Custom Index

This Help file contains a list of all Help topics available for Custom. You can use the scroll bar to see the entries that are not currently visible in the Help window.

For information on how to use Help, press F1 or choose Using Help from the Help menu.

Overview

File

- New
- Open...
- Save
- Save As...
- Set Password...
- Exit

Interface

- Add...
- Duplicate...
- Delete

Setup

- LAN Interface
  - Hardware...
  - Ethernet Type... (Ethernet only)
- All Interfaces
  - IP Address...
  - Subnet Mask...
  - Host Name...
  - Domain Name...
- SLIP/PPP Only
  - Port...
  - Modem...
  - Dial...
  - Login...
- Option for all Interfaces
  - Interface Name...
  - Primary Interface
  - Route Entries...
- Using Bootstrap Protocol
  - BOOTP...
- Logging SLIP/PPP and modem commands
  - LOG...

Services

- Default Gateway...
- Frequent Destination...
- Domain Servers...
- SNMP...
  - Agents

Settings

- Host...

Overview

Custom is the customization and control program supporting NetManage NEWT- Enhanced Windows TCP/IP stack. NEWT can be configured to concurrently utilize multiple network interfaces. NEWT supports Ethernet, Token Ring, FDDI, SLIP (Serial Line Internet Protocol), CSLIP, and PPP (Point to Point Protocol). SLIP/PPP allows the host to communicate with another host or Network using a serial line, directly attached and/or a modem.

Interface configuration can be stored in a file. The default configuration file is TCPIP.CFG, and is loaded by the NMPCIP.DLL at start up.

An animated icon mechanism is provided, to signal that any connection is active or non_active.

New

New creates a new configuration template.

When you choose New, Custom lets you start with a blank configuration template(file).

To select a new file:

1. Point to the File menu and click the mouse button.
2. Click the **New** command.

Open...

Open an existing configuration file.

When you choose Open, Custom lets you load an existing configuration file.

To Open a new configuration file:

Point to the File menu and click the mouse button.

1. Click the **Open** command.
2. Select the Drive and directory by double click the selected item.
3. Enter or double click the filename into the text box.
4. Choose OK.

Save

To save configuration parameter changes, to the default file:

1. Point to the File menu and click the mouse button.
2. Click the **Save** command.

Save As...

The Save As enables you to select the file name, directory, and drive to be used for saving configuration parameters.

To select a new Filename:

1. Point to the File menu and click the mouse button.
2. Click the **Save As** command.
3. Select the Drive and directory by double click the selected item.
4. Enter the filename into the text box.
5. Choose OK.

Set Password...

Set Password enables you set a password for the Custom application. This will prevent users from changing Custom configuration without permission.

To set a password:

1. Point to the File menu and click the mouse button.

2. Click the **Set Password** command.

3. Type your password in the New Password box.

Note: if you have already set a password, Custom will prompt you for your old password before you set up the new password.

4. Enter the new Password in the Confirm Password box.

5. Choose OK.

Note: To delete you old password, type in your old password and click OK. You will be prompted to enter your new password and confirm.

Exit

To exit the configuration program:

1. Point to the File menu and click the mouse button.
2. Click the **Exit** command.

Interface Add

Interface Add, will add the appropriate network interface environment (data structure) for your computer and network interface adapter.

The new interface will be added to the list of available interfaces. Additional information about a specific interface can be displayed by pointing to the list and selecting a given interface.

To add an interface:

1. Point to the Interface menu and click the mouse button.

2. Click the **Add** command.

3. To select the Interface type. Point to the arrow and click, a list of supported interfaces (Ethernet, Token Ring, FDDI, SLIP, CSLIP, or PPP) will drop. Point to the appropriate the list and click.

4. An interface name will be automatically assigned to the new interface. If desired, you can change the assigned interface name. To change the interface name, point to the name text box and click. Enter in the text box the new name.

5. Choose OK.

Interface Duplicate

Interface Duplicate, will copy an existing data structure into a new network interface environment (data structure) using an identical configuration information. You will be asked to identify the new interface by a unique name. This command is very helpful in duplicating SLIP/CSLIP/PPP interface information for multiple phone numbers.

To duplicate an interface:

1 Select the interface to be duplicated from the list of configured interfaces.

2. Point to the Interface menu and click the mouse button.

3. Click the **Duplicate** command.

4. An interface name will be automatically assigned to the new interface. If desired, you can change the assigned interface name. To change the interface name, point to the name text box and click. Enter in the text box the new name.

5. Choose OK.

The new interface will be added to the list of available interfaces. Additional information about a specific interface can be displayed by pointing to the list and selecting an interface.

Interface Delete

Interface Delete, will delete an existing interface from the list of available interfaces.

To delete an interface:

1 Select the interface to be deleted from the list of configured interfaces.

2. Point to the Interface menu and click the mouse button.

3. Click the **Delete** command.

Setup Hardware

Setup hardware, will install the appropriate environment for your computer and network interface adapter.

