerson), video servers, internet telephony, real-time simulations, and other performance critical networking task software.

WFQ lets a router divide the bandwidth available on any link into eight distinct classes of traffic. You (or an application) choose a class by setting the value of the IP Precedence field in the IP header. The IP Precedence field can accept values from 0 (which is the default) to 7. If the IP Precedence field is set to a non-zero value 'n', the router guarantees that all such packets will have at least 'n' + 1 times the bandwidth of standard IP traffic with precedence set to 0. That is, if IP precedence is set to 7 in a stream of packets, these packets are guaranteed 8 times the bandwidth of the standard IP traffic.

Suppose you establish a video conference involving two workstations across a routed LAN where the slowest WAN link is a T1 (1.544 Mbps). The following reflects the minimum bandwidth guaranteed to each IP precedence class:

IP Precedence	Bandwidth Available
0	55142 bps
1	110284 bps
2	165426 bps
3	220368 bps
4	275710 bps
5	330852 bps
6	385994 bps
7	441136 bps

If there is no traffic of a given class, residual bandwidth is available to other classes. But, for example, priority 7 traffic is guaranteed at least 441136 bps. Thus, if the packets for a video-conferencing application are all sent with IP precedence set to 7, the application is guaranteed at least 441136 bps of bandwidth. The application could also be guaranteed more bandwidth by setting multiple, non-zero IP precedence values.

Proper administration of the use of IP precedence values is critical to the success of WFQ. Suppose there are 10 applications that all send at 500 Kbps and the IP precedence for each application is set to 7. Also suppose the limiting link speed on the

network is T1. There will be delays and possibly dropped packets in such a scenario, and the benefits of IP precedence and WFQ are reduced.

You can set the IP precedence of an application using the NPM software. Refer to the Network Policy Management section of this chapter for more information on this capability.

SOCKS

SOCKS is client/server software that ensures a host protected by a firewall does not lose access to Internet resources available through Telnet, FTP, Gopher, the World Wide Web, and so on. If you are using Windows 3.1, use SOCKS to restore Internet communications to a firewall-protected host without compromising your private network's security.

To restore Internet functions lost after you set up a firewall, do the following:

1. Configure a SOCKSPLUS server. (PrivateNet is NEC's SOCKSPLUS server. For details, refer to the PrivateNet Installation Guide)

2. Install your NetManage product. Configure the TCP/IP client and verify that the system is up and running as discussed in this manual.

3. Install your NetManage product. Configure the TCP/IP client and verify that the system is up and running as discussed in this manual.

4. Install the SOCKSPLUS client on the PC that is running your NetManage product.

5. Choose the SOCKSPLUS icon from your Windows Startup group. Then enter the IP address of the SOCKSPLUS server.

   This ensures that the SOCKSPLUS client will always find the SOCKSPLUS server.

Note: TCP is the only protocol SOCKSPLUS supports. NetManage applications that use UDP or other transport protocols cannot pass through the SOCKSPLUS firewall. For this reason, SOCKS does not support the following NetManage applications:

- Archie
- Bind
- InPerson
- NFS
- NISLookup
- PCNetTime
- Ping
- RealAudio

- Talk
- TFTP

NetWareIP

If your NetManage product is running in the Windows 3.1 ODI environment, you can use NetWareIP to communicate with a Novell NetWareIP server. NetWareIP is a feature offered by Novell to allow clients to access Novell servers using the Internet Protocol (IP).

Once NetWareIP is installed, all normal NetWare requests are encapsulated into IP packets which are processed by the client or server software at the endpoints. You can access all standard NetWare server features normally available from Windows. You can view and manage your NetWare directories and files, and you can run NetWare server-based Windows applications. Your Novell server can also act as an IP gateway and IP router for both standard IP traffic and encapsulated NetWare traffic.

NetWareIP will not run in a DOS window. That is, you cannot switch from Windows to the MS-DOS prompt and then work with the server. In addition, you cannot run DOS applications stored on the Novell server.

Setting Up NetWareIP

To access NetWare resources using your NetManage product's transport, install and configure your NetWare/IP server, DNS/DSS server, and NetWare/IP client software as discussed in your Novell documentation. Once this is done, ensure that you can access exported NetWare resources from the client.

After you verify NetWareIP is working properly, enable it to run over your NetManage product by doing the following:

1. Rename or remove Novell's WINSOCK.DLL from your NetWare/IP installation directory. This is C:\NET\BIN by default.

2. Install your NetManage product and use Ping to make sure that the NetWare/IP server is available.

3. Make the following changes to your STARTNET.BAT file or AUTOEXEC.BAT file. Usually the first three changes can be done in STARTNET.BAT, but AUTOEXEC.BAT may include those lines. (NETSTART.BAT is a batch file that AUTOEXEC.BAT refers to.) This discussion assumes that you installed your NetManage product in C:\NETMANAG.

    - Replace the C:\NET\BIN\TCPIP.EXE statement with the C:\NETMANAG\NMODI.COM statement. The NMODI.COM statement must appear between the 3c5x9 driver statement and the NWIP.EXE statement.
    - Remove (rem) the IPXODI.COM and TCPIP.EXE statements.

- Replace the C:\NET\BIN\NWIP.EXE statement with LH C:\NET\BIN\NWIP.EXE. This sets NetWareIP to load high.
- Delete the C:\NETMANAG\NMODI.COM statement that appears at the end of your AUTOEXEC.BAT file.

The following is an example of the changes you need to make in STARTNET.BAT or AUTOEXEC.BAT:

```
lsl
3c5x9
C:\NETMANAG\NMODI.COM
rem ipxodi
rem tcpip
C:\NET\BIN\NWIP.EXE
vlm
```

4. Reboot your system.

   Note: If your AUTOEXEC.BAT file fails at the NWIP.EXE statement, increase the FILES= statement of your CONFIG.SYS file. For example, FILES=60.

5. Define your domain server and gateway by using Custom as discussed in this manual. You can specify the NetWare/IP domain server as your domain server and the NetWare/IP server as your gateway, but you do not have to.

Chapter 3. Setup

This chapter discusses hardware and software requirements and setting up NEWT.

Hardware Requirements

Before you begin installing your NetManage product, you need an IBM PC (or compatible computer) with 4 MB or more of RAM, 386 CPU or later capable of running your Microsoft Windows operating system, mouse, CD ROM or a 1.44 meg, 3.5" floppy disk drive, and a hard disk with at least 20 MB free for product installation..

Software Requirements

Microsoft Windows NT, Windows 95, or Windows 3.1 is required.

Preparing for Installation

Before you install your NetManage product, make sure you have completed and verified the installation of your Microsoft's Windows operating system. For more information, please refer to Microsoft documentation.

Contact Microsoft if you experience any Windows NT, Windows 95, or Windows 3.1 related difficulties.

To complete your installation, you will need some system and network information. Use the following form to help you collect the necessary information before you start the installation process. Example values are shown in brackets. If you are unsure of any information you need, see your system administrator.

General

Where to install software [C:\NETMANAG]	_____
Interface type [Ethernet]	_____
Internet address [156.27.1.51]	_____
Host name [my host}	_____
Subnet mask [255.255.0.0]	_____

For LAN interfaces

Adapter vendor name [3COM]	_____
Adapter type [3C503]	_____
Interrupt level [5]	_____
I/O base address [0x300]	_____

For SLIP/CSLIP/PPP interfaces

COM port [COM2]	_____
Baud rate [9600]	_____
Flow control [Hardware]	_____
Modem type [Hayes]	_____
Telephone number [408-123-1234]	_____

For ISDN interfaces

Vendor [ISDN.TEK]	_____
Board Type [ISDN.TEK1]	_____
IRQ_Level [5]	_____
Memory [0x300]	_____
SPID1	_____
SPID2	_____

Optional

Domain Name [netmanage.com]	_____
Default gateway [156.27.1.1]	_____
Domain server address [156.27.1.2]	_____

Installing Your NetManage Product

For details on installing your NetManage Product, see your installation instructions.

Setting Up NEWT

NEWT is NetManage's TCP/IP stack that is available for Windows 95 and Windows 3.1 users. If you are using NEWT rather than the Microsoft TCP/IP stack, you need to set up NEWT after installing your NetManage product.

How you set up NEWT depends on whether it is installed on a Windows 95 or Windows 3.1 system. Separate discussions on setting up NEWT in the different environments follow.

Setting Up NEWT in Windows 95

To set up NEWT in the Windows 95 environment, do the following:

1. Open the Control Panel.
2. Determine whether your system has a network adapter, and if it does, the type of network driver in use (NDIS or ODI). If you already know, proceed to step 3. If you are unsure, do the following:

   a) Choose the Network icon in the Control Panel.

   b) Look for a network adapter component in the network component list box . If you do not find one, your computer is not currently configured for use on a LAN. Make a note of None and proceed to the next step. If you do find one, select it and choose the Properties... button. The network adapter Properties dialog box appears.

   c) Make a note of the selected Driver Type option button: Enhanced mode NDIS, Real mode NDIS, or Real mode ODI. Choose the Cancel button. The Network dialog box appears.
3. Choose the Add button. The Select Network Component Type dialog box appears.
4. Select Protocol from the list box, then choose the Add button. The Select Network Protocol dialog box appears.
5. Select NetManage from the Manufacturers list box.
6. From the Network Protocols list box, select the appropriate NetManage TCP/IP protocol for your interface.

   - If you noted None in step 2, select the Dialup only protocol type.
   - If you noted Enhanced mode NDIS or Real mode NDIS in step 2, select the NDIS/Dialup protocol type.
   - If you noted Real mode ODI in step 2, select the ODI/Dialup protocol type.
7. Choose the OK button. The Network dialog box appears.
8. Choose the OK button.

   The Windows operating system copies the necessary system files and modifies the system registry. If any of these files cannot be located, the Windows operating system prompts you to specify the file's path (either the NetManage product's

program directory or the Microsoft Windows installation CD). When all files have been copied, the System Settings Change dialog box appears.

9. When you are prompted to restart your computer, choose the Yes button to exit NetManage Setup and restart your system. When the system has been restarted, configure your system as discussed in the Customizing Your Setup, Using Dialup Protocols, and Router chapters.

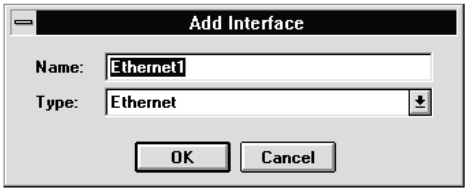
Note: The folder (directory) in which you installed your NetManage product will contain a folder for each installed application's program group and shortcuts for commonly used applications.

Setting Up NEWT in Windows 3.1

After you install your NetManage product in the Windows 3.1 environment , the Custom application takes you through the following steps that let you set up NEWT. If you are performing an upgrade installation, Custom will not start automatically.

Note: You can always run the Custom application separately (after you install the software) to change any values you specify; there is no need to run Setup again.

- After Custom starts, the Add Interface dialog box appears. In the Name text box, type a descriptive name for the interface. From the Type drop-down menu, choose the interface type (Ethernet, Token Ring, SLIP, PPP, or CSLIP). Choose the OK button and a new line entry is added to the Custom window for this interface.



- For LAN interfaces, the Hardware dialog box appears for NDIS only. For ODI, the Hardware... command is unavailable because your adapter should already be configured and functioning. Select the network adapter vendor name and adapter type.

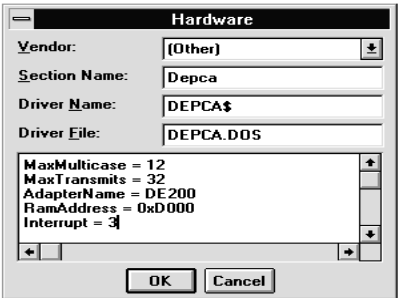
For each combination, there can be a different set of additional values that must be specified (for example, interrupt and base address). The defaults for these values are automatically selected, based on adapter type. Select the values that match your network adapter settings and choose the OK button.

- For the ISDN interface, the information you provide is used by your NetManage product to configure your ISDN.INI file for use with your adapter board.
- If your network card is not included in our vendor list, you can still use your NetManage product by entering information about this card in the 'Other' selection during the Hardware Setup.

To configure Custom to work with a network card not listed in our supported vendor list, do the following:

1. Complete the preparation form included in the Preparing for Installation section of this chapter.
2. Choose the Custom icon to start Custom. The Custom window appears.
3. Choose the Hardware... command from the Setup menu.

   The Hardware dialog box appears.



4. Specify information in the Hardware dialog box as discussed in the following table.

   Note: The information you provide is used by your NetManage product to configure your PROTOCOL.INI and CONFIG.SYS files for use with your adapter board. If you are familiar with the configuration of these files you may want to manually edit them and bypass the Other hardware setup in Custom by choosing None. If you choose to have Custom configure your PROTOCOL.INI and CONFIG.SYS files and your ISDN.INI file, you can still edit them manually later.

The following information also applies to the ISDN.INI file.

Option	Description
Vendor	Choose Other to specify that you are using another vendor.
Section Name	Type the name of the header in the PROTOCOL.INI file used to describe your network card. This name is placed in square brackets in the PROTOCOL.INI file. To determine this information look at the sample PROTOCOL.INI file that comes with your network cards NDIS driver.
Driver Name	Type the name used by the Drivername= parameter in the PROTOCOL.INI file. To determine this information look at the sample PROTOCOL.INI file that comes with your network cards NDIS driver.
Driver File	Type the actual name of the NDIS driver file for your network card. Entering this information will edit the CONFIG.SYS file to load the NDIS driver for your card.
Text box at the bottom of the dialog box	Enter additional parameters necessary for the PROTOCOL.INI network adapter section as required by your specific card. Consult the instructions that accompany your network adapter card for details. The information will typically appear under the NDIS or LAN Manager sections of the documentation.

In this example, entering the required information in the dialog box produced the following entries in the PROTOCOL.INI file.

```
 [DEPCA]
Drivername=DEPCA$
MaxMulticast = 12
MaxTransmits = 32
AdapterName  = DE200
RamAddress  = 0xD000
Interrupt = 3
 [Netmanage]
Drivername=NETMNG$
Bindings=DEPCA
```

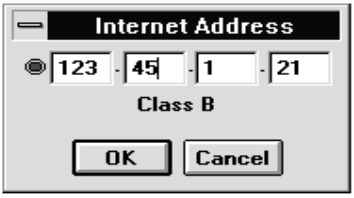
Note: Standard Micro Systems line of PLUS and ELITE Series adapter boards will require you to use the SMC provided NDIS driver, SMCMAC.DOS, rather

than the MACWD.DOS driver originally supplied by Western Digital. You can get this driver by contacting SMC or downloading it from their BBS. A representation of the entries require in the PROTOCOL.INI file is listed below:

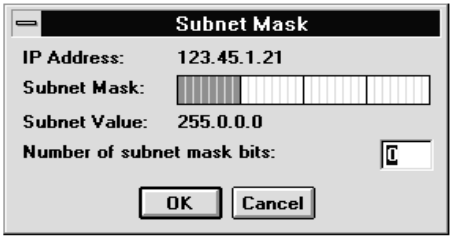
```
 [SMCMAC_NIF]
Drivername=SMCMAC$
IOBase=0x280
RamAddress=  0xD000
IRQ=3
 [Netmanage]
Drivername=NETMNG$
Bindings=SMCMAC_NIF
```

5. Choose the OK button.

6. In the Internet Address dialog box that appears, type your IP address. Avoid illegal addresses. For details on IP addresses, see the Custom online help.



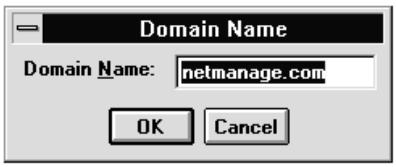
7. In the Subnet Mask dialog box that appears, type the number of subnet mask bits or drag the dialog box's subnet partition graphic display to the correct location. Then choose the OK button.



The subnet division is used to partition the IP address into a network portion and a host portion, if needed. See the Custom online help for more information. Depending on your network, a subnet mask may be optional.

8. In the Host Name dialog box that appears, type the network name of your computer. Then choose the OK button.

9. In the Domain Name dialog box that appears, type the name of the domain in which your computer resides. Then choose the OK button.



10. If your network uses the Network Information Service (NIS), specify the NIS domain name as discussed in the Customizing Your Setup chapter.

    NIS centralizes network administration including host and user list management. For details on NIS, see the Customizing Your Setup chapter.

11. Define the order in which your computer searches for IP address information. To do so, use Custom to define the host resolution order as discussed in the Customizing Your Setup chapter.

12. Select Save from the File menu to save your configuration.

    - If Custom needs to install an NDIS driver for your network card, it may prompt you to insert a specific diskette.
    - If you are using ODI, you will be prompted to specify the directory in which the NET.CFG file is located. Refer to the ODI appendix for detailed information on using ODI.

13. You are prompted to reboot, which you need to do to permit the NDIS drivers to load before you can use your NetManage product. Choose the OK button to exit Windows and restart your computer.

Verifying Installation and Setup

To verify that the installation process was successful, check your own IP address using the Ping application that is available with your TCP/IP product. If the Ping application fails, try the following to diagnose the problem:

❑ Run Ping. If a dialog box appears and indicates an interface initialization failure, check your network adapter settings and verify that they match those specified in the Custom application.

- ❏ If your system appears to crash or freeze, a conflict between Windows and other drivers may be the problem. Memory managers, such as EMM386, must have EXCLUDE statements for address ranges used by your network adapter. The interrupt setting may be in conflict with another device.
- ❏ Use your Ping application to check your local IP address. If this fails, you may have specified an illegal IP address.
- ❏ If you are able to ping other hosts on the network but not a device on the network, then try an IP address rather than the host name. If this fails, use the NEWT application statistics to determine if there are packet errors, a failure to receive or transmit, and so on. Lots of errors usually indicates a network adapter setting problem. Failure to receive anything usually indicates an interrupt problem. Receive problems may also mean an incorrect Ethernet Type setting or Frequent Destinations with incorrect physical addresses.
- ❏ If you want to refer to systems by name and not IP address, you must first define a host table or domain server. Refer to the Customizing Your Setup chapter for more information.
- ❏ If you want to communicate with systems that are on a different subnet, you must first define a default gateway or add Route Entries. Refer to the Customizing Your Setup chapter for more information.

