1 Introduction

This User Guide will show you how to set up the Neobit 1012VAADSL Bridge/Router, and how to customize its configuration to get the most out of your new product.

Features

- Internal ADSL modem for high-speed Internet access
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- Network address translation (NAT), Firewall, and IP filtering functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Relay
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- Configuration program you access via an HTML browser

System Requirement

In order to use the Neobit 1012VAADSL/Ethernet router, you must have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card (NIC)
- An Ethernet hub/switch, if you are connecting the device to more than one computer on an Ethernet network.
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later

Using this Document

Notational conventions

- Acronyms are defined the first time they appear in text and in the glossary (Appendix D).
- For brevity, the Neobit 1012VAis referred to as "the router."
- The terms *LAN* and *network* are used interchangeably to refer to a group of Ethernet-connected computers at one site.

Typographical conventions

- *Italics* are used to identify terms that are defined in the glossary (Appendix D).
- **Bolded** text is used for items you select from menus and drop-down list, and text strings you type when prompted by the program.

Getting Support

Customer support provides a variety of options for obtaining information about Netus products and services, software upgrades, and technical assistance.

You can obtain technical assistant by telephone, email, fax, or regular mail as well as over the Internet.

Enabling Netus to assist you

If you need to contact Netus for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model
- Software and hardware options
- Software version
- Whether you are routing or bridging with your Netus product.
- Type of computer you are using
- Description of the problem

Following is the ways in which you can reach Customer Service.

- Website : www.netustech.com
- Email : administrator@netustech.com
- Hot line : +82-31-622-6600
- Fax : +82-31-622-6601

2 Getting to Know the Neobit 1012VA

Parts Check

In addition to this document, Neobit 1012VAshould arrive with the following:

- Neobit 1012VAADSL Ethernet Bridge/Router
- Power adapter and power cord
- Ethernet cable (“straight-through” type)
- Standard phone/DSL line cable

Modem

Tel Line Cable

Power Adaptor

Lan Cable RJ45, Straight.

Manual

. Neobit 1012VAADSL/Ethernet Router Package Contents

Front Panel

The front panel contains lights called LEDs that indicate the status of the unit

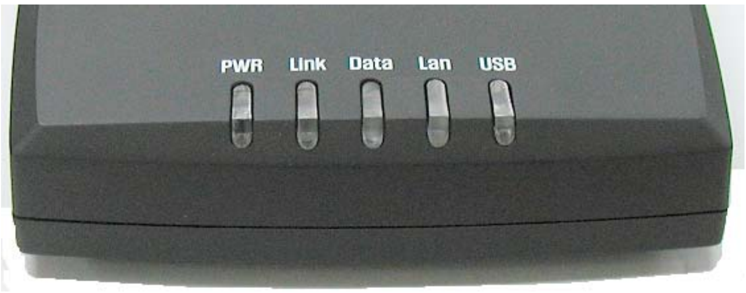


Figure 1. Front Panel and LEDs

Label	Color	Status	Function
PWR	Green	On	Unit is powered on
Link	Green	On	Modem is physically connected to ISP
		Blinking	Physical connecting status between modem and ISP
Data	Green	Blinking	Current data receiving/transmitting status
LAN	Green	On	Physical Ethernet connecting status between PC and modem

***Options**

USB	Green	On	Physical USB connecting status between PC and modem

Rear Panel

The rear panel contains the ports for the unit's data and power connections.

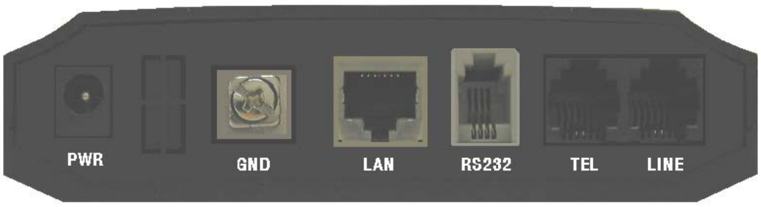


Figure 1. Rear Panel Connections

Label	Function
PWR	Connects to the supplied power converter cable
GND	Connect to Electric Earth
LAN (Ethernet)	Connects the device to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the cable provided
RS-232 (Console)	Connects the device to PC with serial cable for device management
TEL (Phone)	Provides an optional connection to your telephone
LINE (DSL)	Connects the device to a telephone jack for DSL communication
**** Right Side***	
SW (On Off)	Switches the unit "On" and "off"

3 Quick Start

This Quick Start provides basic instructions for connecting the Neobit 1012VAto a computer or LAN and to the Internet.