Note: If your network adapter is **not specified in this list**, select "**Other**" for vendor name. You'll be asked to provide the Protocol Manager section name, driver name, and the NDIS driver file name. All those are provided to you *by the vendor of your network adapter card*. In the **Newt disk** we have also included several drivers as a courtesy service. They are included in ETHERNET, TOKEN RING, and FDDI sub-directories.
The dialog box also provides a space to enter lines necessary for the Protocol Manager network adapter section as required by your specific card (E.g., "IRQ=...", "IOADDRESS=...", etc.).
Consult with the instructions that accompany your Network Adapter Card for details. They will typically be in an "NDIS" or "Lan Manager" section of the installation.

To install the adapter, and the TCP/IP stack, you will need to insert the NetManage Newt diskette with the Drivers into drive A.

To setup the hardware:

1. Point to the **Setup** menu and click the mouse button.

2. Click the **Hardware** command.

3. Select the Vendor of the adapter you are using. Point to the arrow and click, a list of supported vendors will drop. Point to the appropriate one from the list and click.

4. Point to the Board Type arrow and click. A list of supported boards will drop. Select the appropriate LAN Adapter Board.

5. If required, the Interrupt Level, and Transceiver Type text box will be turned on. You must select the interrupt level and transceiver type.

   A. Point to the Interrupt Level arrow and click. A list of supported interrupts will drop. Select the appropriate Interrupt Level.

   B. Point to the Transceiver Type arrow and click. A list of supported Transceivers will drop. Select the appropriate Transceiver Type.

6. If required, additional drivers are copied to the selected directory. At this time a massage will be displayed asking for additional drivers. The default drive selected is drive A. You can enter in the text box any drive and/or directory that contain the NDIS driver for the selected board, and Choose OK.

Setup Ethernet Type

Setup Ethernet Type, will instruct the TCP/IP stack to transmit Ethernet/DIX or 802.3 type packets. Select the appropriate packet type for your network.

NEWT will automatically receive either type.

Setup IP Address

Internet Protocol. A datagram protocol used to transport datagrams over and across LAN - Local Area Networks.

For more information on Network Addresses select-> Network Addresses

To select a new IP Address:

1. Point to the **Setup** menu and click the mouse button.
2. Click the **IP Address** command.
3. Enter the IP address into the text box.
4. Choose OK.

If you wish to reset the IP value, point to the reset button positioned to the left of the IP text box and click the mouse button.

You are allowed to have the IP Address 0.0.0.0 *only* if you are using PPP.

Setup Subnet Mask

Subnetting is a scheme for imposing a simple hierarchy on hosts on a single physical network.

For more information on Network Addresses select-> Subnetting

To set the number of bits to be used in the subnet mask:

1. Point to the **Setup** menu and click the mouse button.

2. Click the **Subnet Mask** command.

3. Enter the number of bits to be used in the text box, or; move the mouse to position the insertion point, click the left button and hold it. Drag the mouse to the left until you get the number of bits desired, and then release the button.

4. Choose OK.

Setup Host Name

To set a host name:

1. Point to the **Setup** menu and click the mouse button.
2. Click the **Host Name** command.
3. Enter the Host Name into the text box.
4. Choose OK.

Setup Domain Name

To set a domain name:

1. Point to the **Setup** menu and click the mouse button.
2. Click the **Domain Name** command.
3. Enter the Domain Name into the text box.
4. Choose OK.

Setup Port

Setup Port, sets the SLIP/PPP communications parameters.

You can set:

Baud Rate--To specify the desired baud rate of a modem.
Data Bits--To specify the number of data bits in the data packets sent between the two computers.
Stop Bits--To specify the time between transmitted characters.
Parity--To specify the parity type.
Flow Control--To tell Terminal what to do if the buffer becomes too full to receive more data from the remote system.
Connector--To select the communications port your modem uses.
Parity Check--To show the byte in which the error occurred.
Carrier Detect--The default is off. If your modem supports Carrier Detector, the script executes only if it detects the carrier. Otherwise, it executes the script immediately.

For more information on Port configuration select-> Port Options

To specify Port parameters:

1. Choose **Port** from the **Settings** menu.
2. Select the options appropriate for your system and the remote computer, and then choose OK.

Setup Modem

Specifying Modem Commands

To specify modem commands:

1. Choose **Modem** from the **Settings** menu.

2. Select your modem type from the Modem Defaults area and choose OK.
   Selecting NONE will indicate a direct connection.

3. Change the commands as appropriate.
   If you make a mistake, reset the commands by choosing the modem type again.

4. Choose OK.

Setup Dial

Setup Dial is used to set the phone number and other control information to be used with the current name settings.