Once these procedures are complete, you should have no problem using any of the NetManage user's applications. If a particular application fails to work, refer to the Troubleshooting section in the chapter discussing that application.

Chapter 4. Customizing Your Setup

You need to customize your setup as discussed in this chapter if you are using the NEWT TCP/IP stack.

The initial setup performed in the preceding chapter can be further customized through the use of the Custom application or the Dialer application. The next time a NetManage application is launched, the changes take effect. The following sections discuss setting passwords and modifying an interface to customize your set up.

Setting Passwords

To prevent users who do not have permission from changing Custom configurations, you can select the Set Password... option from the File menu to set a password for the Custom application. To set a password, do the following:

1. Start Custom.
2. Choose the Set Password... command from the File menu.
3. Type your password in the New Password box.

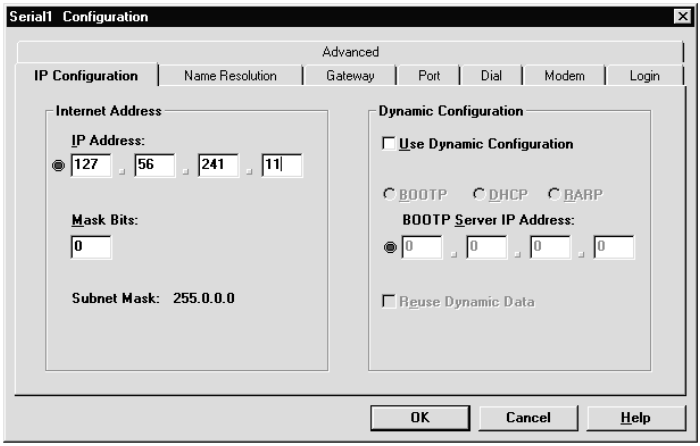
   If you have already set a password, Custom prompts you for your old password before you set up the new password.
4. Type the new password in the Confirm Password field and choose the OK button.

To delete your old password, type your old password and choose the OK button. You are prompted to enter your new password and confirm.

Modifying an Interface

Custom supports the following interfaces: Ethernet, Token Ring, FDDI, SLIP, PPP, CSLIP, or ISDN. Dialer supports SLIP, CSLIP, PPP, and ISDN interfaces.

You can modify these various interfaces. Most of the modifications you make to an interface are done through Custom's Configuration dialog box. You access this dialog box through either Custom or Dialer.



The tabs available in the Configuration dialog box depend on the type of interface you are configuring and whether you open the dialog box in Custom or in Dialer. The following table summarizes the function of each tab and whether a tab is available in Custom only or in both Custom and Dialer.

Tab	**Function**	**Available in**
IP Configuration	Sets the IP address, subnet mask bits, and configures your NetManage product dynamically	Custom (All interfaces)
Name Resolution	Specifies server information so that the mapping of IP addresses and computer names can be resolved	Custom (All interfaces)
Gateway	Sets the default gateway and two alternates and provides routing information	Custom (All interfaces)
Port	Sets communication port options	Custom and Dialer (Serial interfaces only)
Dial	Lets you enter telephone numbers you want to dial and set connection options	Custom and Dialer (ISDN and serial interfaces only)
Call Type	Sets options that provide support for data, video, voice, or X.25 calls	Custom and Dialer (ISDN interfaces only)
Modem	Sets options you need to configure if you are using a modem	Custom and Dialer (Serial interfaces only)

Tab	Function	Available in
Login	Lets you setup a login command and specify a login script	Custom and Dialer (ISDN and serial interfaces only)
Advanced	Lets you enter IP and physical address information for frequent connections, set up an interface as a primary interface, set the interface type or Ethernet type, and set multiple interface connection options	Custom (All interfaces)

Details on performing the tasks summarized in the preceding table are given in this chapter and the Using Dialup Protocols and Using Routing chapters.

Opening the Configuration Dialog Box in Custom

To open the Configuration dialog box in Custom, do the following:

1. Start Custom.
2. In the Custom window's list box, select the interface you want to modify.
3. Choose the Configuration... command from the Setup menu.

   The Configuration dialog box appears. The tabs available in this dialog box depend on the type of interface you selected.

Note: You can also open the Configuration dialog box by choosing (double-clicking) the interface you want to modify in the Custom window's list box.

Opening the Configuration Dialog Box in Dialer

To open Custom's Configuration dialog box from within Dialer, do the following:

1. Start Dialer.
2. Choose the desired interface in the Selected Interfaces option.
3. Choose the Configure.... button.

   The Configuration dialog box appears. The tabs available in this dialog box depend on the type of interface you selected.

Setting IP and Dynamic Configuration Options

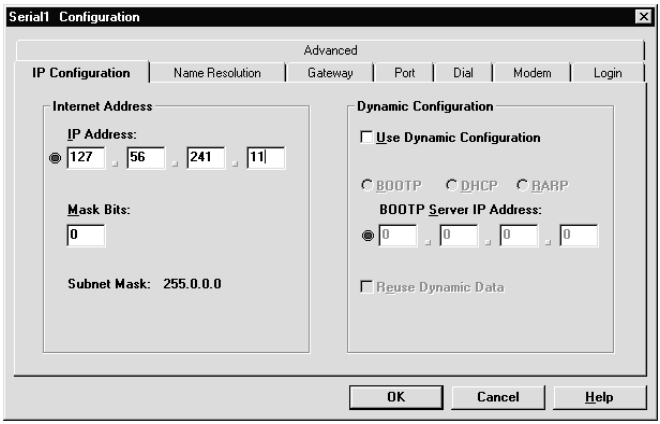
You set IP and dynamic configuration options to

- define the computer's IP address and subnet mask
- configure your NetManage product dynamically by setting up your computer as a client using one of the following protocols:
  - UDP/IP bootstrap protocol (BOOTP) client
  - Dynamic Host Configuration Protocol (DHCP) client
  - Reverse Address Resolution Protocol (RARP) client

  Your computer uses these protocols to find its configuration information, such as its IP address. For details on a protocol, see the section in this chapter discussing that protocol.

To set IP and dynamic configuration options, do the following:

1. In Custom, select the IP Configuration tab in the Configuration dialog box.



2. In the IP Address text box, type your IP address.

   Avoid illegal addresses. For details see the Custom online help.

3. In the Mask Bits text box, type the number of subnet mask bits.

   The subnet division is used to partition the IP address into a network portion and a host portion, if needed. See the Custom online help for more information. Depending on your network, a subnet mask may be optional.

4. Select the Use Dynamic Configuration check box. Then choose the button of the protocol (BOOTP, DHCP, RARP) you want your computer to use to find its configuration information.

Note: RARP is not available for serial dialup interfaces.

This chapter includes separate discussions on each of the protocols you can choose. For details on a particular protocol, see the appropriate section.

5. If you chose the BOOTP button and you want to specify a server IP address, do so in the BOOTP Server IP Address text box.

   Note: If you do not specify a server IP address, the BOOTP request will broadcast on the network. This is usually preferable.

6. To save the configuration information on your computer, select the Reuse Dynamic Data check box.

   If you store the configuration information obtained from a BOOTP or DHCP server, your computer will have access to that information if the server becomes unavailable.

7. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

About a BOOTP Client

The UDP/IP bootstrap protocol (BOOTP) permits a workstation to find its Internet address and other configuration information, such as default gateway and domain name server. A workstation running BOOTP client broadcasts onto the network a BOOTP request packet.

A machine running the BOOTP server application returns a response that includes the host's Internet address, the address of a boot server, the address of a default gateway, and other configuration information such as the addresses of the domain name servers, the subnet mask, and its host and domain name.

Note: The BOOTP information returned by the server will supersede your current configuration.

The BOOTP server must be on the same subnet or else a BOOTP helper is needed on the router.

About a DHCP Client

The Dynamic Host Configuration Protocol (DHCP) permits a workstation to find its Internet address and other configuration information, such as the default gateway and domain name server.

A machine running the DHCP server application returns a response that may include the host's Internet address, the address of a boot server, the address of a default gateway and other configuration information such as the addresses of the domain name servers, the subnet mask, and its host and domain name.

DHCP is more flexible and returns more information than BOOTP. It is a dynamic lease, meaning it may return different IP addresses depending upon what negotiation has taken place between your workstation and the DHCP server.

The DHCP server must be on the same subnet or else a DHCP helper is needed on the router.

About a RARP Client

The Reverse Address Resolution Protocol (RARP) permits a workstation to find its IP address. It returns no additional information other than the IP address which is based on a MAC address (Media Access Control). This protocol is useful for users who only have access to a Reverse ARP server. RARP is not as flexible as BOOTP or DHCP.

Note: RARP is not available for serial dialup interfaces.

Name Resolution

Computers on the network can identify one another through their IP address. However, you probably use names rather than cumbersome IP addresses to identify computers. The names and IP addresses need to be mapped to one another. You could do this by defining a host table on many computers on the network. As an alternative to a host table on many computers, some networks use a centralized name server to maintain name-to-IP address mappings.

Custom lets you

- specify server information
- define a host table

Specifying Server Information

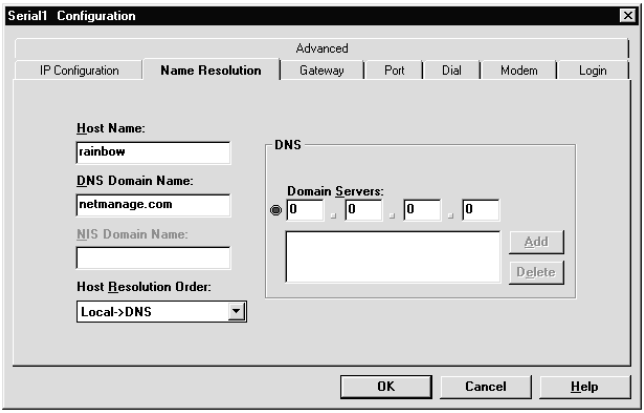
Specify server information to

- define which servers your computer can obtain name-to-IP address mapping information
- specify in which order your computer searches for IP addresses

  One or more tables may be referenced. These tables include the local host table available on your computer, a domain name server (DNS) if specified.

To specify server information, do the following:

1. In Custom, select the Name Resolution tab in the Configuration dialog box.



2. In the Host Name text box, type the network name of your computer.

3. In the DNS Domain Name text box, type the name of the domain in which your computer resides.

4. If you are using NIS, which you can do in the Windows 3.1 environment, enter an NIS domain name.

   The NIS Domain Name text box is dimmed in the Windows 95 environment.

5. Specify the order in which the tables that determine the IP address for a given host name are referenced. To do so, choose the desired option from the Host Resolution Order drop-down menu.

   The default resolution order is: 1) local HOSTS file 2) DNS.

   The HOSTS file is a table you can create as discussed in the Defining a Host Table section.

6. Specify which servers maintain name-to-IP address mappings. You do so by typing a server's IP address in the Domain Servers text box and then choosing the Add button.

   The IP address of a domain name server (DNS) and up to two alternates may be added to the list box. If you add one or more domain servers, a name lookup request is sent to the IP address of the DNS. If the request is not satisfied, the alternates are queried in the order specified in the dialog box.

   You can delete an IP address from the list box by selecting that address and then choosing the Delete button.

7. Do one of the following:
   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

Note: Your NetManage product can also be used as a domain server. Refer to the Bind chapter in your user's guide for more information.

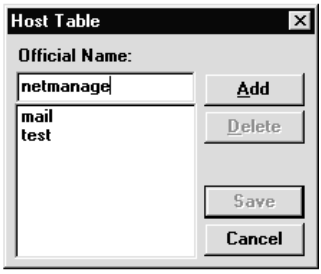
Defining a Host Table

Specifying systems by IP address is cumbersome and the addresses are hard to remember, whereas using names is a much more natural process. A standard hosts file (HOSTS), defined on many computers, can be used for this purpose.

To define the host table, do the following:

1. In Custom, choose the Host Table... command from the Services menu.

2. Type or select a host name, and choose the Add or Modify button. After all changes are completed, choose the Save button to update the host table file.



A second dialog box appears in which the IP address for the specified name and its aliases can be entered.

3. For each alias, type the name and choose the Add button. Once all changes are completed, choose the OK button to return to the Host Table dialog box.

Note: Changes to the host table can be made at any time, even while a NetManage application is running. Once these changes are saved, every program will have access to these new settings. The host table entries appear in all NetManage applications as a list of selections for a host name choice.

You may copy an existing host table file from another NetManage installation, or from another system, such as a Sun workstation. Place the file in your NetManage directory under the name HOSTS.

Setting Up Default and Alternate Gateways

Communication is normally limited to the systems directly connected to your network. Many networks actually consist of a collection of networks (called subnets) interconnected with routers (or gateways).

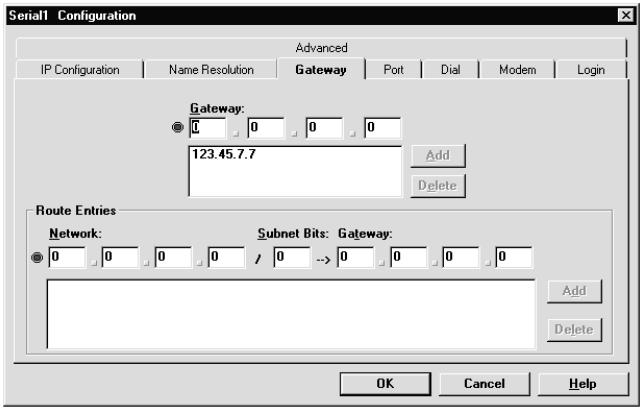
These routers are responsible for letting one subnet talk to any other indirectly connected subnet. To specify which router should receive communication destined for addresses in an unknown subnet, you need to set up a default gateway.

You can configure your set up for multiple gateway capability. This means if the first entry fails, the second and third gateway entries will be automatically tried.

The default and alternate gateways must exist on the same subnet as your local PC. For example, if your IP address is 123.27.1.2, your default gateway might be 123.27.1.1. assuming the subnet mask value is the same.

To set up a default gateway and its alternates, do the following:

1. In Custom, select the Gateway tab in the Configuration dialog box.



2. Specify the IP addresses of the default gateway and its alternates. To add a gateway's IP address, do the following:

   a) Type the IP address in the Gateway text boxes located at the top of the dialog box.

   b) Choose the Add button.

      The IP address is added to the Gateway list box. If you decide later to delete the IP address from the Gateway list box, do so by selecting the address and then choosing the Delete button.

3. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

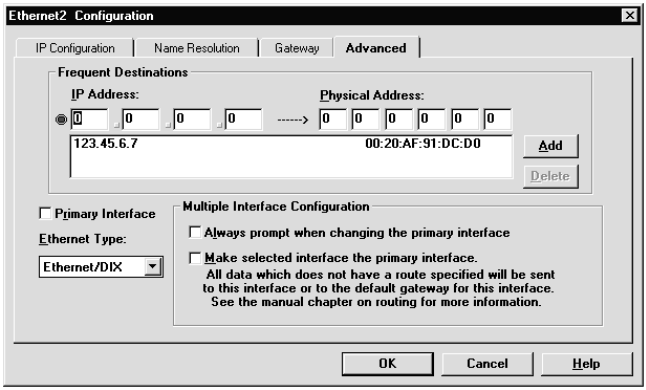
The Gateway tab also lets you set up routers as discussed in the Using Router chapter.

Configuring Advanced Settings

You can use Custom to set the following:

- frequent destinations
- primary interface
- Ethernet type
- multiple interface configuration

1. In Custom, select the Advanced tab in the Configuration dialog box.



2. If you plan to use the connection frequently, type the IP address and the physical address in the appropriate text boxes. Then choose the Add button.

When communication is first attempted to a particular IP address, the network software must determine the physical address for that IP address. This is accomplished through the use of the Address Resolution Protocol (ARP). You can avoid repeating this process for frequently requested connections by entering both addresses (IP address and physical address) in the Advanced tab.

Caution: Be careful when setting frequent destinations; an incorrect physical address may cause network communication conflicts.

3. If you want the interface to be the primary one, select the Primary Interface check box.

   Many software packages assume that the system on which it is running contains only one network interface and therefore has only one IP address. Because NEWT can support multiple interfaces concurrently confusion can result. The Primary Interface check box indicates which interface should supply the IP address of this system for these applications as well as default gateway and DNS.

   Caution: This setting is automatically set by Custom to the correct interface; modifications to this setting should be performed with caution.

4. If you are using Ethernet, use the Ethernet Type drop-down menu to specify the type of Ethernet packets your computer can transmit and receive.

   Ethernet physical layer packets are one of two forms: DIX or IEEE. The vast majority of networks use DIX, though all systems are designed to receive IEEE packets as well.

   Your NetManage product can receive both DIX and IEEE packets simultaneously and will send out the format selected in the dialog box. Many other machines will only receive the selected format.

   Caution: Unless you are absolutely positive that you are on an IEEE packet network, do not change this value. Many systems do not respond correctly to IEEE packets, making troubleshooting your network very difficult.

5. If you have set up your computer with multiple interfaces, you need to define how their operation is controlled. To do so, set the multiple interface configuration options as discussed in the Using Routing chapter.

6. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

Adding New Interfaces

How you add an interface depends on whether you are adding it in Custom or Dialer. Separate discussions for adding interfaces in each application follow.

Adding Interfaces in Custom

To add an interface in Custom, do the following:

1. Choose the Add...command from the Interface menu.
2. In the Name text box, type the name you want to assign to the interface.
3. From the Type drop-down menu, choose the type of interface you want to add. Then choose the OK button.
4. If you are adding an ISDN interface in Custom, choose the Hardware... command from the Setup menu. Enter the appropriate information in the Hardware dialog box.
5. Choose the Configuration... command from the Setup menu to open the Configuration dialog box.
6. Enter the IP address and subnet mask bits information. For details on specifying these options and the other IP Configuration options, see the Setting IP and Dynamic Configuration Options section.
7. Select the Name Resolution tab and the host resolution order. For details on specifying these options and the other Name Resolution options, see the Specifying Server Information section.
8. If desired, configure the options on the other tabs.

Adding Interfaces in Dialer

To add an interface in Dialer, do the following:

1. Choose the Add...command from the Interface menu.
2. In the Name text box, type the name you want to assign to the interface.
3. From the Type drop-down menu, choose the type of interface you want to add. Then choose the OK button.
4. Choose the Configure... button to open the Configuration dialog box. Then configure the options on the various tabs as discussed later in this book.