- Part 1 describes setting up the hardware.
- Part 2 describes how to configure Internet properties on your computer(s).
- Part 3 shows you how to configure basic settings on the Neobit 1012VAto get your LAN connected to the Internet.

After setting up and configuring the device, you can follow the instructions on page 25 to verify that it is working properly.

This Quick Start assumes that you have already established ADSL service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Part 1 — Connecting the Hardware

In Part 1, you connect the device to the phone jack, the power outlet, and your computer or network.

WARNING

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and the Neobit 1012VA.*

Figure 2 illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

Neobit 1012VAE ADSL Ethernet Router

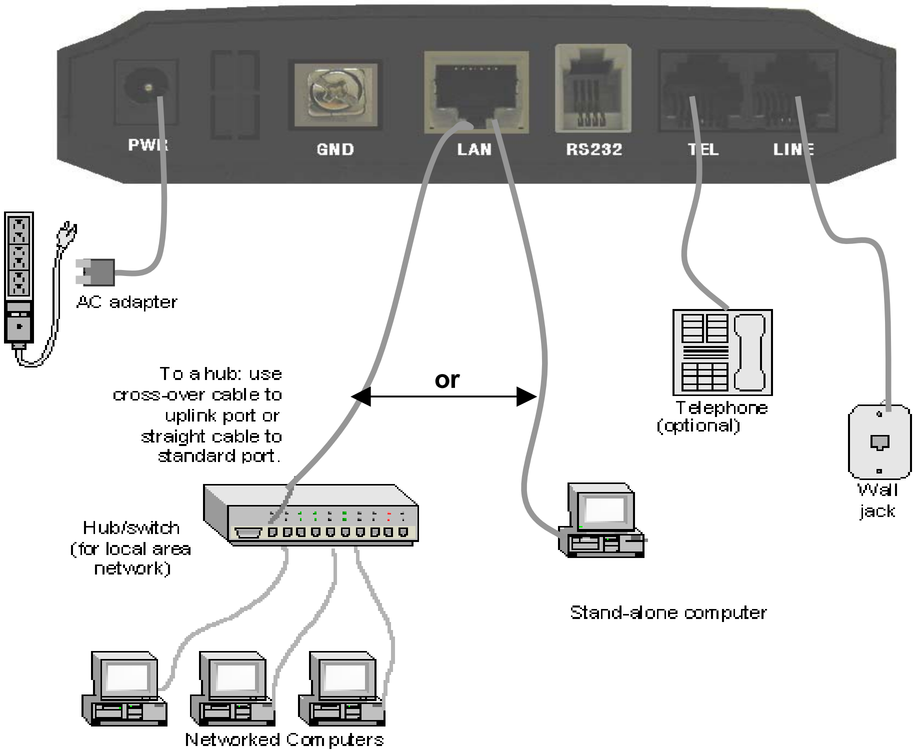

PWR
GND
LAN
RS232
TEL
LINE
AC adapter
To a hub: use cross-over cable to uplink port or straight cable to standard port.
or
Telephone (optional)
Wall jack
Hub/switch (for local area network)
Stand-alone computer
Networked Computers

Figure 2. Overview of Hardware Connections

Step 1. Connect the ADSL cable and optional telephone.

Connect one end of the provided phone cable to the port labeled ADSL on the rear panel of the device. Connect the other end to your wall phone jack.

You can attach a telephone line to the device. This is helpful when the ADSL line uses the only convenient wall phone jack. If desired, connect the telephone cable to the port labeled PHONE.

WARNING

*Although you use the same type of cable, The ADSL and PHONE ports are **not** interchangeable. Do not route the ADSL connection through the PHONE port.*

Step 2. Connect the Ethernet cable.

If you are connecting a LAN to the Neobit 1012VAADSL/Ethernet router, attach one end of a provided Ethernet cable to a regular hub port and the other to the Ethernet port on the Neobit 1012VA.

If you are using the Neobit 1012VAwith a single computer and no hub, you must use a "crossover" Ethernet cable (not provided) to attach the PC directly to the device. The crossover cable is wired differently than the cable you would use to connect to a hub. When you compare the colored wires on each end of a straight-through cable, they will be in the same sequence; on crossover cables, they will not. Contact your ISP for assistance.

Step 3. Attach the power connector

Connect the AC power adapter to the PWR connector on the back of the device and plug in the adapter to a wall outlet or power strip.