To specify the phone number that SLIP/CSLIP/PPP will dial:

1. Choose **Dial** from the **Setup** menu.

2. Enter the phone number in the Dial text box.
   Enter commas to add pauses.
   If a phone number is left blank, Connect will assume an answer mode.

3 Select the other options:

Timeout If Not Connected In:
Set the number of seconds Terminal waits for a connect signal from the remote computer.

Redial After Timing Out:
Dial the phone number again if a previous attempt failed.

Signal When Connected:
Ring the system bell when a successful connection has been made.

Redial After Carrier is Lost:
Redials automatically as soon as connection is lost.

Open Log When Connecting:
Opens log automatically upon connecting.

4. Choose OK.

Setup Login

Setup Login, will use the information provided by the user to facilitate the login process to networks (Internet) that require a User Name, Password, and a command to notify the host that the connection is a SLIP/CSLIP or PPP connection.

1. Point to the **Setup** menu and click the mouse button.
2. Enter the user name into the User Name text box.
3. Enter the password into the User Password text box.
4. Enter the SLIP command into the Startup Command text box.
5. Choose OK.

Using CHAP

The Challenge Handshake Authentication Protocol (CHAP), which is used with PPP, is now supported. The server has to be configured to use CHAP.

The user login and password defined in Custom are used during the CHAP process and the CHAP secret is stored in the Custom Password field. If the server does not prompt for a user login and password, then use the -n in the script `(SCRIPT=-n)`. Refer to the Scripting chapter.

Do not leave the script blank, otherwise Custom will automatically use the default

```
[DEFAULT]
(SCRIPT=login: $u$r word= $p$r)
TYPE=PPP
```

Custom supplies two fields: Login and Password. The CHAP secret is stored in the Custom Password field. On remote sytems that have the three fields (Login, Password, and CHAP Secret), you can normally disable their Password field.

SLIP/CSLIP/PPP Scripting

Use SLIP, CSLIP, or PPP's scripting language if you require automatic network dialogs different than the ones provided. You can define a different script for each SLIP interface. The default SLIP.INI file will satisfy your needs in most of the cases. By default, the SLIP file resides in your NETMANAG directory. If you choose to modify the scripts provided, update the SLIP file using the scripting language syntax below:

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

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

$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 DEC code XX
$u - send the user id
$p - send the password

$c - send the SLIP COMMAND
$d - send the phone number
$$ - send a "$" character
$f - define a prompt
$l - call-back mode

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

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

Using the $f Prompt

Use the $f to define a prompt (caption title) that you want to appear on your login message box. 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."

[DEFAULT]
SCRIPT=name: ur word: pr -n 6c$r -i
TYPE=SLIP

[SLIP0}
SCRIPT=login: ur word: $fPassword $r
TYPE=SLIP

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.

Using the $l Prompt

To use the $1 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 will cause Custom to close the connection and put the modem in call-back mode, anticipating a call from the server.

[NetCom]
SCRIPT=login: ur word: pr $l

Anything after $l in a script will be ignored, so always make sure it is the last item.

Default Script in SLIP.INI File

The following is the default script in your SLIP.INI file:

```
[DEFAULT]
SCRIPT=name: $u$r word: $p$r -n $6$c$r -i
TYPE=SLIP
```

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)

Setup Interface Name

To set a Interface name:

1. Point to the **Setup** menu and click the mouse button.
2. Click the **Interface** Name command.
3. Enter the Interface Name into the text box.
4. Choose OK.

Setup Primary Interface

To set an Interface as the Primary Interface:

1. Point to the **Setup** menu and click the mouse button.
2. Click the **Primary Interface** command.

Setup Route Entries

Route Entries informs the NEWT Router about the networks the router supports on designated interfaces. NEWT will attempt to route packets designated to destinations other then this host, or redirects, by checking the route entries. If a an entry matching the destination is found, the packet will be routed to the appropriate gateway through the designated interface. Packets with unknown destination be dropped.

To set Route Entries:

1. Point to the **Setup** menu and click the mouse button.

2. Click the **Route Entries** command.

3. Add up to 5 IP address and Subnet information (optional), of networks that can be reached through the designated interface.

   If the selected interface is SLIP, a list of IP's is sufficient.

   If the selected interface is not SLIP, you must enter the IP address of the designated gateway to which the packet will be routed.

4. Choose OK.

BOOTP...

The IP/UDP bootstrap protocol (BOOTP) allows a workstation to find its Internet address. A workstation running BOOTP client broadcasts onto the network a BOOTP request packet. A machine running 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 overwrite your configuration.

1. Choose the Custom icon.

2. Select the **BOOTP...** option from the Setup menu. The BOOTP dialog box appears.

3. Select the Use BOOTP option.

4. If desired, enter the BOOTP server IP address.

5. If you do not specify a server IP address, the BOOTP request will broadcast on the network.

6. Choose the OK button.

Log Option

Log allows you to record modem and SLIP configuration commands. Log works only during SLIP operations. Currently log collection can be started and stopped, saved to a file, printed and deleted, using Windows shortcut keys only.