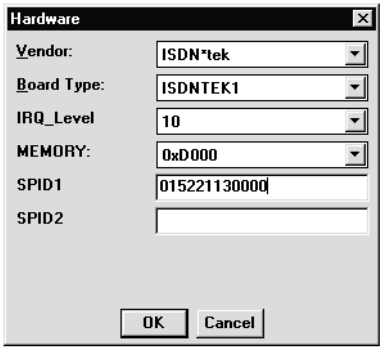
Selecting an ISDN Interface

You can select the Integrated Services Digital Network (ISDN) interface during the installation process. You can also select this interface after installation if you already have a dialup interface and are adding ISDN.

To select the ISDN interface in Custom or Dialer, do the following:

1. Choose the Add... command from the Interface menu.
2. Choose ISDN from the Type drop-down menu. Then choose the OK button. The ISDN interface name appears on the Custom window.
3. If you are using Custom, do the following. If you are using Dialer, go to the next step.

    a) Choose the Hardware... command from the Setup menu.

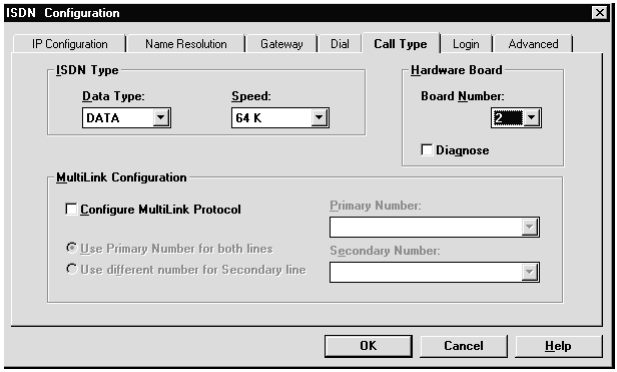


    b) Select the desired vendor from the Vendor drop-down menu. Type the appropriate numbers in the SPID1 and SPID2 text boxes and choose the OK button. Do not make any other changes in the Hardware dialog box.

    You can obtain the SPID1 and SPID2 numbers from your ISDN providers.

    Note: The IRQ_Level and Memory fields are the card defaults. If you need to change the hardware, you need to make the appropriate changes in the IRQ_Level and Memory fields.

4. Open the Configuration dialog box. To do so in Custom, choose the Configuration... command from the Setup menu. To open the dialog box in Dialer, choose the Configure... button.
5. Select the Call Type... tab.



6. Choose the appropriate data type and speed. Then choose the OK button.

   The Data and B 64K options are the default selections. This default configuration should be compatible with your system.

   Note: If you encounter any problems using 64K, check that your ISDN provider supports this speed end-to-end. If not, use the B 56K option instead.

7. If you want diagnostic information displayed in the log window at the time of connection, select the Diagnose check box. Choose the OK button.

The Board Number option specifies the ISDN board number.

For details on the MultiLink Configuration options, see your online help.

To make a successful ISDN call, you need to complete all the other options that are relevant such as login and dial/phone number.

INETD Configuration

The INETD (Internet Services Daemon) feature is based upon the UNIX INETD super-server which automatically launches other servers when requested. INETD saves memory and helps eliminate the necessity to launch individual servers.

For example, if someone wants to reach you using the Talk application and you do not have it open, but have it listed in your INETD configuration, then INETD will open it automatically when it senses that someone is trying to reach you through Talk.

Installing Servers Under INETD

To install servers under INETD, do the following:

1. Start Custom.

2. Choose the INETD Configuration... command from the Services menu. The INETD Configuration dialog box appears.

All the servers that INETD can open when requested are listed in the Services list box. A default list of servers that NetManage supplies initially appears.

3. Select the server or servers you want to install and choose the right-arrow button (>>). All selected servers will now appear under the Installed field.

   To remove any installed servers, select the desired server in the Installed field and choose the left-arrow (<<) button.

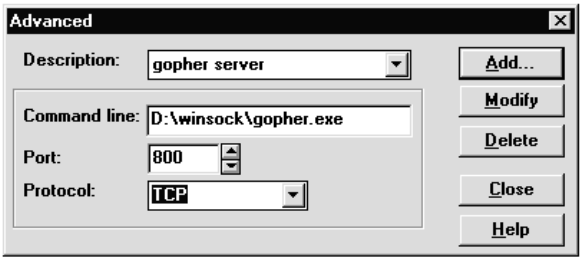
4. Choose the OK button to save changes.

Note: For any changes to take effect, you must restart Windows**.**

Adding New Servers to INETD

If you want to add additional servers that are not in the default list, do the following:

1. From the INETD Configuration dialog box, choose the Advanced button. The Advanced dialog box appears.



2. In the Description option, enter the name of the server you want to add. For example, if you want to add a winsock-based Gopher server, you could specify gopher server for this option.

3. In the Command line option, type the pathname of the server application you want to add. Then specify the port number in the Port field, and the protocol type in the Protocol field.

4. Choose the Add button to add the server to the list of servers in the INETD Configuration dialog box.

Chapter 5. Using Dialup Protocols

This section discusses how to use the following serial protocols with the NEWT TCP/IP stack:

- SLIP (Serial Line Internet Protocol)
- CSLIP (Compressed SLIP Protocol)
- PPP (Point to Point Protocol)

Before attempting a dialup connection using SLIP, CSLIP, or PPP, some additional settings are needed. These settings are made once initial installation and setup is complete. They vary, depending on the type of Serial/IP connection you are using. A sample of the various configurations that are supported includes:

- Direct serial connection (no modems)
- Modem connection directly to another system
- Modem connection through an Internet Provider (for example, PSI)
- Modem connection in Answer mode

Once a Serial/IP connection has been established, it appears to all network applications no differently than a LAN interface. This is an important point in that the network addressing rules that apply for LAN interfaces must also apply to Serial/IP interfaces.

For example, the two systems on the Serial/IP network (your local system and the remote system) must have a unique IP address (such as 123.27.4.1 and 123.27.4.2).

If one of the systems is a PC running your NetManage product with two interfaces, standard router addressing must apply. For example, the router may have an Ethernet side with address 135.27.4.1 and a Serial/IP side of 136.27.4.1. This places them on the separate subnets. Your Serial/IP address must be on the Serial/IP subnet.

Additional Information about SLIP/CSLIP/PPP

- SLIP and CSLIP are basically the same protocol, except header compression is used in CSLIP packet format. The TCP connection is faster when compressed header is used.
- PPP has the ability to negotiate several parameters such as header compression and IP addressing. PPP is faster due to header compression and larger packet sizes and provides enhanced security.
- The default MTU (Maximum Transmission Unit) for PPP is 1500.
- The default MTU for SLIP/CSLIP is 1006.

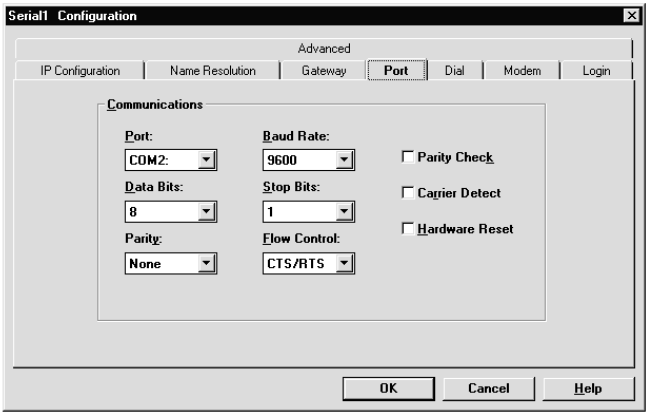
- CHAP and PAP - special packet format for negotiation of security with PPP (this is supported by NetManage PPP).
- NetManage PPP is in PASSIVE mode for the first 3 sec. If NetManage PPP does not receive any negotiation packet within first 3 sec, it will change to the ACTIVE mode begin PPP negotiation.
- SLIP / PPP / CSLIP are 8bit protocols (currently NetManage products only support 8bit login).

SLIP/CSLIP/PPP Setup

To set up NEWT for dialup access using SLIP, CSLIP, or PPP, do the following:

1. Follow the instructions described in the Installation and Setup chapter then select SLIP or any other serial connection interface as the interface type.

2. In Custom or Dialer, select the Port tab from the Configuration dialog box.



3. Specify the appropriate values for your dialup connection as discussed in the Changing Port Options section.

   Note: Changes to port settings other than the baud rate and connector settings should be performed with caution. In particular, hardware flow control is the default setting due to binary communication requirements.

4. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

SLIP/CSLIP/PPP Routing and Configuration

When setting up a SLIP connection, verify that the local PC and the remote device that you are dialing into (remote SLIP host) are on the same sub-net.

Example

If the IP address of the remote SLIP host is 156.27.50.1 and the sub-net mask is 255.255.255.0 (a class B address subnetted 8 bits) then the local PC's (HOST) IP address can be 156.27.50.2 with the same subnet mask.

Refer to the above example to note that a local PC and the remote server are located on the same subnet.

If the remote SLIP host is a Chameleon ATX PC with multiple interfaces (SLIP/PPP and Ethernet), then you must make sure that the SLIP/PPP and Ethernet interfaces are configured on separate subnets.

Example

SLIP/CSLIP/PPP Network Ethernet network
(A)==========(B) (C)----------(D)

Remote PC Router Host
running Chameleon ATX

In order to understand the addressing better, assign an IP address to each of the devices on the sample network

(A) -- Remote PC - 156.27.50.2 Subnet mask - 255.255.255.0

(B) -- SLIP/PPP interface on the Server: 156.27.50.1 (Chameleon ATX PC with two interfaces defined)

Subnet mask: 255.255.255.0

(C) -- Ethernet interface on the Server : 156.27.10.1 (Chameleon ATX PC with two interfaces defined)

Subnet mask: 255.255.255.0

(D) -- Host on the Ethernet network : 156.27.10.2

Subnet mask: 255.255.255.0

In order to establish communication from device **(A)** to device **(D).** Device **(D)** must know how to route back to the SLIP/CSLIP/PPP network via device **(C)**. You can accomplish this by specifying Device C as the Default Gateway for Device D.

After addressing issues are resolved, verify the SLIP/PPP port settings in the CUSTOM application (assuming that the user has defined SLIP, CSLIP or PPP interface already).

SLIP and PPP Differences from Ethernet Interfaces

Note that certain values in custom are not applicable to SLIP or PPP interfaces and do not need to be set. In particular, custom no longer requires either a Subnet Mask or Default Gateway for these interfaces. Other entries that will be ignored for SLIP and PPP are values for Route Entries or Frequent Destinations.

Changing between SLIP, PPP, and CSLIP

You can easily change the interface type between SLIP, PPP, and CSLIP by using the Interface Type option. Therefore, if you are using the pre-defined interfaces, you can automatically change the type of access defined for the provider of your choice by doing the following:

1. Select the Advanced tab in the Configuration dialog box.

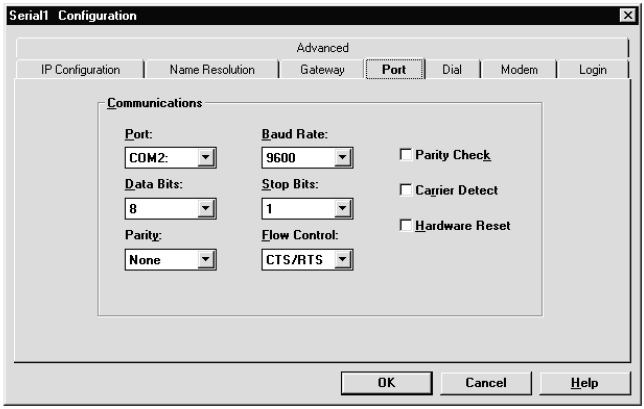
2. From the Interface Type drop-down menu, choose the appropriate interface type button (SLIP, CSLIP, or PPP) and choose the OK button.

Changing Port Options

Note: Changes to port settings other than the Baud Rate and Connector settings should be performed with caution. In particular, hardware flow control is the default setting due to binary communication requirements.

To change port settings, do the following:

1. In Custom or Dialer, select the Port tab from the Configuration dialog box.



2. Specify the appropriate values for your dialup connection.

   SLIP/PPP/CSLIP are 8-bit protocols and must have the following settings: 8 Data Bits, 1 Stop Bit, and None Parity.

Note: Changes to port settings other than the Baud Rate and Connector settings should be performed with caution. In particular, hardware flow control is the default setting due to binary communication requirements.

NetManage products do not support 7bit login.

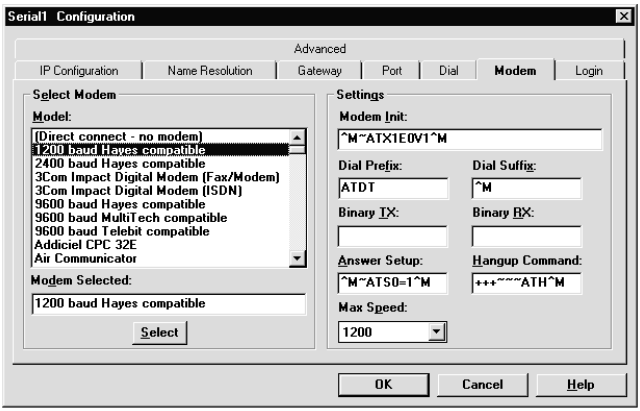
3. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

Changing Modem Settings

To change modem settings, do the following:

1. In Custom or Dialer, select the Modem tab in the Configuration dialog box.



2. From the Model list box, select the appropriate modem type and then choose the Select button.

   If your modem is not listed, selecting Hayes for the modem type works across most modem types. To indicate a direct null-modem connection, select [Direct connect - no modem]. A direct connection does not require any dialing.

3. In the Modem Init text box, type the modem initialization string that you want sent to your modem to prepare it for a dial-in connection. In the Dial Prefix text box, you can enter information that prepares the modem for dialing. In the Dial Suffix text box, you can enter information that signals the modem that dialing is to end.

   To configure for pulse dialing, specify ATDP in the Dial Prefix text box.

   NetManage supplied modem initialization strings are:

   - ^M (Ctrl + M): ASCII#13, <Enter>

- ~ (Tilde) - time delay, each '~' is a one second delay

Note: For information about any other string settings, refer to the manual provided by your modem vendor.

4. In the Answer Setup text box, type the string that you want sent to your modem to prepare it to answer a dial-back attempt.

5. In the Hangup Command text box, type the string that is to tell your modem to hang up.

6. From the Max Speed drop-down menu, choose the speed at which your PC is to communicate with your modem. The available speeds are in bits per second (BPS).

7. Do one of the following:

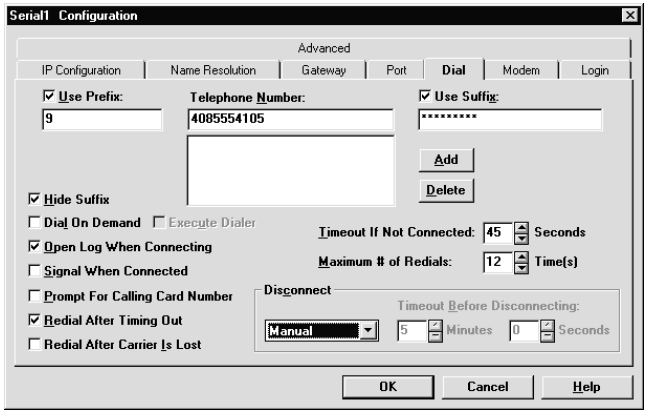
   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

Changing Dial Settings

To change dial settings, do the following:

1. In the Custom window, select the interface you want to change. Then choose the Configuration... command from the Setup menu.

2. In Custom or Dialer, select the Dial tab in the Configuration dialog box.



3. If a prefix must precede the telephone number you want to dial, select the Use Prefix check box. Then type the desired prefix in the Use Prefix text box. If a prefix is unnecessary, skip this step.

   The numbers you include in the Use Prefix text box can be any number that must precede the area code and phone number you want to dial. Typically such numbers

are another country's access code or an access line. (Dialing 9 before you can dial out is an example of using an access line.)

4. Specify the phone number you want to dial by either selecting it from the Telephone Number list box or typing it in the Telephone Number text box. If you want to indicate Answer mode when connected, leave the Telephone Number text box blank.

   You can create a list of frequently dialed numbers by doing the following:

   a) Type the desired number in the Telephone Number text box.

   b) Choose the Add button.

      The specified number is added to the Telephone Number list box. If you decide later to delete a number from the Telephone Number list box, select that number and choose the Delete button.

5. If a suffix must follow the telephone number, select the Use Suffix check box and then type the desired suffix in the Use Suffix text box. If a suffix is unnecessary, skip this step.

   A suffix is any additional numbers that you will need to enter before the connection can be made. For example, you can include a credit card or calling card number in the Use Suffix text box. A suffix could also be the numbers you are prompted for by your Internet provider's voice mail.

   You can keep your credit card or calling card numbers private by selecting the Hide Suffix check box.

6. If you anticipate that the connection may take a long time, increase the value specified in the Timeout If Not Connected text box.

   The minimum value for the timeout before disconnecting is 30 seconds.

7. Specify the method you want to use for disconnecting by doing one of the following:

   - If you want to disconnect any serial interface connection manually, choose Manual from the Disconnect drop-down menu. You disconnect manually by selecting the interface you want to disconnect and then choosing the Disconnect menu option.
   - If you want the interface connection disconnected automatically when the system detects no traffic (no packets being sent to or received from your system) for a specified amount of time, choose No Traffic from the Disconnect drop-down menu.. Then type the number of minutes and seconds you want to elapse before the interface is disconnected because no traffic was detected.
   - If you want the interface connection to disconnect automatically when the system detects no open connections, choose the No Connection from the Disconnect drop-down menu. For example, if you are currently connected and

running the FTP application, the interface connection will automatically disconnect after you close the FTP connection according to the specified timeout. If you choose this option, you need to type the number of minutes and seconds you want to elapse before the interface is disconnected because there is no open connection.

8. If you want to automatically connect or disconnect your interface through another application (such as FTP), select the Dial On Demand check box.

   For example, if you select this option, your system will automatically dial up when you choose Connect in FTP. Depending on how you selected your Disconnect option under the Dial tab, your serial connection can also automatically terminate when you disconnect your FTP session.