Step 4. Turn on the Neobit 1012VAand power up your systems.

Press the Power switch on the back panel of the device to the ON position.

Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Part 2 — Configuring Your Computers

Part 2 of the Quick Start provides instructions for configuring the Internet settings on your computers to work with the Neobit 1012VA.

Before you begin

By default, the Neobit 1012VAautomatically assigns all required Internet settings to your PCs. You need only to configure the PCs to accept the information when it is assigned.

Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the Neobit 1012VAto do so. See "Assigning static Internet information to your PCs" on page 21 for instructions.

- If you have connected your PC of LAN via Ethernet to the Neobit 1012VA, follow the instructions that correspond to the operating system installed on your PC.

Windows® XP PCs:

1. In the Windows task bar, click the Start button, and then click **Control Panel**.
2. Double-click the Network Connections icon.
3. In the LAN or High-Speed Internet window, right-click on icon corresponding to your network interface card (NIC) and select **Properties**. (Often this icon is labeled *Local Area Connection*).

   The Local Area Connection dialog box displays with a list of currently installed network items.
4. Ensure that the check box to the left of the item labeled Internet Protocol TCP/IP is checked, and click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
6. Click OK twice to confirm your changes, and close the Control Panel.

Windows 2000 PCs:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.

   The Local Area Connection Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click Install... .
5. In the Select Network Component Type dialog box, select **Protocol**, and then click Add... .
6. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click OK .

   You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
7. If prompted, click OK to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Neobit 1012VA:

8. In the Control Panel, double-click the Network and Dial-up Connections icon.
9. In Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.
10. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click Properties .
11. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
12. Click OK twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.

   The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click Add... .
5. In the Select Network Component Type dialog box, select **Protocol**, and then click Add... .
6. Select **Microsoft** in the Manufacturers box.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click OK .

   You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
8. If prompted, click OK to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Neobit 1012VA:

9. In the Control Panel, double-click the Network and Dial-up Connections icon.
10. In Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
11. In the Network Properties dialog box, select **TCP/IP**, and then click Properties .
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server assigned IP address**. Also click the radio button labeled **Server assigned name server address**.
13. Click OK twice to confirm and save your changes, and then close the Control Panel.

Windows 95, 98 PCs:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network icon.

   The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.
3. If TCP/IP does not display as an installed component, click Add... .

   The Select Network Component Type dialog box displays.
4. Select **Protocol**, and then click Add... .

   The Select Network Protocol dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click OK to return to the Network dialog box, and then click OK again.

   You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click OK to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the Neobit 1012VA:

8. Open the Control Panel window, and then click the Network icon.
9. Select the network component labeled TCP/IP, and then click Properties .

   If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
10. In the TCP/IP Properties dialog box, click the IP Address tab.
11. Click the radio button labeled **Obtain an IP address automatically**.
12. Click the DNS Configuration tab, and then click the radio button labeled **Obtain an IP address automatically**.
13. Click OK twice to confirm and save your changes.

    You will be prompted to restart Windows.
14. Click Yes .

Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double click the Network icon.
3. In the Network dialog box, click the Protocols tab.

   The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.
4. If TCP/IP does not display as an installed component, click Add... .
5. In the Select Network Protocol dialog box, select **TCP/IP**, and then click OK .

   You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

   After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
6. Click Yes to continue, and then click OK if prompted to restart your computer.

Next, configure the PCs to accept IP information assigned by the Neobit 1012VA:

7. Open the Control Panel window, and then double-click the Network icon.
8. In the Network dialog box, click the Protocols tab.
9. In the Protocols tab, select **TCP/IP**, and then click Properties .
10. In the Microsoft TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
11. Click OK twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

In some cases, you may want to assign Internet information to some or all of your PCs directly (often called "statically"), rather than allowing the Neobit 1012VAto assign it. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN (subnets are described in Appendix A).

Before you begin, contact your ISP if you do not already have the following information:

- The IP address and subnet mask to be assigned to each PC to which you will be assigning static IP information.
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the Neobit 1012VA. By default, the LAN port is assigned this IP address: **192.168.1.1**. (You can change this number, or another number can be assigned by your ISP. See Chapter 5 for more information.)
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions on pages 16 through 20 relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server, and default gateway, click the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place them in the same subnet as the Neobit 1012VA's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Chapter 5 to change the LAN port IP address accordingly.

Part 3 — Configuring the Neobit 1012VA

In Part 3, you log into the program on the Neobit 1012VAand configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.