The log file is very useful for debugging and tracing interoperability issues, and is usually used by network administrators.

Default Gateway

Default Gateway is used to informs the NEWT Router about a designated gateway that NEWT will use if an attempt was made by this host applications to send a packet to an unknown destination.

If a Default Gateway is not specified (Default Gateway IP all 0's), packets with unknown destination be dropped.

To set a new IP address for the default gateway:

1. Point to the **Services** menu and click the mouse button.
2. Click the **Default Gateway** command.
3. Enter the IP address into the text box.
4. Choose OK.

If you wish to reset the value, point to the reset button positioned to the left of the text box and click the mouse button.

Frequent Destinations

The frequent destinations table is provided as a mechanism to minimize the number of ARPs the stack will have to perform to resolve the Internet to Ethernet address identification procedure. If you communicate frequently with the same devices you can enter the information into the table which will be used at initialization.

To set the frequent destination table:

1. Point to the **Services** menu and click the mouse button.

2. Click the **Frequent Destinations** command.

3. Enter the IP address into the IP Address text box.

4. Enter the Physical address into the Physical Address text box in hex

5. Repeat steps 3, and 4 for every frequent destination, up to three destinations.

6. Choose OK.

If you wish to reset the value, point to the reset button positioned to the left of the text box and click the mouse button.

Domain Servers

Domain Servers. A set of IP address of domain name servers to be used by this application.

To set the IP address for the domain name servers:

1. Point to the **Services** menu and click the mouse button.
2. Click the **Domain Servers** command.
3. Enter the IP address into the text box.
4. Repeat step 3 for every domain name server you wish to use, up to three servers.
5. Choose OK.

If you wish to reset the value, point to the reset button positioned to the left of the text box and click the mouse button.

SNMP

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

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

Note: The SNMP Daemon icon and application included with this release of ChameleonNFS is now an integral part of the NEWT TCP/IP protocol stack. It is not necessary to run the SNMP application, but it is included for backward compatibility.

Several SNMP agents are provided with ChameleonNFS. 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, ChameleonNFS 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
Trusted Managers 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 Custom icon.

2. Select SNMP, then Settings and then the Host Administration... option from the Services 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 Custom icon.

2. Select SNMP, then Settings and then the Trusted Managers... option from the Services 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 Custom icon.

2. Select SNMP, then Settings and then the Trap Administration... option from the Services 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 Custom icon.

2. Select SNMP, then Settings and then the Community... option from the Services menu.

3. Enter the a 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.

Selecting Agents

You can select the Workstation, DOS, and Windows agents by doing the following:

1. Choose the Custom icon.

2. Select SNMP and then Agents from the Services menu. A box listing the Workstation, DOS, and Windows agents appear.

3. Select the desired agents. A checkmark appears next to the agents you select.

To view a list of current agents, save selections to a configuration file, or monitor SNMP related statistics, refer to the chapter that discusses NEWT.

Agents

"Agents" provides a list of all agents that are currently registered with the SNMPD.

A "check" by the name of the agent means that this agent is currently **active**. If there is no "check" the agent is **passive**.

You toggle the state of the agent by clicking on its name. I.e.,

To turn **on** an agent (the agent name has no check to its left):

1. Point to the Agent menu and click the mouse button.
2. Click the agent name.

To turn **off** an agent (the agent name has a check to its left):

1. Point to the Agent menu and click the mouse button.
2. Click the agent name.

Agents Provided with this release:

MIB-II
SNMP_Daemon
Workstation
DOS
WINDOWS

MIB-II

Groups supported include:

- System Group
- Interface Group
- Address Translation Table Group
- IP Group
- ICMP Group
- TCP Group
- UDP Group

Current support is to RFC 1213. Except the EGP Group and the Transmissions Group.

SNMP Daemon

The SNMP Daemon Group is defined under the NetManage Enterprise (=233). It is defined as Object-Id = **NetManage.1**. It provides information about the agents that are currently registered with the daemon. Its structure is a table (OID=snmpd.1). Each entry in the table (OID=snmpd.1.1) is indexed by the Enterprise-OID of the agent, and consists of the following information:

agentEnterprise (OID=entry.1)
The Enterprise-ID (sub-tree) for which the agent is registered. (OBJECT IDENTIFIER)

agentWindow (OID=entry.2)
Returns the window handle of the agent's process (INTEGER).

agentDescription (OID=entry.3)
Returns a DisplayString with the agent's description.