   Caution: You should always check your dial-up connections at the end of a session to be sure they are closed. Not all modems operate identically and unusual circumstances such as a PC being accidentally powered off may not guarantee a complete disconnect.

9. Set dial preferences by selecting or clearing the remaining check boxes. The following table describes the additional options you can set:

Option	**Description**
Hide Suffix	Select this check box if you want asterisks (***) rather than numbers to appear in the Use Suffix text box. This helps you keep your credit card or calling card numbers private.
Open Log When Connecting	Select this check box if you want to display the log while the connection is being made.
Signal When Connected	Select this check box if you want to be signaled with a beep when a connection is made.
Prompt For Calling Card Number	Select this check box if you want a prompt to appear reminding you to enter a calling card number while a connection is being made.
Redial After Timing Out	Select this check box if you want to automatically redial if there is a connection try time out. If you select this check box, you can specify how many times Custom or Dialer is to redial after a time out. To do so, enter the maximum number of redials in the Maximum # of Redials text box. You can specify up to 99 redials.

Option	Description
Redial After Carrier Is Lost	Select this check box if you want to automatically redial after a connection is lost.

10. Do one of the following:

    - Select another tab if you want to continue customizing your setup.
    - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

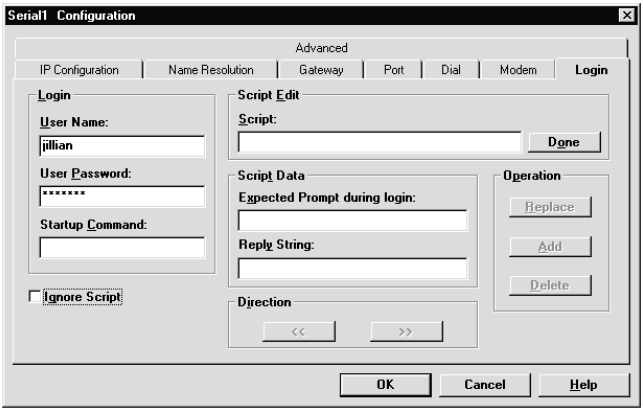
Specifying Login Settings and Script Edit Settings

You can specify login settings and integrate serial scripting features into Custom or Dialer. You no longer need to use the SLIP.INI file that was used in previous versions of your NetManage product to make changes to the scripts. Or, you can choose to use the Interactive Log Window feature instead as discussed in this chapter.

Note: You do not need to write your own script if you use the Dialer learn mode feature as discussed in the Capturing Scripts section in this chapter.

To set your login settings and edit a script, do the following:

1. In Custom or Dialer, select the Login tab.



2. Type the username, password, and startup command string for dialup service providers.

   These fields are transmitted when the login script is executed. The username is required for the script to be executed even if there is no need for a username.

3. In the Script text box, enter the script you want to edit. If you already know what you want to edit, you can edit the script directly in this field. Otherwise, do the following:

   - To display each Expect and associated Send statement, use the left arrows (<<) to move backward through the script, and use the right arrows (>>) to move forward through the script.
   - To replace existing statements in the script, move through the script until the desired Expect and Send statements appear. Make the necessary changes. Then select the section you want to replace in the above script and choose the Replace button.
   - To insert new statements in the script, type new Expect and Send statements in the appropriate text boxes. Place your cursor in the Script text box where you want to insert the new statements and choose the Insert button.

   For details on writing scripts and example scripts, see the SLIP/CSLIP/PPP Login Scripting section of this chapter.

4. Choose the Done button when the script changes are complete.

5. Choose the Save command from the File menu to save these changes.

6. Do one of the following:

   - Select another tab if you want to continue customizing your setup.

Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

If you prefer to manually connect to the host rather than using the script automatically, select the Ignore Script check box and then refer to the Using the Interactive Log Window Feature (Custom Terminal) section.

Using Dialer's Learn Mode Feature

Dialer's learn mode feature lets you capture scripts so that you do not have to write your own. Discussions on capturing scripts and using a captured script follow.

Capturing Scripts

To capture a script for a dial-up interface, do the following:

1. Open Dialer . From the Selected Interface option, choose the interface for which you want to capture a script

2. Choose the Configure... button to open the Configuration dialog box. Then select the Login tab.

3. Select the Ignore Script check box. Then choose the OK button to close the Configuration dialog box. When prompted to save your changes, do so.

4. Choose the Learn Mode button.

   The NEWT - Terminal dialog box appears.

5. Choose the Capture button.

   Dialer begins building the script needed to login to the selected interface.

6. When you are prompted to login, do so.

7. When you are prompted for your password, choose the Password button and then enter your password. Also enter additional information if your dial-up server prompts you to do so.

8. Choose the End button.

9. Choose Exit from the File menu and then save your changes to your configuration file when prompted to do so.

Using Captured Scripts

To use a script you captured in Dialer, do the following:

1. Open Dialer.

2. Choose the Configure... button to open the Configuration dialog box. Then select the Login tab.

3. Clear the Ignore Script check box. Then choose the OK button to close the Configuration dialog box.

4. Choose the Connect button.

Using the Interactive Log Window Feature (Custom Terminal)

Use the Interactive Log Window feature if you prefer to manually connect to the host before establishing a script, or if you want to test your connection before creating a script.

If you already have an established script, follow steps 1-6. If you do not have a script defined then follow steps 3-6.

Note: Make sure you have completed the Port, Modem, and Dial settings before using the Custom Terminal feature.

1. In Custom or Dialer, select the Login tab.

2. Select the Ignore Script check box and choose the OK button.

3. In Custom choose the Connect menu option. In Dialer, choose the Connect... button.

The Custom-Terminal log window appears. You will hear the dial tone and see the dialing information appear in the Custom Terminal dialog box.

4. In the Custom Terminal log window, enter your login and password at the Login and Password prompts.

5. Choose the Set IP button to display the Internet Address dialog box. Enter your known IP address or the IP address given by the host in the Custom Terminal window and choose the OK button. Note that the IP Address button is equivalent to the -i option in Script.

6. In the Custom-Terminal log window, choose the Done button when the login process (entered and set IP Address) is complete. The Connect menu item in Custom now changes to Disconnect.

   If you begin to see an unrecognized series of ASCII characters in the Terminal window, then most likely the remote server has finished the login process and begun PPP negotiation. Or the remote server is sending SLIP data packets. Choose the Done button to end the login process.

7. When the connection is complete, choose the Close button to close the Custom Terminal log window.

   Note: You can also close the Custom Terminal log window after your system is connected by choosing the Close button. However, if you choose the Close button while a connection is taking place, a prompt appears asking if you want to disconnect.

Configuring MTU Sizes

NetManage products now have a configurable MTU size for serial interfaces. The default value for MTU is 1500 for PPP and 1006 for SLIP and CSLIP. To change the MTU value you can edit your WIN.INI file as follows:

```
 [TCPIP] section, add:
pppmtu=1500
slipmtu=1006
```

(Depending on your server configuration, it should not exceed this value)

The MTU corresponds to the largest packet that can be sent over the serial line. Packets are often smaller than 1000 bytes, so applications like Telnet may not show an improvement by raising the MTU, since most Telnet packets are small, containing only a few data characters.

Note: For additional information on configuring read and write size using SLIP and PPP, please refer to the section that discusses dialup protocols.

Connecting and Disconnecting the Interface

Once the interface has been properly defined as described in the setup section of this chapter, you must connect the interface using the Custom application. This is accomplished by selecting the interface in the Custom application and selecting the Connect menu item. A dialog box appears indicating that a connection is in progress. Once the connection is successfully established, the Connect menu item changes to Disconnect.

Choose the Disconnect menu option to terminate the connection after you have completed your work to disconnect manually. Choose the Log... command to view the connection progress.

Note: If you have chosen the No Traffic or No Open Connections items under the Dial menu then the connection will automatically terminate according to the timeout specified.

An icon appears at the beginning of the interface entry to signify that the interface is connected. It then appears in the list of current interfaces in the NEWT application. Disconnecting the interface removes the plus sign and the entry from the NEWT application. The icon for Custom also changes, indicating the connection. This appears when the Custom application is minimized. Note that NEWT will show a captured IP address.

You may change any of the setup values and connect the interface without saving the changes to the configuration file. This can be used to try a variety of settings before settling on the best one for your purposes. You can also use the Duplicate menu item in the Interface menu to create copies of an interface entry that differ only slightly, such as the IP, subnet, port, and so forth, each with its own telephone number. Additional SLIP entries may also be defined with entirely different settings.

Establishing Connections with Dialer

To use Dialer to connect a serial or ISDN interface to the Internet, do the following:

1. Start Dialer.

2. Specify the desired interface in the Selected Interfaces option.

3. If you want to configure an ISDN interface so that it can support up to two calls at the same time, select the Use MultiLink Protocol check box.

4. If you need to dial any numbers before dialing the desired phone number, select the Use Prefix check box then type the necessary numbers in the Use Prefix text box. If no numbers must precede the phone number, skip this step.

   The numbers you include in the Use Prefix text box can be any number that must precede the area code and phone number you want to dial. Typically such numbers

are another country's access code or an access line. (Dialing 9 before you can dial out is an example of using an access line.)

5. In the Telephone Number text box type the area code and phone number you want to use when connecting to the selected interface.

6. If you need to enter additional numbers after dialing the phone number, select the Use Suffix check box. Then type the additional numbers in the Use Suffix text box. If such numbers are not necessary, skip this step.

   For example, you can enter a credit card or calling card number in the Use Suffix text box. You could also use the Suffix text box to enter the numbers you are prompted for by your Internet provider's voice mail.

7. Choose the Connect button.

Verifying Setup

To verify that your SLIP/CSLIP/PPP setup was performed correctly, do the following:

1. Start Windows 95 or Windows 3.1.

2. Start Custom and connect the interface.

3. Verify the IP address and phone number

4. Make sure the COM port is available and not in use by another application (such as Microsoft Windows Terminal) if the connect reports an error immediately.

5. Verify that the Modem and Dial settings are correct if the connect reports an error after communicating with the modem. If you have an external modem, you can use the lights on the modem to help diagnose modem communication problems.

6. Verify that the port settings in Custom are 8 Data Bits, 1 Stop Bit, and None Parity.

7. Use the Log window to determine where errors occur.

8. Use the Ping application to check the domain name server IP address.

9. If you have trouble connecting, try again using a lower baud rate, for example 2400.

Once you do these steps, you should have no problem using any of the NetManage applications. If a particular application fails to work, refer to the Troubleshooting section of the specific application chapter.

Using PAP and CHAP

Your NetManage product supports the following two authentication protocols for PPP:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

The server has to be configured to use PAP or CHAP.

The user login and password defined in Custom are used during the PAP/CHAP process. The user login is stored in the Custom User Name field and the PAP password or the CHAP secret are stored in the Custom Password field. On remote systems that have the three fields (Login, Password, and CHAP Secret), you can normally disable their Password field.

SLIP/CSLIP/PPP Login Scripting

By default an interactive window will pop up to allow you to log into the SLIP/PPP server and start a SLIP/PPP session. You can write a script to automate this process.

You can use Custom or Dialer to create or modify scripts. You can also use preconfigured scripts that are retrieved from the Internet provider when you run Automatic Internet.

Writing Login/Connection Scripts

The scripting language is used to negotiate the initial login to the remote host. The remote host could be a UNIX system, a special SLIP/CSLIP/PPP router like a Telebit NetBlazer, a PC running a NetManage product, or a terminal server that supports the SLIP, CSLIP or PPP protocols.

The scripting language is simply a series of alternating Expect and Send statements. The Expect statements tell the script to wait for a character or a series of characters before it Sends a reply. The Send statements send the information in response to a prompt (the preceding Expect) from the remote host.

Script Example#1

If you define both a SLIP and a PPP interface in the Custom utility, your Script will look something like this:

```
name: $u$r word: $p$r -n $6$c$r -i
```

By default, no script is created which requires the user to do manual logon in the interactive window.

In order to successfully execute a dial-up script, you must know the login sequence, the exact prompts, the order, and the information for which you are prompted.

Script Example #2

If you need to send a username at the Login prompt, the script will look like this:

```
Login: $u$r
```

Login: - is the exact prompt to be expected (**expects are case sensitive**)

$u - will send the login name from the User Name field in Custom

$r - will send a CR (Carriage Return)

Script Example # 3

Sometimes you need to send a Carriage Return (CR) (hit ENTER) to the "wake-up" server, before you can send the username. The script will look like this:

```
-n $r Login: $u$r
```

-n Skip an expect. Anything following this character will be a send. In the above example we are sending a CR represented by the $r character.

Lets take a look at the following script for interface:

```
name: $u$r word: $p$r -n $6$c$r -i
```

After the dial-up is complete and the baud rate is negotiated, the script tells your NetManage product to expect the characters "name:" contained in the initial prompt from the remote host. After the prompt is received the program will send the userID (the $u parameter) and a Carriage Return ($r).

Your NetManage product next expects the password prompt "word:". Even though the actual prompt says "password:", you only need to put in the last few characters of any prompt to create an "expect" string. After the prompt is seen by the script, the script will send the value contained in the login Password field in Custom and a CR (pr).

Then the script waits for a 6 second delay ($6), sends the command to start SLIP, CSLIP or PPP (represented by $c which sends the value specified in the Startup Command field of CUSTOM application LOGIN menu), after skipping an expect with the (-n) parameter. The script reads -n 6c$r immediately after the password is sent.

The (-i) option at the end of the script, tells the system to expect an IP address (an IP address displayed in text by the remote SLIP host). The (-i) is not used for PPP. PPP negotiates the addresses automatically.

Script Example #4

Suppose the remote device that the user is dialing into has a (login:) prompt instead of the (name:), and no SLIP command. The script will look like this:

```
login: $u$r word: $p$r
```

A user can specify all of the send commands right in the script.

For example, we have a userID: Joe and the password: Chameleon ATX

The script will look like this:

```
login: Joe$r word: ChameleonATX$r
```

Note: Use the $s option, if you want to create a send string with spaces.

If the user is sending the parameters directly in the script file, the user *must* specify something in the Username field under the Custom login menu. If the Username field is blank, the script will not be sent.

Modifying Existing Scripts

If you choose to modify the scripts provided, update the SLIP file using the following scripting language syntax:

```
<expect1><send1><expect2>...
```

Words are separated by white space, that is, spaces or tabs. Within a <send> string you can include the following escapes:

Escape	Description
$n	send a new line
$r	send a carriage-return
$s	send a space
$b	cause a short "break" on the line
$t	send a tab
$1 - $9	pause the indicated number of seconds
$xXX	send the character with ASCII Decimal code XX
$u	send the user id
$p	send the password
$c	send the Startup Command
$d	send the phone number
$$	send a "$" character
$f	define a prompt
$g	define an encrypted prompt
$l	call-back feature
$-	skip a send

Within an <expect> string you can include the following escapes:

Escape	Description
--	expect "-"
-n	skip an expect
-i	expect IP address (to replace your own)

Prompting Users for Information

By using the $f prompt or $1 prompt, you can prompt users for information. Separate discussions on using each prompt follow.

Defining Prompts with the $f Prompt

Use the $f prompt to define a prompt (caption title) that you want to appear on your login message box. Normally, you would want to use $f when using a secure ID and you have to manually respond to a security prompt.

For example, in the following SLIP0 script, the user is prompted to enter his or her password at connect time. This is because the $f<prompt> is defined as Password.

```
login:  $u$r word:  $fPassword$r
```

When $f is encountered, a dialog box appears with an edit field whose label is the Prompt (in this case Password). In this example, the user is prompted to enter his or her password at connect time.

$f Prompt Example

```
login: $fEnter_Login$r
```

This script prompts you, by displaying a dialog box in Windows, to enter a login name. The text Enter_Login specifies the name of the dialog box that appears when the script encounters the $f parameter.

In the script, after the login prompt is received the dialog box named Enter_Login appears on the screen. Type in the username and choose the OK button.

Defining Prompts with the $l Prompt

To use the $l prompt, the SLIP or PPP server must be configured for a call-back account. In the following example, the user first makes a typical SLIP connection. The $l prompt will cause Custom to close the connection and put the modem in call-back mode, anticipating a call from the server

Note: You can place the $l prompt anywhere in the script.

```
[SLIP1]
login: $u$r word: $p$r $l
```

Expecting an IP Address in SLIP

When you are expecting an IP address in SLIP, in some cases the remote server can return a message such as:

```
My IP address is xxx.xxx.xxx.xxx  Your IP address is xxx.xxx.xxx.xxx
```

If you are using the -i option and expecting an IP address to be assigned by the server, using the -i by itself will not work. The IP address captured by the -i option will be the first IP address found on this line, which is the IP address of the server. In this case, you must put an expect on the first IP address and use the $- option to skip all the data until the next IP address is located.

For example, the system returns the following message:

```
My IP address is 156.27.1.1  Your IP address is 156.27.1.155
```

Using the above example, the script might look something like this:

```
name: $u$r word:  $p$r -n $6$c$r 27.1.1 $- -i
```

In the above example, we are using 27.1.1 to expect the first address, then the $- option is used to skip to the next IP address value on the same line.

Example Script Entry

The following pre-configured script is set up for use with PSInet, and the corresponding interface defined in PSINET.CFG:

```
name: $u$r word: $p$r -n $6$c$r -i
```

Which translates to:

Expect: name: (end of username:)

Send: user id and a carriage-return

Expect: word: (end of password:)

Send: password and a carriage-return

(skip an expect)

(wait for 6 seconds)

Send: the command line and a carriage-return

(wait for an IP address, in the form of a.b.c.d)

Dial-up Login (Internet Service Providers)

There are many companies that offer an Internet connectivity solution, and each solution provides a different login procedure. NetManage has an easy solution that offers dial-up scripting capabilities, thus allowing you to write a simple script that automates the login procedure. Before connecting to an Internet Service Provider you must have access to the following information:

- Type of connection (SLIP/CSLIP/PPP)
- Phone number
- Username and password
- Local IP address (if not dynamically assigned)
- Default Gateway IP address (IP address of the provider)
- IP address for Domain Name Server (optional)
- Mail Gateway, Mail Server and POP Server IP addresses (if Mail application will be used) (optional)

After you have obtained the above information and added it to the Custom application, you will be able to dial out.

When configuring the PORT settings in Custom you must use:

- Data Bits (other bit settings not supported currently)
- Stop Bit
- Parity None

Note: You must fill in the User Name field, located in the Login tab, in order execute the dial-up script. If you are only required to send a PASSWORD, you must have a dummy entry in the User Name field.