Logging in to the Neobit 1012VAQuick Configuration Page

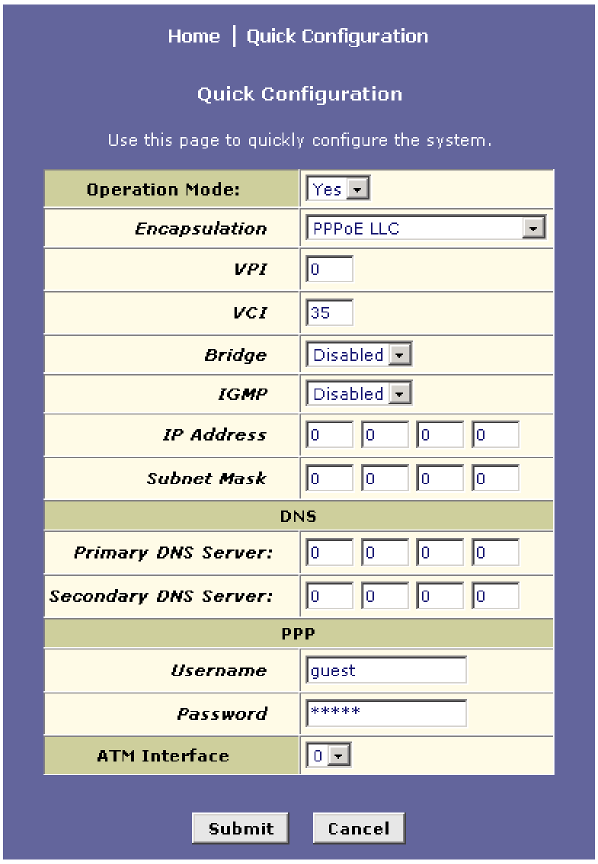
The Neobit 1012VAprovides a preinstalled software program called Configuration Manager which enables you to configure the operation of the device via your Web browser. The settings that you are most likely to need to change before using the device are grouped onto a single Quick Configuration page.

Follow these instructions configure the device settings:

1. At any PC connected to the Neobit 1012VAvia Ethernet, open your Web browser, and type the following URL in the address/location box:

   192.168.1.1/setup

   When you press <Return>, the page shown in Figure 3 should display (see Appendix C, "Troubleshooting," if you receive an error message or the page does not display).



Quick Configuration

Use this page to quickly configure the system.

Operation Mode:	Yes
Encapsulation	PPPoE LLC
VPI	0
VCI	35
Bridge	Disabled
IGMP	Disabled
IP Address	0 0 0 0
Subnet Mask	0 0 0 0
DNS	
Primary DNS Server:	0 0 0 0
Secondary DNS Server:	0 0 0 0
PPP	
Username	guest
Password	*****
ATM Interface	0

Figure 3. Quick Configuration Page in Configuration Manager

The fields are described in the following table. Consult with your ISP to determine which settings you need to change.

Field	Description
Operation Mode	This setting enables or disables the Neobit 1012VA. When set to "No", the device cannot be used to provide Internet connectivity for your network. Set it to "Yes" now, if necessary.
Encapsulation	This setting determines the type of data link your ISP uses to communicate with your ADSL/Ethernet router. Contact them to determine the appropriate setting.
VCI and VPI	These values are provided by your ISP and determine the unique path your connection uses to communicate with your ISP.
Bridge	This setting enables or disables bridging between the Neobit 1012VAand your ISP. Your ISPs may also refer to this using "RFC 1483" or "Ethernet over ATM".
IGMP	This setting enables or disables the Internet Group Management Protocol, which some ISPs use to perform remote configuration of your device.
IP Address and *Subnet Mask*	If your ISP has assigned a public IP address to your LAN, enter the address and the associated subnet mask in the boxes provided. (Note: in some configurations, the public IP address should be entered on your PC rather than on the ADSL/Ethernet router; check with your ISP.)
Primary/ Secondary DNS Server	Enter the Primary and Secondary DNS addresses provided by your ISP. If you selected *Auto Discovery + User Configured*, you are not required to enter addresses here; they will be used in addition to any addresses discovered automatically.
User Name and *Password*	Enter the username and password you use to log in to your ISP. (Note: this is different from the information you used to log in to Configuration Manager.)
ATM Interface	Select the ATM interface you want to use (usually atm-0). You system may be configured with more than one ATM interface if you are using different types of services with your ISP.