Workstation

The Workstation Group (ws) is defined under the NetManage Enterprise (=233). It is defined as Object-Id = **Netmanage.2** and includes the following objects:

wsCPU (OID=ws.1)
Returns (Display String) the workstation CPU type (e.g., 386)

wsComputerType (OID=ws.2)
Returns (Display String) the workstation Computer Type (e.g., PC/AT).

wsModel (OID=ws.3)
Returns (INTEGER) model number.

wsSubmodel (OID=ws.4)
Returns (INTEGER) submodel number.

wsBiosVersion (OID=ws.5)
Returns (INTEGER) the Bios version.

wsOS (OID=ws.6)
Returns (DisplayString) the operating system name (e.g., MS-DOS)

wsOSMajVersion (OID=ws.7)
Returns (INTEGER) the operating system major version number (e.g., "5" for DOS 5.0)

wsOSMinVersion (OID=ws.8)
Returns (INTEGER) the operating system minor version number (e.g., "0" for DOS 5.0)

wsNDISstable (OID=ws.9).
==========
This is a table which describes the different adapter cards that reside inside the workstation. The table is indexed by the physical address of the entries. The structure of each entry (OID=ws.9.1) consists of the following information:

wsPermPhysAddr (OID=entry.1)
Return the permanent address of the adapter (PhysAddress)

wsCurrPhysAddr (OID=entry.2)
Returns the current address assigned to the adapter (not always equal to the "permanent address". Some communications packages, such as Decnet, change it) (type is PhysAddress)

wsDescription (OID=entry.3)
Return a DisplayString that describes the adapter.

wsModuleName (OID=entry.4)
Returns a DisplayString that describes the module name.

wsMACType (OID=entry.5)
Returns a DisplayString describing the MAC used by the adapter.

wsIEEECode (OID=entry.6)
Returns (Octet) the IEEE code assigned to the manufacturer of the adapter.

wsIRQ (OID=entry.7)
Returns (INTEGER) the interrupt line used by the adapter.

wsFrameSize (OID=entry.8)
Returns (INTEGER) the Frame Size used by the adapter.

wsTXCapacity (OID=entry.9)
Returns (INTEGER) the Transmit Buffer capacity of the adapter.

=========(end of NDIS table definition)==========

wsMathCoprocessor (OID=ws.10)
Returns 1 if math co-processor exists, 0 otherwise.

wsFloppyDrives (OID=ws.11)
Returns the number of floppy drives defined for the workstation.

wsRS232Ports (OID=ws.12)
Returns the number of serial ports defined for the workstation)

DOS MIB

The DOS Group is defined under the NetManage Enterprise (=233).

It is defined as Object-Id = **Netmanage.3** and includes the following objects:

- Current Drive (OID=Dos.1)

  Returns the "Current Drive" in use at your machine, with 1=A, 2=B, etc.

- DOS memory size (OID=Dos.2)

  Returns DOS base memory size in K-bytes (typically 640)

WINDOWS MIB

The Windows Group is defined under the NetManage Enterprise ID (=233)
It is defined as Object-Id = Netmanage.4 and includes the following objects:

Windows Version (OID=Windows.1)

Returns a string showing the Windows version number of your PC

.

Memory Above (OID=Windows.2)

Returns the amount of memory (in bytes) available above the EMS bankline (refer to "Windows guide to Programming" for more information).

Memory Below (OID=Windows.3)

Returns the amount of memory (in bytes) available below the EMS bankline (refer to "Windows guide to Programming" for more information).

Windows Flags (OID=Windows.4)

Returns the Windows' configuration flags on your PC. (refer to the Windows manual for bit interpretation)

windows task table (OID=windows.5).

==========

This is a table which describes the tasks (applications) that are currently running at the workstation. The table is indexed by the window handler of the task. This list is the same as the one you'll see in Window's "Task List" (double-click anywhere on the background to see the task-list). The structure of each entry (OID=windows.5.1) consists of the following information:

winHandle (OID=entry.1)

Returns (INTEGER) the window handle of the task (meaningful only to programmers)

winStyle (OID=entry.2)

Returns (INTEGER) the window style (a bit mask of different attributes, meaningful only to programmers)

winClass (OID=entry.3)

Returns a DisplayString that describes the class of the task.

winTitle (OID=entry.4)

Returns (DisplayString) the title (name) of the task (e.g., "program Manager", "ping-Unix", etc.)

winModule (OID=entry.5)

Returns (DisplayString) with the task module (typically the command that started it, e.g., c:\netmanag\ping.exe)

Host

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 Host administration information, do the following:

1. Choose the SNMP icon.

2. Select the **Host Administration...**option from the Setting 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.

This information will be available for management stations that support the MIB-II.

Trusted Managers

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 Custom icon.

2. Select SNMP, then Settings and then the Trusted Managers... option from the Services 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

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. Select the **Trap Administration...** option from the Settings menu.

2. Enter the default destination to where SNMP agent notification will be sent.

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

Community

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. Select the **Community...** option from the Settings menu.

2. Enter the a 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.

3. Choose the OK button.

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

Host Table

The hosts table / file contains information regarding the known hosts on the TCP/IP network. For each host a single line should be present with the following information:

- Internet-address
- official-host-name
- aliases

Here is a typical line from the hosts file:

100.100.100.10 sunny

If you wish to designate your own names to hosts you communicate with, you can use this command to create your local HOSTS file.