Multiple SLIP/CSLIP/PPP Interfaces

If you want to have more than one SLIP, CSLIP, or PPP interface, add the interfaces through Custom as discussed in the Customizing Your Setup chapter.

For example, when you add SLIP interfaces they will automatically be named as SLIP0, SLIP1, SLIP2, SLIP 3, SLIP4 and so on. However, you can change the default names and specify the IP numbers and domain names.

Chapter 6. Using Routing

This section discusses how to configure your system for routers if you are using the NEWT TCP/IP stack.

Routers are used to interconnect subnets. This permits the breakup of large networks into smaller workgroup networks with transparent connections between these workgroups. Each individual system need only specify a default gateway for routing network traffic to unknown subnets. Each router knows about the overall network in order to make intelligent decisions about how to route individual packets.

Your NetManage product supports routing between multiple networks through the use of static route entries. This is a perfect solution for moderate routing needs, where a dedicated router is not available. An example is someone in the field dialing in with SLIP and being rerouted to the Ethernet.

The Custom application can be used to define multiple network interfaces of any type. Routing is performed automatically between these networks. To perform routing to additional networks that are not directly connected to the router, static route entries must be defined. Each entry must consist of the subnet that you want to route to, and the next router in the transmission sequence.

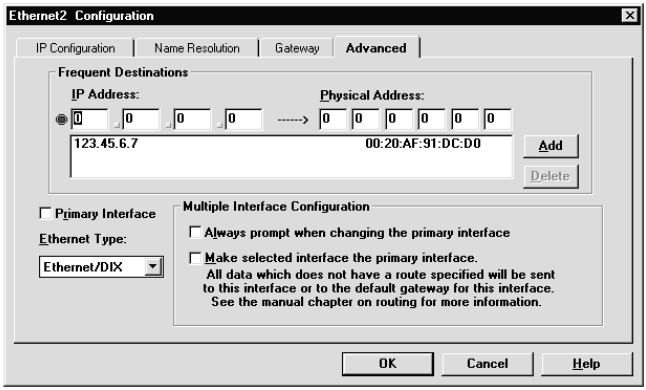
Note: Systems with multiple interfaces do not use a defined default gateway when routing between network interfaces. Only directly connected interfaces and any defined route entries are consulted when routing packets.

Using Multiple Interfaces

Your NetManage product provides sophisticated support for multiple interfaces built into the TCP/IP protocol stack. Configuration for this support is done through the Custom application.

Within Custom you define multiple interfaces by adding an interface and specifying the interface type, its default gateway, and its DNS. Once you have configured the various LAN and dialup interfaces you can control their operation by the following:

1. In Custom, select the Advanced tab in the Configuration dialog box.



2. Select or clear the Always prompt user when changing the primary interface check box.

   Select this check box if you want to be prompted each time you select an interface. The prompt will ask you to confirm whether you want the selected interface to be the new primary interface. If you do not want the prompt to appear, clear this check box.

   If you select this check box, Custom displays a dialog box that shows you what all the parameter values for the current primary interface are and what they will change to if you change the primary interface.

   For example, suppose you have multiple LAN interfaces each with its own default gateway defined. Most of the time when you change primary interfaces you want the default gateway for that interface to be used. However there might be a few occasions where you want the default gateway on the first interface to continue to be used even when the second interface was last selected. By selecting this option you will be warned each time the primary interface is about to be changed so that you can decide if you want to make the change.

3. Select or clear the Make selected interface the primary interface check box.

   If you select this check box, the protocol stack will check whenever data needs to be sent out to see if the data is destined for one of the active interfaces. If the packet is not destined for an active interface, then the packet will be sent to the default gateway of the currently selected interface which is also the primary interface. The selected interface is the one that is currently highlighted.

   For example, suppose you have a PC with both a LAN and dial-up connection where the LAN connection has a default gateway defined for it and the dial-up connection is connected to the Internet. Both interfaces have a DNS defined for them. If you were to use Ping to verify a site on the Internet, NEWT would need to decide which DNS to use to resolve the name of the host you are verifying. If you select the Make selected interface the primary interface check box, NEWT uses the DNS for the selected/primary interface.

If you clear this check box, NEWT uses the information specified for the current active interface.

4. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

For details on the other options available on the Advanced tab, see the Customizing Your Setup chapter.

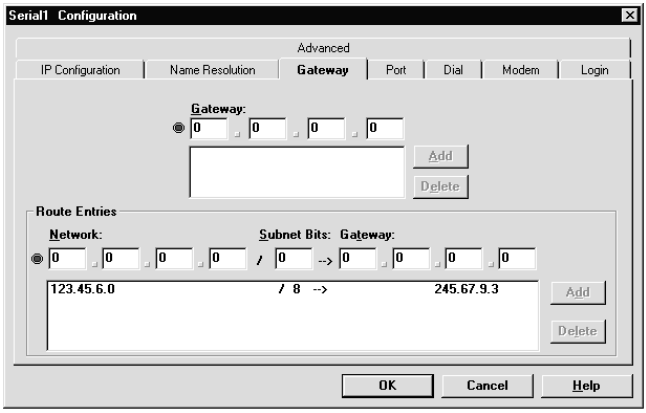
Router Setup

Installation of additional interfaces in the Custom application is performed in the same manner as described in the Installation and Setup chapter. Once these interfaces are defined and it is verified that they are installed correctly, route entries must be defined for each accessible network that is not a local interface.

Note: Routing between locally defined interfaces is automatic: no route entries are required.

To route each entry specified from within the Custom or Dialer application, do the following:

1. In Custom, select the Gateway tab in the Configuration dialog box.



2. Type the network address in the Network text boxes and the subnet bits in the Subnet text box. Then type the IP address of the gateway router that should receive packets sent to the specified network.

   Note: The network address must be fully specified, up to the host portion of the address. The network address must end with a zero (0). For example, a

class B address with eight subnet bits must be specified as X.X.X.0 (for example, 137.27.4.0).

The gateway must be on the locally connected subnet interface. (For SLIP interfaces, specification of a gateway is not needed.)

3. Choose the Add button.

4. If you want to add additional routers, repeat steps 2 and 3. You can enter up to five routes per interface.

5. Do one of the following:

   - Select another tab if you want to continue customizing your setup.
   - Choose the OK button to close the Configuration dialog box. Then save your settings by choosing the Save command from the File menu.

Verifying Setup

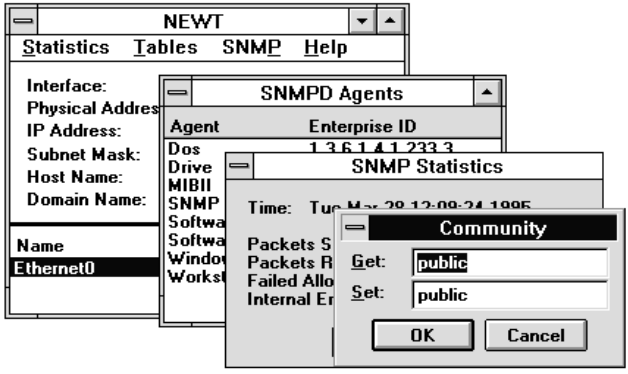
To verify that your router setup was performed correctly, do the following:

- ❑ Use the Ping application from a system on one of the networks to ping the local side of the router. If this fails, refer to the Verifying Installation and Setup section in the Installation and Setup chapter.
- ❑ Use the Ping application to ping another interface of the router. A failure usually indicates improper setting of the default gateway or subnet mask. Ensure that the default gateway specifies the IP address of this router.
- ❑ Use the Ping application to ping through the router to another network. A failure can indicate a route entry error on the router. It is also possible that the remote host does not know how to respond properly. Make sure the network destination and subnet are properly set up for this router. You can use the NEWT application to verify route entries by selecting Route from the Tables menu to display all defined routes.

Chapter 7. NEWT and SNMP

When you use NEWT, an icon representing the NEWT TCP/IP kernel appears on the screen. The NEWT application permits you to view information about the current network interfaces. The NEWT application must be running for network connectivity to be enabled. It cannot be terminated explicitly, but exits automatically when the last NEWT application exits. NEWT provides information through a set of dialog boxes which you can display by choosing the NEWT icon.

Note: You can minimize the NEWT application with many open dialog boxes and it will minimize all the dialog boxes as well. When the NEWT application is restored, all dialog boxes reappear as they were prior to being minimized.



Network Statistics

The Statistics menu consists of selections for all network protocol layers (Interface, ARP, IP, ICMP, UDP, TCP and SNMP). The following tables describes the type of statistics each protocol level displays.

Protocol	Types of Statistics
Interface	Ethernet board statistics
ARP	Address lookup statistics
IP	IP address statistics
ICMP	IP management protocol statistics
UDP	Datagram statistics

Protocol	Types of Statistics
TCP	Connection oriented statistics
SNMP	Network Management protocol statistics

The Interface statistics are displayed for the currently selected interface. Double-clicking on a particular interface entry also displays the Interface statistics dialog box.

Each menu selection displays a dialog box with statistic values for that protocol. Each of these dialog boxes can be set to update values every second, by pressing the Start button. Further updates can be prevented by pressing the Stop button (which appears after you have pressed the Start button). The Reset button can be used at any time to reset the statistics values to zero for that window.

Network Tables

The Tables menu consists of selections for all network protocol tables (ARP, route, socket, Gateway and DNS, and SNMP).

- The ARP table displays the current mapping of IP addresses to physical addresses and any defined Frequent Destinations.
- The Route table displays the current set of route entries corresponding to all local interfaces, static route entries, and the default gateway, if specified.
- The Socket table displays the currently open sockets, as well as their connections and states. There is always at least one socket entry used by the NEWT application.
- The Gateway and DNS table provides a view of the current default gateway, as well as the DNS (Domain Name Server) IP addresses. The default gateway specifies the machine that will accept and route packets destined for other networks. The IP address of a DNS and up to two alternatives may be specified.
- The SNMP table provides a view of currently active agents with their corresponding Enterprise ID. The Enterprise ID is a unique identification number given by the Internet registration to organizations who request an ID for purposes of defining SNMP MIBs. This is done to ensure the uniqueness of all managed objects for SNMP. NetManage's Enterprise ID is 233.

Using the SNMP Protocol

SNMP is the Simple Network Management Protocol that allows TCP/IP Managers to manage Agents over the network.

NEWT offers an extensible SNMP agents that greatly extend the capabilities of SNMP-based management applications. SNMP is a standard feature of NEWT and requires no additional base memory space.

Several SNMP agents are provided with NEWT. The main MIB agent (Management Information Base) is known as MIB-II, which is the industry standard for managing the TCP/IP protocol suite. In addition, NEWT includes an enterprise MIB for managing Windows desktops. For example, this NetManage MIB can provide information about DOS and Windows versions or about software currently running on the workstation. Additional agents written by NetManage or other developers can be registered with SNMPD and easily become part of your managed PC.

Setting UP SNMP

When you use the SNMP for the first time, you need to enter the following:

- Host administration information
- Trap information
- Community setting information

This information will be available to management systems that support MIB-II.

Host Administration Information

In order to personalize your workstation, you need to enter information that describes it. This information is part of the "system" group of MIB-II, and includes the following:

- your name
- administrative contact regarding this workstation
- location where the workstation resides

To enter the host administration information, do the following:

1. Choose the NEWT icon.
2. Choose the Host Administration... command from the SNMP menu..
3. Enter your name, the name of an administrative contact for this workstation, and the location where the workstation resides.

4. If desired, select the Generate Traps option, and choose the OK button.

Trusted Managers Information

The Trusted Managers option allows you to assign special permissions to an SNMP manager. Special permissions include, for example: the ability to launch applications.

1. Choose the NEWT icon.
2. Choose the Trusted Managers... command from the SNMP menu.
3. Enter the node IP address or name from the list of SNMP managers provided in the field.

4. Choose the OK button.

Trap Administration Information

The trap administration option allows you to determine which destinations receive notification from an SNMP agent. To enter trap administration information, do the following:

1. Choose the NEWT icon.
2. Choose the Trap Administration... command from the SNMP menu.
3. Enter the default destination to where SNMP agent notification will be sent.

4. If desired, select additional preferences and choose the OK button.

Community Information

The Community... option allows you to enter the community string you want to apply to the Get and Set receipt operations. When you do not enter community field information, the community is not checked and any message is accepted. To enter Community information, do the following:

1. Choose the NEWT icon.
2. Choose the Community... command from the SNMP menu.
3. Enter the string you want to apply in the Get and Set fields.

   Many systems use a community of "public" for Get and "private" for Set. Note that the text you enter in each field is case sensitive and your selections are saved *encrypted* in the configuration file.
4. Choose the OK button.

This personalized information is now included in the administration portion of the MIB-II in your agent.

Chapter 8. NEWTToolbar

NEWTToolbar maintains a list of applications that you can start without having to switch to a window. You can make additions, modifications, and deletions to NEWTToolbar's list of applications.

Starting NEWTToolbar

When you install ChameleonNFS ATX, NEWTToolbar is automatically added to your Startup group and the Desktop Management group. If you do not want NEWTToolbar to be started each time you start Windows NT, Windows 95, or Windows 3.1, remove the NEWTToolbar icon from your Startup group. You can then start NEWTToolbar by choosing it from the Desktop Management group.

Note: The NEWTToolbar application is automatically placed in the group called Startup. If you are running non-English Windows, your system has a startup group with a different name that automatically launches applications. Therefore, you need to copy the NEWTToolbar application from the group called Startup to the group in your system that automatically launches applications.

After NEWTToolbar is started, the toolbar appears. The toolbar includes a button for each application that is on the NEWTToolbar application's list. By default, NEWTToolbar includes buttons for the following applications:

- Go IntraNet!
- ZMail Pro
- Forum
- WebSurfer
- WebSpider
- Telnet

For details on an application included in the NEWTToolbar, see your user's guide.

Main Menu

To open the main menu, use the right mouse button to click on either the NEWTToolbar clock or on the outside of any toolbar button.

Note: Be sure to click on the outside of a button and not directly on a button. Otherwise, you will open the button menu.

The main menu includes the following commands:

Main Menu commands	Description
Add Toolbar Buttons...	Lets you add an application to the NEWTToolbar list. For details, see the Adding Applications to NEWTToolbar section.
Docking	Controls where you can move the NEWTToolbar window. If this command is disabled, you can move the window anywhere. If this command is enabled, you can move the window only to the top, bottom, left side, right side, or a corner of the screen.
Fit to Screen	Fits the toolbar to the size of your computer screen and fits the toolbar buttons to the size of the NEWTToolbar window. This command is useful if some buttons are not currently displayed.
Always on Top	Lets you control whether the toolbar is always on top of other applications. Select this option if you frequently use Go IntraNet! When you select text to shoot to ZMail Pro or WebSurfer, you must select the desired text first, and then immediately choose the Go IntraNet! button and drag your cursor to the desired menu option.
Display Icon Only	Lets you control whether toolbar buttons include only an application's icon or the application's name and icon.
About NEWTToolbar...	Displays information about the NEWTToolbar application. Choose the Copy button to copy version information to the clipboard. You can then paste this information into any application. Choose the OK button to continue.
Close NEWTToolbar	Exits the NEWTToolbar application

If you enable the Docking, Fit to Screen, Always on Top, or Display Icon Only command, a check mark appears next to the command's name.

Button Menu

To open the button menu, use the right mouse button to click on any toolbar button.

Note: Be sure to click directly on a button and not on the outside of a button. Otherwise, you will open the main menu.

The button menu includes the following commands:

Button Menu Command	Description
Remove Toolbar Button	Removes the application and its associated button from the NEWTToolbar application's list. **Note:** You cannot remove the Go IntraNet! button.
Modify Toolbar Button...	Lets you modify the application's button name and command line information. For details, see the Modifying Toolbar Buttons section.

Adding Applications to NEWTToolbar

Add an application to NEWTToolbar if you want to be able to start that application from NEWTToolbar. To add an application, do the following:

1. Use the right mouse button to click on either the NEWTToolbar clock or on the outside of a toolbar button. The main menu appears.
2. Choose the Add Toolbar Button... command from the main menu.
3. In the dialog box that appears, type the name you want to use for the application you are adding. This name will appear on the toolbar button if the Icons Only command is not enabled.
4. In the command line text box, enter the pathname for the .EXE file of the application you want to add. If necessary, choose the Browse button to help you locate the desired file.
5. If you want to include any command line options for the application, type those options in the command line text box.

   For example, suppose you do not want the ZMail Pro splash screen (large ZMail Pro box with copyright information) to appear each time you start ZMail Pro from within NEWTToolbar. You can bypass this screen by entering the following in the command line text box:

   ```
   C:\NETMANAG\MAIL.EXE -nologo
   ```
6. Choose the Add button.

Modifying NEWTToolbar Buttons

To change a toolbar button's name or command line information, do the following:

1. Use the right mouse button to click on any toolbar button. The Button menu appears.

2. Choose the Modify Toolbar Button... command from the button menu.

3. Edit the dialog box as desired.

   For details on entering information in the command line text box, see the Adding Applications to NEWTToolbar section.

4. Choose the OK button.

Starting an Application in NEWTToolbar

To start an application in NEWTToolbar, use the left mouse button to click on the button of the application you want to start.

Note: Be sure to click with the left mouse button. Otherwise, you will open the button menu. If you try to start an application that is already running, that application's window becomes the active window.

Exiting NEWTToolbar

To exit NEWTToolbar, use the right mouse button to click on either the NEWTToolbar clock or on the outside of a toolbar button. Choose the Close NEWTToolbar command from the main menu.

Any changes made in NEWTToolbar are saved to the NEWTToolbar application's configuration file.

Chapter 9. Ping - Network Testing

The Ping application is a network diagnostic tool used to verify connectivity to a particular system on your network. The Ping application transmits any number of echo requests to a particular system and displays the results for each echo reply. This exchange is referred to as pinging. These echo requests and replies are supported by all systems on the network, including those that are currently running one or more NetManage applications. This is accomplished through the use of the Internet Control Message Protocol (ICMP). If you encounter a problem in an application, pinging determines if the problem is with the application or due to a non-responding host. You may have multiple instances of the Ping application active simultaneously.