2. When finished customizing these settings, click Submit.

   The settings are now in effect; however, if you reboot or if the power is disconnected, your settings will be lost. In step 3, you save the changes to permanent memory:

3. Click the Admin tab that displays in the upper right of the page, and then click **Commit & Reboot** in the task bar.

4. Click Commit.

   A page will display briefly to confirm your changes, and then you will be returned to the Commit & Reboot page.

You are now finished customizing basic settings. Read the following section to determine if you need to change additional settings.

Default Router Settings

In addition to handling the DSL connection to your ISP, the Neobit 1012VAADSL/Ethernet router can provide a variety of services to your network. The device is pre configured with default settings for use with a typical home or small office network.

Table 1 lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review the settings in Table 1 to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

Before you modifying any settings, review Chapter 4 for general information about accessing and using the Configuration Manager program. We strongly recommend that you contact your ISP prior to changing the default configuration.

Table 1. Default Settings Summary

Option	Default Setting	Explanation/Instructions
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.3 through 192.168.1.20	The Neobit 1012VAmaintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in Part 2 of the Quick Start. See Chapter 7 for an explanation of the DHCP service.
NAT (Network Address Translation)	napt rule enabled	Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever they access the Internet. See Chapter 8 for a description of the NAT service.
LAN Port IP Address	Static IP address: 192.168.1.1 subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See Chapter 5 for instructions.

Testing Your Setup

The Quick Start process should enable any computer on your LAN to use the Neobit 1012VA's ADSL connection to access the Internet.

To test the connection, turn on the device, wait about 30 seconds, and then verify that its LEDs are illuminated as shown in Table 2.

Table 2. LED Indicators

This LED:	...should be:
PWR	Solid green to indicate that the device is turned on. If this light is not on, check the power cable attachment.
Sync	Flashing on/off while the device is booting. After about 10-15 seconds, it should turn off.
LAN	Solid green to indicate that the device can communicate with your LAN.
DSL	Solid green to indicate that the device has successfully established a connection with your ISP.
Data	Flashing when the device is sending or receiving data from the Internet. It may be unlit, flashing, or appear solid depending on the current activity.

If the LEDs illuminate as expected, test your Internet connection from a LAN computer:

Open your web browser, and type the URL of any external website (such as *http://www.yahoo.com*). The LED labeled WAN ACT should be blinking rapidly and may appear solid as the device connects to the site.

If the LEDs do not illuminate as expected or the web page does not display, see Appendix C for troubleshooting suggestions. Or, contact your ISP for assistance.

4 Getting Started with the Configuration Manager

The Neobit 1012VAincludes a preinstalled program called the *Configuration Manager*, which provides an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You access it through your web browser from any PC connected to the Neobit 1012VAvia the LAN port.

This chapter describes how to use the Configuration Manager.

Accessing the Configuration Manager

The Configuration Manager program is preinstalled into memory on the Neobit 1012VA. To access the program, you need the following:

- A PC or laptop connected to the LAN port on the device as described in the Quick Start chapter.
- A web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions.

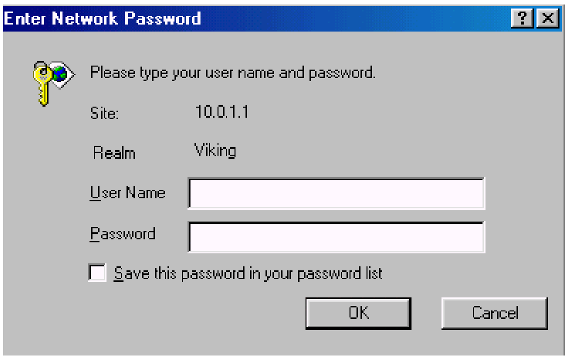
You can access the program from any computer connected to the Neobit 1012VAvia the LAN ports.

1. From a LAN computer, open your web browser, type the following URL in the web address (or location) box, and press **<Enter>**:

   `http://192.168.1.1`

   These are the predefined IP addresses for the LAN port on the Neobit 1012VA.

   A login screen displays, as shown in Figure 4.



Enter Network Password
?
Please type your user name and password.
Site: 10.0.1.1
Realm Viking
User Name
Password
□ Save this password in your password list
OK
Cancel

Figure 4. Login Screen

Note

In some pictures in this manual, there might be different from the real pictures which you are seeing as above. In the figure 4, the right value is not 192.168.1.1 but 192.168.1.1. You should refer to the texts prior to the figures. The revised manual will be released soon at the directory "Tech Info" of "Service" in

our website (www.netustech.com). For further information, please email us to administrator@netustech.com.