To create a local HOSTS file:

1. Point to the **Services** menu and click the mouse button.
2. Click the **Host Table** command.
3. Enter the official name in the text box.
4. Point to the Add button and click the mouse.
5. A new dialog box will pop-up, it allows you to set the IP address, as well as Aliases to the official name.
6. Enter the IP address into the text box.
7. If you wish to add aliases to the official name, point to the Aliases text box, enter the name, and point and click the Add button. You can manage the aliases by adding or deleting names from the table by using the appropriate buttons.
8. When you are done point and click the Ok button.
9. Repeat steps 3 to 7 for every name you wish to add official names to the file.
10. Choose OK, the Hosts file will be updated for you at this time..

Note: the hosts file changes are effective immediately after the changes are saved.

Connect

Connect is used to establish a SLIP connection to a remote computer or network.

To establish a SLIP connection:

1 Select the SLIP interface to be connected from the list of configured interfaces.

2. Point to the **Connect** menu and click the mouse button.

Disconnect

Disconnect is used to close the connection between this computer and the remote computer or network.

To Disconnect:

1 Select the SLIP interface to be disconnected from the list of configured interfaces.

2. Point to the **Disconnect** menu and click the mouse button.

Setting ODI

The Open Data-Link interface (ODI) is an architecture that enables multiple protocol stacks to be used with one or more LAN adapters in a workstation on the network and is an alternative to NDIS.

ODI allows multiple network protocols and LAN adapters to be used concurrently on the same workstation or file server. ODI is comprised of three components:

Network drivers: Network or Multiple Link Interface Drivers (MLIDs) are device drivers that handle the sending and receiving of packets to and from a physical or logical LAN medium.

Link Support Layer (LSL): The 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 ODI components running during setup time, and if so automatically installs the version of the stack that supports ODI. After ODI is installed you can access the Novell server, for example, as well as use Chameleon in Windows.

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 ChameleonNFS (new installation) for the first time.

Follow steps 7 - 10 if *you have* ODI on your system and are installing ChameleonNFS (new installation) for the first time.

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)

1. At the DOS prompt, create a directory named C:\ODI.

2. Copy the LSL.COM, LAN driver (3C503.COM for example), protocol stack files (IPXODI.COM), and Netware shell (NETX.COM) 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)
C:\ODI\IPXODI.COM
C:\ODI\NETX
```

4. Create a NET.CFG file and place it in the C:\ directory.

A NET.CFG file is required to run *both* NetWare and Chameleon*NFS*.

If you have any questions or problems about establishing an ODI environment, refer to your network

adapter vendor's ODI documentation.

5. Reboot your system.

6. 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

7. Start Windows

8. Install ChameleonNFS (refer to your Quick and Install Card).

   You can tell when ODI 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. Then, a message prompts you for the location of your NET.CFG file.

9. Custom automatically detects the location of the NET.CFG file after it is invoked by LSL.COM, 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 C root.

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.

10. Reboot your system.

ODI Online Help File

The ODI online help file contains the following information: ODI driver requirements, a sample NET.CFG file, advanced NET.CFG parameters, FRAME FORMATS, and troubleshooting tips.

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.

1. Start Windows in the Enhanced mode.

2. Install ChameleonNFS (upgrade installation) according to the instructions on your Quick Install Card.

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

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

4. When the installation is complete, delete this line from the AUTOEXEC.BAT file:

   C:\NETMANAG\NETBIND

5. Follow Steps 1 - 4 from the previous section *Setting Up Your ODI Environment.*

6. Reboot your system.

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

   C:\NETMANAG\CUSTOM.EXE -o

8. Custom automatically detects the location of the NET.CFG file after it is invoked by LSL.COM, 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 C root.

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.

9. When complete, close Custom. Reboot your system.

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.

1. Start Windows in the enhanced mode.

2. Install ChameleonNFS (upgrade installation) according to the instructions on your Quick Install Card.

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

   ODINSUP
   NETBIND

Then add this line at the end of the file, but *before* you start Windows:

   C:\NETMANAG\NMODI

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.   05/11/93
#
# 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 of 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 RARP8035   ETHERNET_II
#   TokenRing Adapters:
#            Frame TOKEN-RING_SNAP
#            Protocol IP  800    TOKEN-RING_SNAP
#            Protocol ARP 806    TOKEN-RING_SNAP
#            Protocol RARP8035   TOKEN-RING_SNAP
#
# Please note that all ethernet sections are similar
# as well as all token-ring sections.
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #

Link Support
       Buffers      8 4212 ;for token-ring
       MemPool      4096
       Max Stacks 8

# 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 Ehter 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
       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
#IBM LAN Support Program
Link Driver LANSUP
       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
#OLICOM Tken Ring Adapter
Link Driver OCTOK16
       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
#Madge Token Ring
Link Driver MADGEODI
       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

# eof # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
```

Troubleshooting

Make sure your system is running the latest version of the following ODI drivers:

- LSL
- IPXODI
- NE2000
- 3C509
- TOKEN
- LANSUP

If you are not running the latest version of the drivers, then get them from CompuServe (GO NOVLIB) or use FTP to retrieve them from FTP.NOVEL.COM.