The current options and host name can be saved to a configuration file named PING.CFG (default). The configuration file is loaded when the Ping application is started. If a host name or IP address is specified, the Ping application immediately begins pinging that host. You can also supply a command line option to specify the host name or IP address.

Ping Host

To ping another system, do the following:

1. Select Start. The Host dialog box appears.
2. Type or select a host name or IP address in the Host dialog box.
3. Choose the OK button. The application sends an echo request and waits for the echo reply. If no reply is received within the timeout value (default is 6 seconds), the ping fails.

A single ping produces summary lines in the Ping window. Multiple iterations or continuous pinging produces a single summary line for each ping. After each ping, summary lines are generated, giving the total statistics for this sequence of pings.

Note: When minimized, an animated icon of a ping-pong ball indicates active pinging. The ball moving back and forth indicates successful pings.

Ping Settings

The Ping Settings menu lets you access the Preferences dialog box and the Auto Start option.

The Preferences dialog box contains the following options:

Iteration: Specify the number of echo requests to transmit (1 through 9999 seconds); for an unlimited number of iterations, select Continuous.

Data Length: Specify the length of each echo request (0 through 1,400 bytes). The default is 64 bytes.

Interval: Specify the time the application waits for a response to the ICMP_ECHO request sent (1 through 999 seconds). If there is no response after the specified time the ping returns "0 bytes received".

Timeout: Specify the timeout value for the echo reply (1 through 999 seconds).

To automatically start Ping through your Windows application, do the following:

1. Choose the Auto Start command from the Settings menu.
2. Choose Run from the Start menu and type the following command line:
   `ping<system name>`

Additional Online Information

The online help file for Ping includes a description of each menu command.

Troubleshooting

If you experience difficulties using the Ping application, refer to the following items:

- ❏ Try to Ping by using the IP address (instead of host name) to determine if there is a name resolving problem.
- ❏ The network portion of the IP address must be a locally connected interface, or a default gateway must have been specified to route unknown networks.
- ❏ A local host table or domain server must be specified when pinging by host name. The host name entry must specify the correct IP address.
- ❏ For a Windows system, the NetManage application must be running for it to respond to an echo request.
- ❏ Make sure that the Ethernet type is correct: it should be Ethernet/DIX in almost all cases.
- ❏ Verify that there is a valid Frequent Destinations entry for this IP address.

Appendix A. Windows for Workgroups

Note: This appendix is intended only for users who are:

- installing NEWT to run in a Windows for Workgroups environment.
- installing NEWT on Windows for Workgroups replacing a Microsoft Stack with NetManage stack..
- using OEM Setup for Windows for Workgroups.

Installing Windows for Workgroups

Generally, the Install application makes all the necessary changes to your configuration. However, if you are upgrading from NEWT 3.11 or earlier, you may refer to this section for additional information. (You may also refer to this section to see a list of changes that have been made automatically to your configuration.)

The section includes separate headings, describing how NEWT is configured to coexist with each of the following:

- Windows for Workgroups version 3.11 over NDIS
- Windows for Workgroups version 3.11 over NDIS with no workgroups networking installed.
- Windows for Workgroups version 3.11 and Novell version 3.X shell/ODI or later.
- Windows for Workgroups version 3.11 and Novell version 3.X shell/ODI or later, with no workgroups networking installed.

Prerequisites

Before installing NEWT make sure that Windows for Workgroups is configured properly and all functions are operational. It is recommended that you upgrade to Windows for Workgroups version 3.11 from 3.10 or Windows 3.1 to have a successful install.

Over NDIS

This section describes configuring NEWT version 4.6 or later to coexist with Windows for Workgroups version 3.11 over NDIS.

Follow these steps:

1. Install Windows for Workgroups, version 3.11.
2. Install NEWT according to the installation instructions below:

NEWT Installation Instructions

Your NEWT product includes several diskettes.

New Installation

To install the product for the first time, start Windows in enhanced mode:

1. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.
2. Continue to insert the remaining diskettes when prompted.

   At this point, Setup will start Custom. The Custom application guides you through a customized configuration portion of your installation with a short series of dialog boxes, prompting you to make selections.

   Note that you will not be prompted for setting domain servers and entries for Host Table. You must manually define these names for name resolving.
3. Select the Save option from the File menu and exit the Custom application.
4. At the prompt, remove all diskettes and choose the OK button to reboot.

Upgrade Installation

To upgrade from a previous NetManage installation, start Windows in enhanced mode:

1. Quit all NEWT applications and any other TCP/IP applications.
2. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.
3. Continue to insert the remaining diskettes when prompted.
4. At the prompt, remove all diskettes and choose the OK button to reboot.

The following files will be modified:

- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI

- PROTOCOL.INI

Verifying the Changed Files

The automated Install program generally makes all the necessary modifications. If you experience any problems with these modifications, check these files as follows:

File Name: AUTOEXEC.BAT

Modifications: Adds NETMANAG to Path.

Example:

```
C:\WINDOWS\SMARTDRV.EXE
C:\WINDOWS\net start
PATH C:\NETMANAG;C:\WINDOWS;dos
SET TEMP=C:\WINDOWS\TEMP
```

Note: If a NETBIND statement exists from a previous installation of NetManage, you must remove it. The NETBIND functionality is performed by the NET START command provided by Windows for Workgroups.

File Name: CONFIG.SYS

Modifications: None

Notes:

- Do not load the IFSHLP.SYS file into high memory.
- There should not be a NETMANAGE.DOC device driver in CONFIG.SYS. Many of the drivers that were loaded from CONFIG.SYS previously, are now loading from the SYSTEM.INI file. See the example of the SYSTEM.INI file.

File Name: WIN.INI

Modifications: Adds [TCPIP] section

Example:

```
[TCPIP]
ID=XXX... (your encrypted serial number)
FILE=C:\NETMANAG\TCPIP.CFG
.
.
.
```

Note: You should create a pasted backup of the [TCPIP] section for future possible troubleshooting.

File Name: SYSTEM.INI

Modifications:

- changes [network drivers] section
- changes LoadRMdrivers value from No to Yes

Example:

The following line will be added to the [386Enh] section:

```
.
.
.
[386Enh]
;BEGIN NetManage Modification.
device=c:\netmanag\nmtcpip.386
;END NetManage Modification.
.
.
.
```

In the [network drivers] section, the netmanag.dos driver is added to the transport line:

```
[network drivers]
netcard=elnk3.dos
transport=ndishlp.sys,c:\netmanag\netmanag.dos,*netbeui
```

Install changes the value for LoadRMDrivers line from No to Yes.

```
devdir=C:\WINDOWS
LoadRMDrivers=Yes
```

File Name: **PROTOCOL.INI**

Modifications: Adds [netmanag] section

Example:

```
[network.setup]
version=0x3110
netcard=ms$elnk3,1,MS$ELNK3,3
transport=ms$nwlinknb,NWLINK
transport=ms$ndishlp,MS$NDISHLP
transport=ms$netbeui,NETBEUI
lana0=ms$elnk3,1,ms$nwlinknb
lana1=ms$elnk3,1,ms$ndishlp
lana2=ms$elnk3,1,ms$netbeui

[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP

[NETMANAGE]
DRIVERNAME=netmng$
```

```
BINDINGS=MS$ELNK3   <=== Inserted during Netmanage install

[MS$ELNK3]                          <=== network card section
DriverName=ELNK3$

[ELNK3]
Adapters=MS$ELNK3

[NWLINK]
BINDINGS=MS$ELNK3

[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=MS$ELNK3

[NETBEUI]
DriverName=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=MS$ELNK3
LANABASE=1
```

Over NDIS with No Workgroups Networking Installed

This section describes configuring NEWT version 4.6 or later to coexist with Windows for Workgroups version 3.11 over NDIS with no Workgroups Networking installed.

Follow these steps:

1. Install Windows for Workgroups, version 3.11.
2. Install NEWT according to the installation instructions below:

NEWT Installation Instructions

Your NEWT product includes several diskettes.

New Installation

To install the product for the first time, start Windows in enhanced mode:

1. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.
2. Continue to insert the remaining diskettes when prompted.

   At this point, Setup will start Custom. The Custom application guides you through a customized configuration portion of your installation with a short series of dialog boxes, prompting you to make selections.

Note that you will not be prompted for setting domain servers and entries for Host Table. You must manually define these names for name resolving.

3. Select the Save option from the File menu and exit the Custom application.

4. At the prompt, remove all diskettes and choose the OK button to reboot.

Upgrade Installation

To upgrade from a previous NetManage installation, start Windows in enhanced mode:

1. Quit all NEWT applications and any other TCP/IP applications.

2. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.

3. Continue to insert remaining diskettes when prompted.

4. At the prompt, remove all diskettes and choose the OK button to reboot.

Verifying the Changed Files

The automated Install program generally makes all the necessary modifications. If you experience any problems with these modifications, check these files as follows:

- AUTOEXEC.BAT
- CONFIG.SYS
- WIN.INI
- SYSTEM.INI
- PROTOCOL.INI

File Name: AUTOEXEC.BAT

Modifications: Adds a line for NETBIND and adds NetManag to Path line.

Example:

```
C:\NETMANAG\NETBIND
C:\WINDOWS\SMARTDRV.EXE
PATH C:\NETMANAG;C:\WINDOWS;C:\Dos
SET TEMP=C:\WINDOWS\TEMP
```

File Name: CONFIG.SYS

Modifications: Adds NDIS driver

Example:

```
FILES=30
BUFFERS=30
```

```
LASTDRIVE=Z
DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
DEVICE=C:\WINDOWS\IFSHLP.SYS
STACKS=9,256
DEVICE=C:\NETMANAG\PROTMAN.DOS /I:C:\NETMANAG
DEVICE=C:\NETMANAG\ELKNII.DOS
DEVICE=C:\NETMANAG\NETMANAG.DOS
```

File Name: WIN.INI

Modifications: Adds [TCPIP] section

Example:

```
[TCPIP]
FILE=C:\NETMANAG\TCPIP.CFG
 .
 .
 .
```

Note: You should make a pasted backup of the [TCPIP] section for future possible troubleshooting.

File Name: SYSTEM.INI

Modifications: adds nmtcpip.386 in [386Enh] section

Example

The following lines will be added to the [386Enh] section:

```
 [386Enh]
;BEGIN NetManage Modification.
device=C:\netmanag\nmtcpip.386
;END NetManage Modification
.
.
```

File Name: **PROTOCOL.INI**

Modifications: Adds [NETMANAG] section

```
[EtherLink3]
DRIVERNAME=ELNK3
 [NETMANAGE]
DRIVERNAME=netmng$
BINDINGS=EtherLink3
```

With Novell and Workgroups Networking

This section describes configuring NEWT version 4.6 or later to coexist with Windows for Workgroups version 3.11 and Novell 3.X or later running in the ODI environment.

Prerequisites

Before installing NEWT make sure that Windows for Workgroups is configured to run with Novell over ODI and all of the Novell and Windows for Workgroups functions are working properly. In particular, make sure Novell's latest version of LSL.COM is loaded.

Note: We highly recommend installing the Novell network over ODI before installing the Windows for Workgroups.

Once the two networks, Microsoft Windows Network 3.11 and Novell NetWare (shell) are functioning properly over ODI, you can install NEWT. The new version of NEWT (4.6) will automatically detect the ODI and Windows For Workgroups environments and will make the necessary changes.

Follow these steps:

1. Install Windows for Workgroups, version 3.11.
2. Install NEWT according to the installation instructions below:

NEWT Installation Instructions

Your NEWT product includes several diskettes.

New Installation

To install the product for the first time, start Windows in enhanced mode:

1. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.
2. Continue to insert the remaining diskettes when prompted.

   At this point, Setup will start Custom. The Custom application guides you through a customized configuration portion of your installation with a short series of dialog boxes, prompting you to make selections.

   Note that you will not be prompted for setting domain servers and entries for Host Table. You must manually define these names for name resolving.
3. Select the Save option from the File menu and exit the Custom application.
4. At the prompt, remove all diskettes and choose the OK button to reboot.

Upgrade Installation

To upgrade from a previous NetManage installation, start Windows in enhanced mode:

Note: Make sure that you do not have PROTMAN.DOS and NETMANAG.DOS drivers loaded in CONFIG.SYS. In addition, NETBIND and ODINSUP should be removed from the AUTOEXEC.BAT file.

Note: Be sure to configure Windows for Workgroups for ODI before continuing.

1. Quit all NEWT applications and any other TCP/IP applications.
2. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.
3. Continue to insert the remaining diskettes when prompted.
4. At the prompt, remove all diskettes and choose the OK button to reboot.

The following files will be modified:

- NET.CFG
- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI
- PROTOCOL.INI

Verifying the Changed Files

The automated Install program makes all the necessary modifications. If you experience any problems with these modifications, check these files as follows:

The following NET.CFG file was created by Windows for Workgroups when configured to support Novell NetWare. The NEWT added more settings to this file. The order of Frame and Protocol statements is important.

Please refer to the Ethernet and IBM Token Ring examples below.

NET.CFG

```
#Ethernet Adapter
Link Driver 3C509
     Frame Ethernet_802.3
     Frame Ethernet_802.2
     Frame Ethernet_SNAP
     Frame Ethernet_II
     Protocol RARP 8035 ethernet_ii
     Protocol ARP 806 ethernet_ii
     Protocol IP 800 ethernet_ii
#IBM Token Ring Adapter
Link Driver TOKEN
Frame TOKEN-RING
```

```
Frame TOKEN-RING_SNAP
Protocol IPX E0     TOKEN-RING
Protocol IP  800    TOKEN-RING_SNAP
Protocol ARP 806    TOKEN-RING_SNAP
Protocol RARP       8035   TOKEN-RING_SNAP
```

The installation of NEWT will add the NMODI driver to the AUTOEXEC.BAT file. This driver allows NEWT to run on top of ODI.

File Name: AUTOEXEC.BAT

Modifications: Install makes the following changes to this file:

- Adds nmodi
- Adds netmanag to Path

Note: The Windows for Workgroups configuration should include the ODIHLP.EXE driver in this file. While you are verifying the file, check also for the ODI driver.

Example:

```
C:\WINDOWS\net start
@ECHO OFF
PATH C:\NETMANAG;C:\WINDOWS;C:\DOS;C:\ODI
PROMPT=$p$g
c:\odi\lsl
c:\odi\3c509         <=== The ODI driver for your
             Network Interface Card
c:\odi\ipxodi
c:\netmanag\nmodi           <=== Added by the Install
                   program
C:\WINDOWS\odihlp.exe
c:\odi\netx
File Name:  CONFIG.SYS
Modifications:  None
Example:
FILES=30
BUFFERS=30
LASTDRIVE=Z
DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
DEVICE=C:\WINDOWS\IFSHLP.SYS
STACKS=9,256
```

File Name: WIN.INI

Modifications: Adds [TCPIP] section

Example:

```
[TCPIP]
ID=XXX... (your encrypted serial number)
FILE=C:\NETMANAG\TCPIP.CFG
 .
 .
 .
```

Note: You should make a pasted backup of the [TCPIP] section for future possible troubleshooting.

Following is a short example of the lines that are modified in the SYSTEM.INI file.

File Name: SYSTEM.INI

Modifications: Adds nmtcpip.386 in [386Enh] section

Example:

The following line will be added to the [386Enh] section:

```
[386Enh]
;BEGIN NetManage Modification.
device=C:\netmanag\nmtcpip.386
;END NetManage Modification.
```

Following is an example of a PROTOCOL.INI file.

Example: PROTOCOL.INI

```
[network.setup]
version=0x3110
netcard=ms$odimac,1,MS$ODIMAC,4
transport=ms$nwlinknb,NWLINK
transport=ms$netbeui,NETBEUI
lana0=ms$odimac,1,ms$netbeui
lana1=ms$odimac,1,ms$nwlinknb

[net.cfg]
PATH=C:\WINDOWS\net.cfg

[MS$ODIMAC]
[Link Driver 3c509]
data=Frame Ethernet_802.3
data=Frame Ethernet_802.2
data=Frame Ethernet_SNAP
data=Frame Ethernet_II
data=Link Driver 3c509

[NWLINK]
BINDINGS=3c509
```

```
[NETBEUI]
BINDINGS=3c509
LANABASE=0
SESSIONS=10
NCBS=12
```

With Novell with No Workgroups Networking Installed

This section describes configuring NEWT version 4.6 to coexist with Windows for Workgroups version 3.11 and Novell 3.X or later running in the ODI environment, with no Workgroups networking installed.

Prerequisites

Before installing NEWT make sure that Windows for Workgroups is configured to run with Novell over ODI.

Note: We highly recommend installing the Novell network over ODI before installing the Windows for Workgroups.

Once Windows for Workgroups and Novell NetWare (shell) are functioning properly over ODI, you can install NEWT. The new version of NEWT will automatically detect the ODI and Windows For Workgroups environments and will make the necessary changes.

Follow these steps:

1. Install Windows for Workgroups, version 3.11.
2. Install NEWT according to the installation instructions below:

NEWT Installation Instructions

Your NEWT product includes several diskettes.

New Installation

To install the product for the first time, start Windows in enhanced mode:

1. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.
2. Continue to insert the remaining diskettes when prompted.

   At this point, Setup will start Custom. The Custom application guides you through a customized configuration portion of your installation with a short series of dialog boxes, prompting you to make selections.

Note that you will not be prompted for setting domain servers and entries for Host Table. You must manually define these names for name resolving.

3. Select the Save option from the File menu and exit the Custom application.

4. At the prompt, remove all diskettes and choose the OK button to reboot.

Upgrade Installation

To upgrade from a previous NetManage installation, start Windows in enhanced mode:

Note: If you have NEWT version 3.11, make sure that you do not have PROTMAN.DOS and NETMANAG.DOS drivers loaded in CONFIG.SYS. In addition, NETBIND and ODINSUP should be removed from the AUTOEXEC.BAT file.

1. Quit all NEWT applications and any other TCP/IP applications.

2. Insert the NEWT diskette in the drive of your choice (a:\ in this example). Select the Run... option under the File menu in Program Manager and type: `a:\setup.` Then choose the OK button.

3. Continue to insert the remaining diskettes when prompted.

4. At the prompt, remove all diskettes and choose the OK button to reboot.

The following files will be modified:

- NET.CFG
- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI

Verifying the Changed Files

The automated Install program generally makes all the necessary modifications. If you experience any problems with these modifications, check these files as follows:

The NEWT installation will add more settings to the NET.CFG file. The order of Frame and Protocol statements is important.