2. Enter your user name and password, and then click OK.

   The first time you log into the program, use these defaults:

Default User Name:	root
Default Password	root

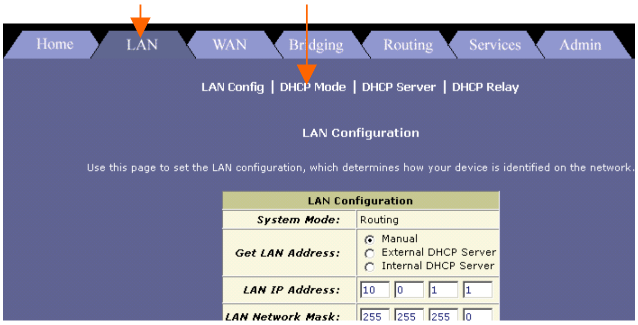
Note

You can change the password at any time (see Changing Your Login Password on page 32). The user name cannot be changed.

The System View page on the Home tab displays each time you log into the program (shown in Figure 5 on page 29).

Functional Layout

Configuration Manager tasks are grouped into categories, which you can access by clicking the tabs at the top of each page. Each tab displays the available tasks horizontally the top of the page. You can click on these to display the specific configuration options.



LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration	
System Mode:	Routing
Get LAN Address:	● Manual ○ External DHCP Server ○ Internal DHCP Server
LAN IP Address:	10 . 0 . 1 . 1
LAN Network Mask:	255 . 255 . 255 . 0

A separate page displays for each task in the task bar. The left-most task displays by default when you click on a new tab. The same task may appear in more than one tab, when appropriate. For example, the Lan Config task displays in both the LAN tab and the Routing tab.

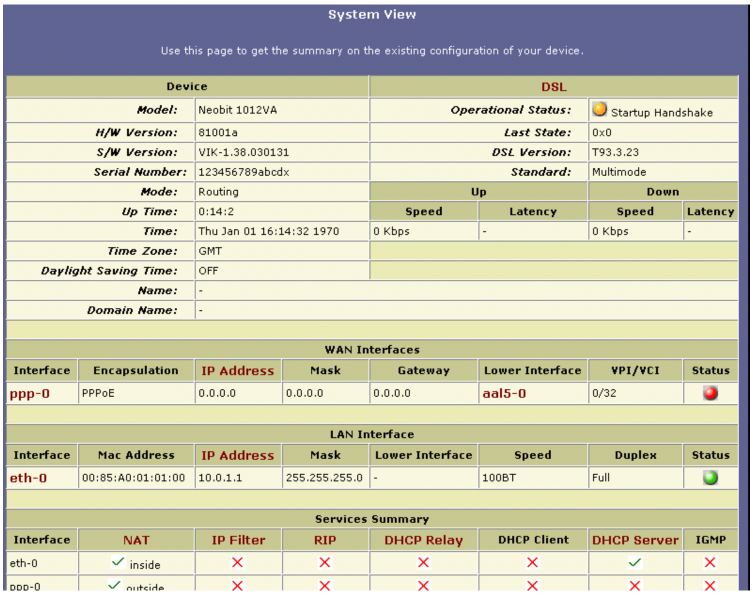
Commonly used buttons

The following buttons are used throughout the application.

Button	Function
Submit	Stores in *temporary* system memory any changes you have made on the current page. See "Committing your changes" on page 33 for instructions on storing changes permanently.
Refresh	Redisplays the current page with updated statistics or settings.
Clear	On pages that display accumulated statistics, this button resets the statistics to their initial values.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.

The Home Tab and System View Table

The System View page displays when you first access the program. This page is one of two options available in the Home tab (the other is the Quick Start page, as described on page 22).



System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL			
Model:	Neobit 1012VA	Operational Status:	● Startup Handshake		
H/W Version:	81001a	Last State:	0x0		
S/W Version:	VIK-1.38.030131	DSL Version:	T93.3.23		
Serial Number:	123456789abcdx	Standard:	Multimode		
Mode:	Routing	Up		Down	
Up Time:	0:14:2	Speed	Latency	Speed	Latency
Time:	Thu Jan 01 16:14:32 1970	0 Kbps	-	0 Kbps	-
Time Zone:	GMT				
Daylight Saving Time:	OFF				
Name:	-				
Domain Name:	-				

WAN Interfaces

Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
ppp-0	PPPoE	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	0/32	●

LAN Interface

Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:85:A0:01:01:00	10.0.1.1	255.255.255.0	-	100BT	Full	●

Services Summary

Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✗	✗	✗	✗	✓	✗
ppp-0	✓ outside	✗	✗	✗	✗	✗	✗

Figure 5. System View Page

The System View table provides a snapshot of your system configuration, and provides links to the software pages that enable you to configure each setting (if available). The following table describes each section of the system view table.