Help

Using Help

To choose a Help topic:

Mouse	Point to the underlined topic you want to view and click the mouse button. When the pointer is over an item you can choose, the pointer changes to a hand icon.
Keyboard	Press Tab to move the highlight to the underlined topic you want to view, and then press Enter.

To exit Help:

Mouse	1 Point to the **File** menu and click the mouse button. 2 Click the **Exit** command.
Keyboard	1 Press **Alt.** 2 Type the letter **F.** 3 Type the letter **X.**

About

Information about the program etc.

1. Choose OK to continue.

Network Addresses

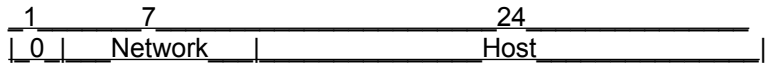
The official description of Internet addresses is RFC1020, Internet Numbers. The DDN Network Information Center (NIC) at SRI International in Menlo Park, California, maintains and distributes the RFC documents. The NIC also assigns Internet addresses and network numbers. When an organization applies to the NIC, the NIC assigns a network number or range of addresses that is appropriate to the number of host devices on the network.

The topics related to Internet addresses are listed below. To choose a topic from the list, click the underline topic you want information about.

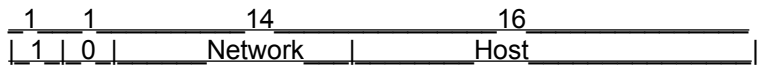
Classes of Internet Addresses

As described in RFC1020, Internet addresses are 32 bit quantities, divided into five classes. Each class differs in the number of bits allocated to the network and host portions of the address. For this discussion, consider a network to be a collection of computers(hosts) that have the same network field value in their Internet addresses.

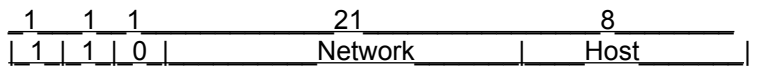
The **Class A** Internet address format allocates the highest eight bits to the network field and sets the highest priority bit to 0 (zero). The remaining 24 bits form the host field. Only 128 Class A networks can exist, but each Class A network can have almost 17 million hosts. The following figure illustrates the Class A format.



The **Class B** Internet address format allocates the highest 16 bits to the network field and sets the two highest-order bits to 1,0. The remaining 16 bits form the host field. Over 16,000 Class B networks can exist, and each Class B network can have up to 65,000 hosts. The following figure illustrates the Class B format.



The **Class C** Internet address format allocates the highest 24 bits to the network field and sets the three highest-order bits to 1,1,0. The remaining eight bits form the host field. Over two million Class C networks can exist, and each Class C network can have up to 255 hosts. The following figure illustrates the Class C format.



The **Class D** Internet address format for multicast groups, as discussed in RFC988. In Class D addresses, the four highest-order bits are set to 1,1,1,0.

The **Class E** Internet address is reserved for future use. In Class E addresses, the four highest order bits are set to 1,1,1,1. The router currently ignores Class D and Class E Internet addresses, except for the global broadcast address 255.255.255.255.

Internet Address Notation

Internet addresses are written as four 3-digit numbers separated by dots (Periods). Each number, written in decimal, represents an 8-bit octet. When strung together, the four octets form the 32-bit Internet address. This notation is called *dotted decimal*.

These examples show 32-bit values expressed as Internet addresses:

100.100.100.10
255.255.255.255
0.0.0.0
195.32.4.200

The largest possible value of a field in dotted-decimal number is 255, which represents an octet of all ones.

Allowable Internet Addresses

Some Internet addresses are reserved for special uses and be used for host, subnet, or network addresses. The following table lists ranges of Internet addresses and shows which addresses are reserved and which are available for use.

Reserved and Available Internet Addresses

Class	Address or Range	Status
A	0.0.0.0	Reserved
	1.0.0.0 through 126.0.0.0	Available
	127.0.0	Reserved
B	128.0.0.0	Reserved
	128.1.0.0 through 191.254.0.0	Available
	191.255.0.0	Reserved
C	192.0.0.0	Reserved
	192.0.1.0 through 223.255.254	Available
	223.255.255.0	Reserved
D,E	224.0.0.0 through 255.255.255.254	Reserved
	255.255.255.255	Broadcast

Internet Address Conventions

If the bits in the host portion of an address are all 0, that address refers to the network specified in the network portion of the address. For example, the Class C address 192.31.7.0 refers to a particular network.