Please refer to the Ethernet and IBM Token Ring examples below.

NET.CFG

```
Filename: #Ethernet Adapter
Link Driver 3C509
     Frame Ethernet_802.3
     Frame Ethernet_802.2
     Frame Ethernet_SNAP
```

```
     Frame Ethernet_II
     Protocol RARP 8035 ethernet_ii
     Protocol ARP 806 ethernet_ii
     Protocol IP 800 ethernet_ii
#IBM Token Ring Adapter
Link Driver TOKEN
Frame TOKEN-RING
Frame TOKEN-RING_SNAP
Protocol IPX E0     TOKEN-RING
Protocol IP  800    TOKEN-RING_SNAP
Protocol ARP 806    TOKEN-RING_SNAP
Protocol RARP       8035   TOKEN-RING_SNAP
```

The installation of NEWT will add the NMODI driver to the AUTOEXEC.BAT file. This driver allows NEWT to run on top of ODI.

File Name: AUTOEXEC.BAT

Modifications:

- Adds nmodi
- Adds netmanag to Path

Example:

```
@ECHO OFF
PATH C:\NETMANAG;C:\WINDOWS;C:\DOS;C:\ODI
PROMPT=$p$g
c:\odi\lsl
c:\odi\3c509         <=== ODI driver for your Network
                    Card
c:\odi\ipxodi
c:\netmanag\nmodi           <=== Added by the Install
                           program
c:\odi\netx
```

File Name: CONFIG.SYS

Modifications: None

File Name: WIN.INI

Modifications: Adds [TCPIP] section

Example:

```
[TCPIP]
ID=XXX... (your encrypted serial number)
FILE=C:\NETMANAG\TCPIP.CFG
 .
 .
 .
```

You should make a pasted backup copy of [TCPIP] for possible future troubleshooting.

Following is a short example of the lines that are modified in the SYSTEM.INI file.

File Name: SYSTEM.INI

Modifications: Adds nmtcpip.386 in [386Enh] section

Example:

The following lines will be added to the [386Enh] section:

```
 [386Enh]
;BEGIN NetManage Modification.
device=C:\netmanag\nmtcpip.386
device=c:\netmanag\nmredir.386
;END NetManage Modification.
```

New Installation Replacing Microsoft Stack with NetManage Stack

If you want to replace the Microsoft stack with NEWT, do the following:

1. Select the Drivers... button to display the Drivers dialog box.
2. Select the Microsoft TCP/IP-32 3.11 option and choose the Remove button.
3. Choose the OK button in the Confirm dialog box. Choose the Close and then the OK buttons.
4. Additional messages appear telling you what files have been modified. Continue to choose the OK buttons until the Windows Setup dialog box appears.
5. Choose the Restart Computer button to reboot your machine.
6. After your machine has been rebooted, restart Windows.
7. Run Setup.

Note: Your SYSTEM.INI and WIN.INI files will automatically be changed by Windows for Workgroups when you remove the Microsoft stack.

OEM Setup for WFW

NetManage provides its own OEM (Original Equipment Manufacturer) support. For example, you may want to recover your original settings in the Network Setup dialog box after you install NEWT.

OEM Setup for NDIS

1. Choose the Network program group and then the Network Setup icon. The Network Setup dialog box appears.
2. Choose the Drivers... button to display the Network Drivers dialog box.
3. Choose the Add Protocol... button to display the Add Network Protocol dialog box.
4. Select the Unlisted or Updated protocol item and choose the OK button. The Install Driver dialog box appears.
5. Select the Browse... button to select the directory where you installed NEWT (default directory is C:\NETMANAG) and choose the OK button to display the Install Driver dialog box.
6. Choose the OK button to display the Unlisted or Updated Protocol dialog box. The NetManage NEWT network now appears on the Drivers list.
7. Choose the Close button. The Network dialog box appears.
8. Choose the OK button. The Network Setup dialog appears and choose the OK button again. Additional messages appear telling you what files have been modified. Continue to choose the OK buttons until the Network Setup dialog box appears.
9. Choose the Restart Computer button to reboot your machine.
10. After your machine has been rebooted, restart Windows.

Note: The network settings in the SYSTEM.INI file are automatically restored to their original settings.

OEM Setup for ODI

1. Choose the Network program group and then the Network Setup icon. The Novell NetWare dialog box appears.
2. Choose IPXODI.COM and LSL.COM (recommended) option and choose the OK button. The Network Setup dialog box appears.
3. Choose the Networks...button to display the Networks dialog box.
4. Select the Other option and scroll to select Unlisted or Updated Network and choose the OK button. The Install Driver dialog box appears.
5. Select the Browse... button to select the directory where you installed NEWT and choose the OK button. (default directory is C:\NETMANAG). The Install Driver dialog box appears.

6. Choose the OK button. The Unlisted or Updated Additional Network dialog box appears. The NetManage NFS Driver is highlighted in the Additional Networks list.

7. Choose the OK button. The Networks dialog box appears.

8. Choose the OK button. The Network Setup dialog appears and choose OK again. Additional messages appear telling you what files have been modified. Continue to choose the OK buttons until the Network Setup dialog box appears.

9. Choose the Restart Computer button to reboot your machine.

10. After your machine has rebooted, restart Windows.

The network settings in the SYSTEM.INI file are automatically restored to their original settings.

Appendix B. Open Data-Link Interface (ODI)

Note: This appendix is intended only for users that are using the Open Data-Link Interface(ODI) for Windows 3.1 or Windows for Workgroups without Workgroups networking.

About the Open Data-Link Interface (ODI)

The Open Data-Link interface (ODI) allows multiple network protocols to be used concurrently on a LAN adapter in a workstation on the network and is an alternative to NDIS. The components of ODI are:

- Network drivers: Multiple Link Interface Drivers (MLIDs) are device drivers that handle the sending and receiving of packets to and from a physical or logical LAN media.
- Link Support Layer (LSL): Novell's LSL handles the communication between protocol stacks and the network drivers (MLIDs)
- Protocol Stacks: Network Layer protocol stacks transmit and receive data over a logical or physical network.

Custom verifies that your system has LSL.COM running during setup time. If it finds LSL.COM, Custom automatically installs the version of the stack that supports ODI. After ODI is installed you can access a Novell NetWare server, for example, as well as use NEWT in Windows.

The three scenarios described in this section regarding ODI installation are:

- setting ODI manually (first time installation)
- switching from an NDIS environment to an ODI environment
- switching from an ODINSUP environment to an ODI environment

Setting ODI Manually

Follow this section if you are performing a *first time* installation.

- Follow steps 1 - 10 if *you do not have* ODI installed on your system and you are installing NEWT (new installation) for the first time.
- Follow steps 7 - 10 if *you have* ODI on your system and are installing NEWT (new installation) for the first time.

  Once your system is configured for ODI drivers, the NEWT installation will load the driver NMODI.COM in the AUTOEXEC.BAT file. This driver allows NEWT to communicate with the ODI drivers.

ODI Online Help File

Refer to ODI online help for additional information about the NMODI driver. The ODI online help file, named ODI.HLP, contains the following information: ODI driver requirements, a sample NET.CFG, advanced NET.CFG parameters, and troubleshooting tips.

Setting Up Your ODI Environment

The files mentioned in the following steps are contained on the Novell ODI diskette:

- LSL.COM
- LAN Driver for network board (for example, 3C503.COM)
- protocol stack file (for example, IPXODI.COM)

Note: Use the latest LSL.COM, IPXODI.COM, and NETX files from Novell before setting up your ODI environment.

1. At the DOS prompt, create a directory named C:\ODI.
2. Copy the LSL.COM, driver (3C503.COM for example), protocol stack files (IPXODI.COM), and NetWare shell (NETX) to this directory.
3. Append the following lines to the end of the AUTOEXEC.BAT file:

   ```
   C:\ODI\LSL.COM
   C:\ODI\<LAN driver> (for example, 3C503)
   ```

   Optionally, you can add the following lines if you want to have the Novell IPX protocol stack:

   ```
   C:\ODI\IPXODI.COM
   C:\ODI\NETX
   ```

4. Create a NET.CFG file and place it in the C:\ODI directory. Refer to the sample file provided at the end of this appendix.

   A NET.CFG file is required to run *both* NetWare and NEWT concurrently.

Caution: You need to know which NET.CFG file is used by the ODI environment (LSL). We suggest that you have only one NET.CFG file on your disk.

To ensure smooth establishment of an ODI environment, refer to your network adapter vendor's ODI documentation.

5. Reboot your system.

6. If you are using Novell NetWare and loaded Novell ODI drivers, then log onto your server using the appropriate account and password, and verify to see if you are connected to the server by using the WHOAMI command.

Running Custom Application

1. Start Windows.

2. Install NEWT as discussed in your installation instructions.

   You can tell when ODI-based NEWT is installed on your system by viewing the Setup menu on the Custom application. If the Hardware option is grayed out, then ODI is installed on your system and has been detected by the installation program.

   When you are finished setting up Custom, select the Save option to save your configuration.

3. Custom automatically detects the location of the NET.CFG file and then modifies it.

   If Custom cannot detect the NET.CFG file, a prompt appears asking you to enter its path. If you know the file's location, then enter its path and choose the OK button.

   If you do not know the location of the NET.CFG file, then choose the Cancel button. Custom will automatically copy NetManage's sample NET.CFG file and place it at the root directory of drive C. Custom will also open a Window Help file that will give you information about NET.CFG.

   Note: The NET.CFG file that NetManage supplies is only a *sample* file. Because user environments are configured differently, this sample file may or may not work with your configuration. There is an ODI online help file available that contains detailed information about the sample NET.CFG file. You can choose to view this help file when prompted for it.

4. Reboot your system.

Switching from an NDIS Environment to an ODI Environment

This section applies to users who are switching from an NDIS-based interface to an ODI-based interface. This section describes, step-by-step how to:

- upgrade your NEWT to version 4.6
- modify your configuration files in order to switch from an NDIS environment to an ODI environment

Follow these steps:

1. Start Windows in the Enhanced mode.
2. Install NEWT (upgrade installation) according to your installation instructions.
3. After completing installation, reboot your system and do the following:
   - Start Windows and then choose the Network icon from the Control Panel icon.
   - Select NetManage NEWT (all versions) from the list of networks and choose the Remove... button. The NEWT icon will disappear from your screen.
4. From the CONFIG.SYS file, delete the lines:

   ```
   DEVICE=C:\NETMANAG\PROTMAN.DOS /I:C:\NETMANAG
   DEVICE=C:\NETMANAG\ELNKII.DOS       (or your card's driver)
   DEVICE=C:\NETMANAG\NETMANAG.DOS
   ```

5. Delete the following line from the AUTOEXEC.BAT file:

   ```
   C:\NETMANAG\NETBIND
   ```

6. At the DOS prompt, create a directory named C:\ODI.
7. Copy the LSL.COM, Multiple Link Interface Driver (MLID) (3C503.COM for example), protocol stack files (IPXODI.COM), and NetWare shell (NETX) to this directory.
8. Append the following lines to the end of the AUTOEXEC.BAT file:

   ```
   C:\ODI\LSL.COM
   C:\ODI\<LAN driver> (for example, 3C503.COM)
   ```

   Optionally, you can add the following lines if you want to have the Novell IPX protocol stack:

   ```
   C:\ODI\IPXODI.COM
   C:\ODI\NETX
   ```

9. Create a NET.CFG file and place it in the C:\ODI directory. Refer to the sample file provided at the end of this chapter.

   A NET.CFG file is required to run *both* NetWare and NEWT concurrently.

Note: Make sure you add C:\ODI to your path statement in your AUTOEXEC.BAT file.

To ensure smooth establishment of an ODI environment, refer to your network adapter vendor's ODI documentation.

10. Reboot your system.
11. Start Windows from the Program Manager, and select the Run entry from the File menu and enter the following:

    ```
    C:\NETMANAG\CUSTOM.EXE -o
    ```

12. Custom automatically detects the location of the NET.CFG file and then modifies it.

    If Custom cannot detect the NET.CFG file a prompt appears asking you to enter its path. If you know the file's location, then enter its path and choose the OK button.

    If you do not know the location of the NET.CFG file, then choose the Cancel button. Custom will automatically copy NetManage's sample NET.CFG file and place it at the root directory of drive C.

    Note: The NET.CFG file that NetManage supplies is only a *sample* file. Because user environments are configured differently, this sample file may or may not work with your configuration. There is an ODI online help file available that contains detailed information about the sample NET.CFG file. You can choose to view this help file when prompted for it.

13. Close Custom, reboot your system and do the following:

    - Start Windows and choose the Network icon from the Control Panel icon.
    - Choose the Add>> button. The Dialog box expands to include a list of available networks.
    - Select NetManage NEWT (all versions) from the list and choose the Install... button. This network is added to the list of Installed Networks.
    - Choose the OK button. The NEWT icon will appear on your screen.

Switching from an ODINSUP Environment to an ODI Environment

This section applies to users who are switching from an ODINSUP-based interface to an ODI-based interface.

Note: There is no need to keep the ODINSUP configuration with native ODI support. You may want to eliminate some extra layers, thus releasing more memory and increasing reliability.

1. Start Windows in the enhanced mode.

2. Install NEWT (upgrade installation) according to your installation instructions.

3. When the installation is complete, delete these lines from the AUTOEXEC.BAT file:

   ```
   ODINSUP
   NETBIND
   ```

4. From the CONFIG.SYS file, delete the lines:

   ```
   DEVICE=C:\NETMANAG\PROTMAN.DOS /I:C:\NETMANAG
   DEVICE=C:\NETMANAG\NETMANAG.DOS
   ```

5. From the Program Manager, select the Run option from the File menu and enter the following:

   ```
   C:\NETMANAG\CUSTOM.EXE -o
   ```

6. Reboot your system.

Sample NET.CFG File

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
# net.cfg
# NetManage, Inc.      2/19/97
#
# This net.cfg file is a working example and tested
# with NetManage TCPIP protocol stack (nmodi/newt) and # Novell IPX
protocol stack #(ipxodi/netx)simultaneously.
#
# In case a problem occurs:
#
# 1. Make sure there's no other net.cfg on your hard      # disk.
#
# 2. In order for nmodi.com to load/run you need at   # least the following
entries in the appropriate LINK    # DRIVER section of NET.CFG.
#   Ethernet Adapters:
#              frame ethernet_ii
#              Protocol IP    800     ETHERNET_II
#              Protocol ARP   806     ETHERNET_II
#              Protocol RARP  8035    ETHERNET_II
#   TokenRing Adapters:
#              Frame TOKEN-RING_SNAP
#              Protocol IP    800     TOKEN-RING_SNAP
#              Protocol ARP   806     TOKEN-RING_SNAP
#              Protocol RARP  8035    TOKEN-RING_SNAP
#
# Please note that all ethernet sections are similar   # as well as all
token-ring sections.
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
# 3COM EtherLink III Adapter
Link Driver 3C509
        Frame ETHERNET_802.3
        Frame ETHERNET_II
        Protocol IPX   0       ETHERNET_802.3
        Protocol IPX   8137    ETHERNET_II
        Protocol IP    800     ETHERNET_II
        Protocol ARP   806     ETHERNET_II
        Protocol RARP  8035    ETHERNET_II
# INTEL Ether Express Adapter
Link Driver EXP16ODI
        Frame ETHERNET_802.3
        Frame ETHERNET_II
        Protocol IPX   0       ETHERNET_802.3
        Protocol IPX   8137    ETHERNET_II
        Protocol IP    800     ETHERNET_II
```

```
        Protocol ARP   806     ETHERNET_II
        Protocol RARP  8035    ETHERNET_II
#IBM Token Ring Adapter
Link Driver TOKEN
        Max Frame Size 1552
        Frame TOKEN-RING
        Frame TOKEN-RING_SNAP
        Protocol IPX   E0      TOKEN-RING
        Protocol IPX   8137    TOKEN-RING_SNAP
        Protocol IP    800     TOKEN-RING_SNAP
        Protocol ARP   806     TOKEN-RING_SNAP
        Protocol RARP  8035    TOKEN-RING_SNAP
#IBM LAN Support Program
Link Driver LANSUP
        Max Frame Size 1552
        Frame TOKEN-RING
        Frame TOKEN-RING_SNAP
        Protocol IPX   E0      TOKEN-RING
        Protocol IPX   8137    TOKEN-RING_SNAP
        Protocol IP    800     TOKEN-RING_SNAP
        Protocol ARP   806     TOKEN-RING_SNAP
        Protocol RARP  8035    TOKEN-RING_SNAP
#OLICOM Tken Ring Adapter
Link Driver OCTOK16
        Max Frame Size 1552
        Frame TOKEN-RING
        Frame TOKEN-RING_SNAP
        Protocol IPX   E0      TOKEN-RING
        Protocol IPX   8137    TOKEN-RING_SNAP
        Protocol IP    800     TOKEN-RING_SNAP
        Protocol ARP   806     TOKEN-RING_SNAP
        Protocol RARP  8035    TOKEN-RING_SNAP
#Madge Token Ring
Link Driver MADGEODI
        Max Frame Size 1552
        Frame TOKEN-RING
        Frame TOKEN-RING_SNAP
        Protocol IPX   E0      TOKEN-RING
        Protocol IPX   8137    TOKEN-RING_SNAP
        Protocol IP    800     TOKEN-RING_SNAP
        Protocol ARP   806     TOKEN-RING_SNAP
        Protocol RARP  8035    TOKEN-RING_SNAP
# eof # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
```

ODI Troubleshooting

Refer to this section for ODI troubleshooting tips.

- ❑ Make sure your system is running the latest version LSL and MLID. Usually manufacturers of network interface cards have the latest version of available MLID.

Or, you can download them from Compuserve (GO NOVLIB), or from FTP.NOVELL.COM using FTP.

- In case the NMODI driver fails to load, check the following:

  a) make sure there is no other NET.CFG on your hard disk.

  b) make sure the following entries are included in the appropriate LINK DRIVER section of NET.CFG.

  Ethernet Adapters:

```
frame ethernet_ii
Protocol IP            800    ETHERNET_II
Protocol ARP   806     ETHERNET_II
Protocol RARP  8035    ETHERNET_II
```

  TokenRing Adapters