Table Heading	Description
Device	Displays basic information about the Neobit 1012VAhardware and software versions, the system uptime (since the last reboot), and the pre configured operating mode.
DSL	Displays performance statistics for the DSL line. You can click **DSL** in WAN tab to display additional DSL settings, which are described in Chapter 14.
WAN Interfaces	Displays the software name(s) and various settings for the device interfaces that communicate with your ISP via DSL. Although you only have one physical DSL port, multiple software-defined interfaces can be configured to use it. See the ATM VCC, PPP, EOA, and IPoA chapters (Chapters 12, 13, 14, and 10, respectively) for more information about the interfaces defined on your system.

Table Heading	Description
LAN Interfaces	Displays the software names and various settings for the device interfaces that communicate directly with your network. These typically include an Ethernet interface named *eth-0.* For information on modifying properties of these interfaces, see Chapter 5.
Services Summary	Displays the following services that the Neobit 1012VAperforms to help you manage your network: o Translating private IP addresses to your public IP address (NAT, see Chapter 8). o Setting up filtering rules that accept or deny incoming or outgoing data. (IP Filter, see Chapter 18). o Enabling router-to-router communication (RIP, see Chapter 9). o Dynamic assignment or receipt of IP information (DHCP, see Chapter 7). o Message forwarding based on Internet Group assignment (IGMP, not configurable).

Changing Your Login Password

The first time you log into the Configuration Manager, you use the default user ID and password (*root* and *root*). The system allows only one user ID and password. Only the password can be changed.

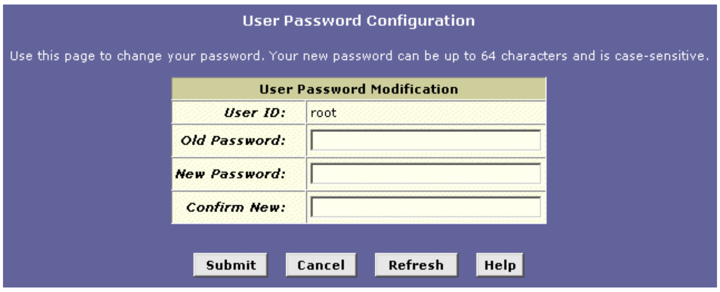
Note

This user ID and password is only used for logging into the Configuration Manager; it is not the same as the login you may use to connect to your ISP (described in Chapter 12).

To change the Configuration Manager login password:

1. Click the Admin tab.

   The User Password Configuration page displays by default.



User Password Configuration

Use this page to change your password. Your new password can be up to 64 characters and is case-sensitive.

User Password Modification	
User ID:	root
Old Password:	
New Password:	
Confirm New:	

Figure 6. User Password Configuration Page

2. Type your current password in the Old Password text box.
3. Type the new password in the New Password text box and again in the Confirm New text box.

   The password can be up to eight ASCII characters long. When logging in, you must type the new password in the same upper and lower case characters that you use here.
4. Click Submit.
5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
6. Click Commit to save your changes to permanent memory.

Committing Your Changes and Rebooting the Device

Committing your changes

Whenever you use the Configuration Manager to change system settings, the changes are initially placed in temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

To save your changes for future use, you can use the commit function. This function saves your changes from RAM to permanent storage (called flash memory).

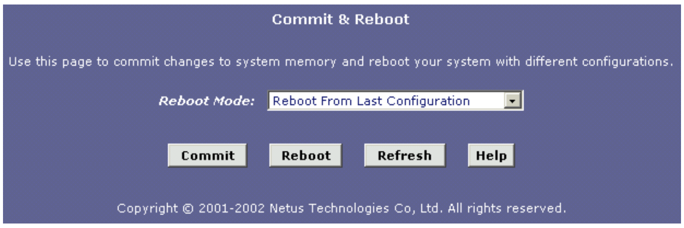
Note

***Submitting** changes activates them immediately, but saves them only until the device is reset or powered down. **Committing** changes saves them permanently.*

Follow these steps to commit changes to permanent storage.

1. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

   The Commit & Reboot page displays:



Commit & Reboot

Use this page to commit changes to system memory and reboot your system with different configurations.