Conversely, if the bits in the network portion of an address are all 0, that address refers to the host specified in the host portion of the address. For example, the Class B address 128.1.255.255 refers to all hosts on the 128.1.0.0 network. (Remember that an octet of zeros becomes the decimal number 255.)

Because of these conventions, do not use an Internet address with all zeros or all ones in the host portion for your router address.

Addresses and Routing

Consider a host sending an Internet data packet. If the destination host and sending host are on the same network, the packet goes directly to the destination host. If the destination host and sending host are on different networks, the packet goes to a router. Addresses make this routing and delivery of data packets possible.

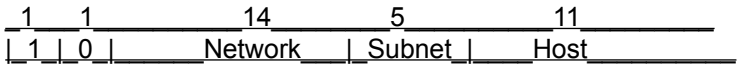
To determine whether the destination host is on the same network, the sending host compares the network portions of the destination address and its own address. If these network numbers are the same, the destination host is on the same network. If the network numbers are different, the destination host is on another network, and the data packet must go to a router.

A router has two or more network interfaces onto different networks. The primary function of the router is to direct packets between these networks, delivering them to their final destination or to another router. (A router-to-router transmission is called a hop.)

To begin the routing process, the router examines the network number of the destination address. Using this number as a key, the router locates applicable routing information in its routing table. The router uses this routing information to send the packet to its final or to an intermediate destination.

Subnetting

Subnetting is a scheme for imposing a simple hierarchy on hosts on a single physical network. The usual practice is to use the first few bits in the host portion of the network addresses for a subnet field. For example, the following figure shows a Class B address with five bits of the host portion used as a subnet field. The official description of subnetting is RFC950, *Internet Standard Subnetting Procedure*.



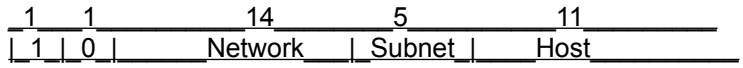
As with the host portion of an address, do not use all zeros or all ones in the subnet field.

Subnetting and Routing

Routers and hosts can use the subnet field for routing. The rules for routing on subnets are identical to the rules for routing on networks. However, correct routing requires all subnets of a network to be physically contiguous. In other words, the network must be set up so that it does not require traffic between any two subnets to cross another network. Also, RFC950 implicitly requires that all subnets of a network have the same number of bits in the subnet field.

Subnet Masks

A subnet mask identifies the subnet field of a network address. This mask is a 32-bit Internet address written in dotted-decimal notation with all ones in the network and subnet portions of the address. For the example in the following figure, the subnet mask is 255.255.248.0



The following table shows the subnet masks you can use to divide an octet into subnet and host fields. The subnet field can consist of any number of the host field bits; you do not need to use multiples of eight. However, you should use three or more bits for the subnet field-a subnet field of two bits yields only four subnets,two of which are reserved(the 1,1 and 0,0 values).

Subnet Masks

Subnet Bits	Host Bits	Hex Mask	Decimal Mask
0	8	0	0
1	7	0x80	128
2	6	0xC0	192
3	5	0xE0	224
4	4	0xF0	240
5	3	0xF8	248
6	2	0xFC	252
7	1	0xFE	254
8	0	0xFF	255

_____Port Options

Baud Rate: Specify the transfer rate of the two modems. Some modems can transmit at more than one baud rate, so check your hardware manual and select one that both systems can handle.

Data Bits: Specify the number of data bits in the data packets sent between the two computers.
Parity: Specify the parity type. If you selected 8 data bits in the previous option, select None now.

Mark parity means that parity is always on.

Space parity means that parity is always off.

Odd parity means the sum of the data bits is odd.

Even parity means the sum of the data bits is even.

Carrier Detect: Use the modem signal to detect a carrier signal. When carrier detect is selected, SLIP uses the carrier detect signal to determine whether the modem is on line. When carrier detect is off, SLIP looks at the modem response string to determine if it is connected. If your modem still isn't connecting after correctly setting the other options, clear this check box to use SLIP's method and try connecting again.

Parity Check: See the byte in which a parity error was encountered. Otherwise, you will see question marks (?) where the modem detected an error. The question marks will appear at every character not transferred correctly.

Connector: Select the communications port your modem uses. If you're using a null modem, select None.

Stop Bits: Specify the time between transmitted characters. Stop bits are not actually bits; they're the timing unit between characters.

Flow Control: Tell Terminal what to do if the buffer becomes too full to receive more data from the remote system.

XON/XOFF causes your system to pause when the buffer fills. While this method (known as software handshaking) is the standard method for most systems, it cannot be used with a remote system that is configured for hardware handshaking.

Select Hardware if the remote system uses the hardware method. Select None if the remote system uses no overflow method. Select XON/XOFF if you don't know what flow control method is used.