```
Frame TOKEN-RING_SNAP
Protocol IP            800    TOKEN-RING_SNAP
Protocol ARP   806     TOKEN-RING_SNAP
Protocol RARP  8035    TOKEN-RING_SNAP
```

  Please note that all Ethernet Link Driver sections are the same as well as all token-ring sections, independent of a particular MLID.

  If your network media is Token-Ring and you have more than one ring, you may want to put the following line in your AUTOEXEC.BAT file before NMODI:

```
C:\ODI\ROUTE BOARD=2
```

The board parameter insures that ROUTE.COM is bound to logical board TOKEN-RING_SNAP, which handles TCP/IP traffic. Refer to the Novell IPX documentation for more information about ROUTE.COM.

Glossary

access Entry to or communication with a particular object, such as an operating system, specific files, or accounts.

account An entity which is established as an authorized user of the system.

address mask A bit mask used to select bits from an IP address for subnet addressing. The mask is 32 bits long and selects the network portion of the IP address and one or more bits of the local portion.

ANSI The American National Standards Institute sets standards for the U.S. computer industry. ANSI participates in defining network protocol standards.

API Application Program Interface. A standard interface that allows upper-layer applications to work with different communication protocol stacks. Some of the most commonly used ones include NetBIOS, Berkeley Sockets, and Named Pipes.

application An application is a computer program that performs a certain task. FTP, Telnet, TN3270 are some of the applications provided by NetManage.

ARP Address Resolution Protocol. The TCP/IP protocol used to dynamically bind a high-level IP address to a low-level physical hardware address. ARP is only across a single physical network and is limited to networks that support hardware broadcast.

ASCII The American Standard Code for Information Interchange, widely accepted code for representing alphanumeric information.

authenticator A password or code that verifies the identity of individual system or network users.

AUTOEXEC.BAT A file that resides on all PCs and contains a series of commands that are executed when the computer starts up. This file includes the path command that points to the NETMANAG directory where the applications reside.

backup The process of preserving copies of files on a different drive, directory, or media to protect against the destruction or loss of the original files.

Bind The Bind application provides name server functions, such as a Domain Name Server (DNS). You can specify multiple domains and a list of host names within each domain. (See also Domain Name System.)

buffer A temporary storage area for data during the transfer of that data between the computer and a peripheral, or between parts of a computer, to prevent loss of information.

client A computer system that uses resources provided by another machine on the network. Most of NetManage's applications can run as both client and server.

command line The entire command string, including the command and any parameters or qualifiers that it may have. A command is an instruction or request for the system to perform a particular action.

CONFIG.SYS file This file resides on all PCs and defines which device drivers to install.

daemon An agent program that runs continuously on a server system in a UNIX environment and provides resources to client systems on the network.

DLL Dynamic Link Library. Windows automatically loads the applications into memory when required and unloads it when space is needed for other applications. The Chameleon for Windows 95 applications are 100% DLL.

default A value supplied by the system when a user does not specify a required command, parameter, or qualifier.

device name Identification of a physical device: for example, LPT1 for a printer. Can also be a logical name that is equated to a physical device name.

DNS Domain Name System. An online distributed database that maps machine names into IP addresses. (See also Bind.)

domain A named group of machines on the network. A domain name consists of a sequence of names (labels) separated by periods (dots).

driver A software module that controls an input/output port or external device such as a keyboard or a monitor. TCP/IP uses a driver to control the network interface cards.

Ethernet Ethernet is a type of network that supports high-speed communication among systems.

Ethernet address A six-part hexadecimal number in which a colon separates each part (for example, 8:0:20:1:2f:0). This number identifies the Ethernet communications board installed in a PC and is used to identify the PC as a member of the network.

export The process that makes a file available so that other systems can access it.

file access Allows users to work with a remote file as if the file were local.

file server A process running on a computer that provides access to files on that computer to programs running on remote machines.

Finger A standard protocol that lists who is currently logged in on another host.

FTP File Transfer Protocol. The FTP application is used to provide file transfer services across a wide variety of systems. Usually implemented as application-level programs, FTP uses the Telnet and TCP protocols. The server side requires a client to supply a login identifier and password before it will honor requests.

group Id A unique number associated with each group name on the server.

HLLAPI High-Level Language Application Program Interface, which you can use to program in high-level languages such as COBOL, Pascal, BASIC, or C.

host Any end-user computer system that connects to a network. Hosts range in size from personal computers to supercomputers.

host table ASCII text file in which each line is an entry consisting of one numeric address and one or more names associated with that address.

HTML Hypertext Markup Language, is the document formatting language used by World Wide Web browsers. HTML enables

	text formatting, embedded pictures, and hypertext links to other documents and different locations within documents.
ICMP	Internet Control Message Protocol. The ICMP delivers error and control messages from hosts to the requesters. An ICMP test can determine whether a destination is reachable and responding.
IMAP	Internet Message Access Protocol. Defines a way for mail programs to access mailboxes on remote computers as if they were local. Includes operations for creating, deleting, and renaming mailboxes; checking for new messages, and permanently removing messages. It also allows users to share remote folders (mailboxes), to connect from multiple locations, and see a consistent mailbox structure and content.
Internet	When capitalized, the world-wide network of networks connected to each other using the IP and other similar protocols. The Internet provides file transfer, remote login, electronic mail and other services. When not capitalized, any collection of distinct networks working together as one.
Intranet	A private enterprise network that uses TCP/IP standards-based networking technologies for host access, workgroup collaboration, desktop and network resources management, and developer tools for custom applications to maximize the enterprise's productivity. For example, Web began as an Internet application and has now been incorporated into internal company applications.
IP	The TCP/IP standard protocol defined as a unit of information passed across the Internet, providing the basis for packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two most fundamental protocols.
IP address	Internet Protocol address. This is a 32-bit address assigned to host on a TCP/IP Internet. The IP address has a host component and a network component.
IPX/link	The IPX/link application for NetWare connects your PC Novell NetWare LAN through the Network Device Interface Specification (NDIS) developed by Microsoft and 3COM.
Java	A programming language. It can also be a program that can be included in an HTML page on the Web.

log in	To perform a sequence of actions at a terminal that establish a user's communication with the operating system and sets up default characteristics for the user's terminal session.
log out	To terminate interactive communication with the operating system, and end a terminal session.
LPR/LPD	Line Printer Remote/ Line Printer Daemon. An application that allows you to print to network printers.
Mail server	A host and its associated software that offer electronic mail reception and forwarding service. Users may send messages to, and receive messages from, any other user in the system.
MIB	Management Information Base. The set of variables that a gateway running SNMP maintains.
MIB-II	An extended management database that contains variables not shared by SNMP.
MIME	Multi-purpose Internet Mail Extensions. MIME enables: files to be attached to mail messages; multiple objects in a single message; an unlimited line length or overall length for text; character sets other than ASCII; multi-font messages, binary or application specific files; images, audio, video and multi-media messages.
mount	NFS user command that makes remote file systems and resources available to the local PC.
NDIS	Network Device Interface Specification. NDIS is used for all communication with network adapters. The specification was developed by Microsoft and 3COM to provide a common programming interface for MAC drivers and transport drivers. NDIS works primarily with LAN Manager and allows multiple protocol stacks to share a single network interface card.
NetBIOS	Network Basic Input/Output system. Provides a Session Layer interface between network applications running on a PC and the underlying protocol software of the Transport and Network Layers.
NETBUI	The NetBOIS Extended User Interface. This is the transport layer driver frequently used by LAN Manager.
NetWare	A network operating system developed by Novell.

NetWareIP	Feature offered by Novell to allow Windows clients to access Novell servers using the Internet Protocol (IP). Once NetWareIP is installed, you can access all standard NetWare server features normally available from Windows.
network address	A unique number associated with a host that identifies it to other hosts during network transactions.
network printing	Printing to a shared printer locally attached to one of the PCs on the network.
NEWT	NetManage TCP/IP communication stack for Microsoft Windows. NEWT provides users with a degree of network access previously only available to workstation and mainframe users.
NFS	Network File System. A protocol developed by Sun Microsystems that uses IP to allow a set of computers to access each other's file systems as if they were local. Originally designed for UNIX systems, this protocol has been implemented on many other operating systems, including DOS and Windows.
NIC	Network Information Center. The NIC at SRI in Menlo Park, California, assigns IP addresses and network numbers by request. The number assigned is appropriate to the number of host devices on the network.
OfficeVision	An electronic mail application that runs on an IBM mainframe. ZMail Pro supports OfficeVision transport that allows you to exchange electronic mail messages and calendar information between your PC and the IBM mainframe.
PCNSD authenticator	A program that runs continuously and authenticates a user name and password before attempting to mount a network drive, access files, or print on the network.
Ping	The Packet Internet Groper is a program that is useful for testing and debugging networks. It sends an echo packet to the specified host, and waits for a response. It reports success or failure and statistics about its operation.
Plug-in	A third-party embedded application that you can launch from within its "host" application.

POP	Post Office Protocol. This protocol is used by mail applications to retrieve electronic mail services from the Internet.
PROFS	An electronic mail application that runs on an IBM mainframe. ZMail Pro supports PROFS transport that allows you to exchange electronic mail messages and calendar information between your PC and the IBM mainframe.
prompt	Word or words used by the system to assist a user's response. Such messages generally ask the user to respond by typing some information in a supplied field.
RAM	RAM is Random Access Memory.
remote	Files, devices, and users not attached to your local machine.
remote host	The computer receiving a network command.
remote printer	In LPR/LPD, a printer with a special network card, or a PC or workstation.
RFC	Request For Comment. The RFC documents describe all aspects and issues associated with the Internet protocols.
router	A router has two or more network interfaces to different networks. The primary function of a router is to direct packets between these networks, delivering them to their final destination or to another router. When used with TCP/IP, the term refers to an IP gateway that routes data using IP destination addresses.
RPC	Remote Procedure Call. A mechanism defined by Sun Microsystems that provides a standard for initiating and controlling processes on remote or distributed computer systems.
script	A sequence of ASCII text lines stored in a file.
server	A computer that provides services to a network.
SMTP	Simple Mail Transfer Protocol. A protocol used by mail applications to send and retrieve electronic mail messages from the Internet.
SNMP	Simple Network Monitoring Protocol. A standard protocol used to monitor network activity on "agent" nodes from management stations.

subnet A field used by routers and hosts for routing packages on the network.

subnet address An extension for the IP addressing that allows a site to use a single IP network address for multiple physical networks.

subnet mask Identifies the subnet field of a network address. The subnet mask is a 32-bit Internet address written in dotted-decimal notation with all the 1s in the network and subnet portions of the address.

TCP/IP Transmission Control Protocol/Internet Protocol. TCP allows a process on one machine to send data to a process on another machine using the IP protocol. TCP can be used as a full duplex or one-way simplex connection.

Telnet Provides virtual terminal services for a wide variety of remote systems using the Telnet protocol. The application allows a user at one site to interact with a remote system at another site as if the user's terminal were connected to the remote machine.

terminal emulator A program that makes a PC screen and keyboard act like a video display terminal of another computer.

TFTP Trivial File Transfer Protocol. A standard TCP/IP protocol that allows simple file transfer to and from a remote system without directory or file listing. TFTP is used where FTP is not available.

token-ring A type of ring-shaped network that supports high-speed communications between computers. A distinguishing packet, called a "token," is transferred from machine to machine. Only the machine that holds the token can transmit the packet.

TSR Terminate-and Stay-Resident. A DOS program that is loaded into memory before Windows and stays in memory until the machine is rebooted.

user id A unique number, created by your system, that is associated with each user name on a server system.

user name A character string, usually assigned by the system administrator that identifies a user on the system.

utility A command or operation that works at the level of the operating system.

Weighted Fair Queuing (WFQ)	ChameleonNFS feature that can guarantee bandwidth to specified IP traffic. WFQ is particularly useful for applications that require real-time performance capabilities across routed networks. Applications for which WFQ is useful include video-conferencing programs (such as NetManage's InPerson), video servers, internet telephony, real-time simulations, and other performance critical networking task software.
VRML	Virtual Reality Modeling Language. Uses a 3D rendering engine to render the image progressively in pieces. Supports the .GIF, .JPEG, .BMP, and SFImage file formats, as well as extensions such as background color.

Index

—A—

activating a script, 59
adapters
  Token Ring, 106
adding applications
  to NEWTToolbar, 77
Address Resolution Protocol (ARP), 39
Advanced
  tabs, 66
Advanced tab, 38
alternate gateway, 37
applications
  starting, 5
ARP, 39
ARP table, 70
Auto Start option, 79

—B—

BBS, 7
BOOTP, 32, 33

—C—

Call Type tab, 42
capturing scripts, 54
Challenge Handshake Authenticator Protocol, 59
CHAP, 59
classes
  of traffic, 14
closing
  NEWTToolbar, 78
column order, changing, 6
column width, changing, 6
community option, 73
Compressed SLIP Protocol, 45
Compuserve, 7
configuration files, 5
CSLIP, 45
CSLIP setup, 46
Custom, 22, 29, 57, 65
  adding interfaces, 40
  ISDN interfaces, 41
Custom Terminal feature, 55
Custom, interface types, 29
customer support, 6

—D—

default gateway, 37
DHCP, 32, 34
Dialer, 29, 31, 57
  adding interfaces, 40
  ISDN interfaces, 41
  learn mode, 54
dialup, 45
Dial-up Login, 64
DLL, 2
DNS, 35
domain name, 26
Domain Name Server (DNS), 35
Dynamic Host Configuration Protocol, 32, 33

—E—

echo reply, 79
Ethernet, 22, 29
Ethernet adapters, 106
Ethernet/DIX, 39
Ethernet/IEEE, 39
exiting
  NEWTToolbar, 78

—F—

filters
  Network Policy Management, 10, 12, 13
flow control, 46, 48, 49
Forum
  NEWTToolbar button, 75
Frequent Destinations, 39

—G—

gateway, 70
  alternate, 37
  default, 37
Gateway tab, 37
Go IntraNet!
  NEWTToolbar button, 75

—H—

hardware, 23
hardware requirements, 19
host administration option, 71
host name, 25
host table, 36

—I—

ICMP, 79
INETD, 42
installing, 20
  preparing for, 19
Interactive Log Window Feature, 55
Interface Type option, 48
interfaces
  adding in Custom, 40
  adding in Dialer, 40
  ISDN, 41
Internet address, 25, 32
Internet Control Message Protocol (ICMP), 79
IP address, 32, 37
  entering, 25
IP address in SLIP, 63
IP Configuration tab, 32
IP precedence, 10, 14
IP/UDP bootstrap protocol, 33
ISDN, 29
  interfaces, 41
ISDN interface, 23
ISDN interfaces, 41
ISDN.INI, 23, 24

—L—

learn mode, 54
license violation, 6
Login tab, 54, 55

—M—

MLID, 102, 106
Modem tab, 49
modifying existing scripts, 61
Multiple Link Interface Driver, 102

—N—

Name Resolution tab, 35
NDIS, 1, 2, 81, 85
NET.CFG, 26, 100, 102
NetWareIP
  overview, 16
  setting up, 16
network adapter, 1
Network Device Interface Specification (NDIS), 1
Network Information Service, 26
Network Policy Management
  filters, 10
  setting up, 10
Network Policy Management (NPM), 9
Network Policy Management filters, 12, 13
NEWT, 20, 27, 57, 68, 69, 80
  setting up
    in Windows 3.1, 22
    in Windows 95, 21
NEWTToolbar
  adding applications, 77
  button menu, 76
  exiting, 78
  main menu, 75
  modifying buttons, 77
  starting, 75
  starting applications from, 78
NIS, 26
NMODI, 106
NMODI driver, 100
NMODI.COM, 100
Novell, 92
NPM. *See* Network Policy Management
null-modem, 49

—O—

ODI, 1, 26, 96
ODINSUP, 103
ONC RPC/XDR, 3
Original Equipment Manufacturer, 95

—P—

PAP, 59
Password Authentication Protocol, 59
Ping, 79
pinging, 79
Point to Point Protocol, 45
PPP, 29, 45
PPP setup, 46
primary interface, 39
protocol extensions, 9
protocols, 32, 39
PSI, 45

—Q—

quitting
  NEWTToolbar, 78

—R—

RARP, 32, 34
registration card, 6
requirements
  hardware, 19
  software, 19
Reverse Address Resolution Protocol, 32, 34
route entries, 67
route table, 70
RPC-SDK, 3

—S—

scripts
  capturing, 54
  using captured, 55
Serial Line Internet Protocol, 45
serial number, 6
setting up
  NetWareIP, 16
  Network Policy Management, 10
setting up NEWT
  in Windows 3.1, 22
  in Windows 95, 21
setup, 19
SLIP, 22, 29, 45
SLIP interface, 64
SLIP scripting, 59
SLIP setup, 46
SLIP/PPP/CSLIP script example, 59, 60
Smart Buttons, 5
SNMP, 69, 70
SNMP agents, 70
SNMP table, 70
socket table, 70
SOCKS, 15
software requirements, 19
starting applications, 5
Status Bar, 5
subnet bits, 25, 32
subnet mask, 25, 32

—T—

tabs
  Advanced, 38, 66
  Call Type, 42
  Gateway, 37
  IP Configuration, 32
  Login, 54, 55
  Modem, 49
  Name Resolution, 35
Telnet
  NEWTToolbar button, 75
Token Ring, 22, 29
  adapters, 106
Toolbar, 5
traffic classes, 14
trap administration option, 72

—U—

UDP/IP, 32
using captured scripts, 55
using dialup protocols, 45, 65
using routing, 65

—W—

WebSpider
  NEWTToolbar button, 75
WebSurfer
  NEWTToolbar button, 75
Weighted Fair Queuing, 14
WFQ, 14
Windows for Workgroups, 81

—Z—

ZMail Pro
NEWTToolbar button, 75

Reader's Comment Form

NetManage Configuration Guide, Version 6.0

Part No. 5000-60-0696

NetManage, Inc. welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented ?
- Do you need more information? if so, where?

If you find any errors or have any suggestions for improvement, please indicate the topic, chapter, and page number.

Please mail or fax your comments to:

Technical Publications, NetManage, Inc.

10725 N. De Anza Blvd., Cupertino, CA 95014, USA

Phone : (408) 973-7171 Fax: (408) 973-8272

e-mail: doc@netmanage.com

If you would like a reply, please give your name, company name, address, and telephone number below. We are committed to responding promptly to your suggestions.

We are grateful for your assistance.