Reboot Mode: Reboot From Last Configuration

Copyright © 2001-2002 Netus Technologies Co, Ltd. All rights reserved.

Figure 7. Commit & Reboot Page

2. Click **Commit**. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.)

   The changes are saved to permanent storage.

   The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly (see the rebooting instructions on page 34).

Rebooting the device using Configuration Manager

To reboot the device, display the Commit & Reboot page, select the appropriate reboot mode from the drop-down menu, and then click

.

You can select from the following three options when rebooting:

Option	Description
Reboot from Last Configuration	Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Backup Configuration	Reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Default Configuration	Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.

WARNING

Do not reboot the device using the Reset button on the back panel of the Neobit 1012VAto activate new changes. This button resets the device settings to the manufacturer's default values. Any custom settings will be lost.

5 Setting IP Properties for the LAN-side Interfaces

This chapter describes how to configure IP properties the interfaces on the ADSL/Ethernet router that communicate with your LAN computer.

Configuring the LAN IP Address

The LAN IP address identifies the LAN port (eth-0 as a node on your network; that is, its IP address must be in the same subnet as the PCs on your LAN.

Definition

*A **network node** can be thought of as any interface where a device connects to the network, such as the Neobit 1012VA's LAN port and the network interface cards on your PCs. See Appendix A for an explanation of subnets.*

You can change the default to reflect the set of IP addresses that you want to use with your network.

If your network uses a DHCP server (other than the ADSL/Ethernet router) to assign IP addresses, you can configure the device to accept and use a LAN IP address assigned by that server. Similarly, if your ISP performs DHCP serving for your network, you can configure the device to accept an IP address assigned from the ISP's server. In this mode, the ADSL/Ethernet router is considered a *DHCP client* of your (or your ISP's) DHCP server.

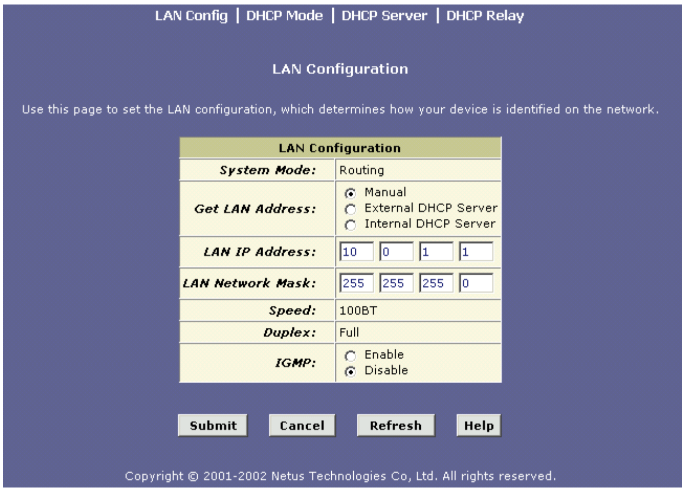
Note

*The Neobit 1012VAitself can function as a DHCP server for your LAN computers, as described in Chapter 5, **but not for its own LAN port**.*

Follow these steps to change the default LAN IP address or to configure the LAN port as a DHCP client.

1. Log into Configuration Manager, and then click the LAN tab.

   The LAN Configuration page displays, as shown in Figure 8.



LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration	
System Mode:	Routing
Get LAN Address:	● Manual ○ External DHCP Server ○ Internal DHCP Server
LAN IP Address:	10 0 1 1
LAN Network Mask:	255 255 255 0
Speed:	100BT
Duplex:	Full
IGMP:	○ Enable ● Disable

Copyright © 2001-2002 Netus Technologies Co, Ltd. All rights reserved.

Figure 8. LAN Configuration Page

The LAN Configuration table displays the following settings:

Setting	Description
System Mode	The pre-configured mode for your device, such as Routing or Bridging mode. This setting is not user - configurable.
LAN IP Address	The IP address your computers use to identify the device's LAN port. Note that the public IP address assigned to you by your ISP **is not** your LAN IP address. The public IP address identifies the WAN (ADSL) port on your ADSL/Ethernet router to the Internet.
LAN Network Mask	The LAN Network mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network. Your device is pre configured with a default network mask of 255.255.255.0.
Use DHCP	Use this setting if you want device to accept LAN IP information assigned dynamically from another DHCP server. If the server is on your network, click *Local*. If the server is on your ISP's network, click *Remote*. The Neobit 1012VAcannot act as a DHCP server for its own LAN port.

2. Enter a LAN IP address and network mask, or click the DHCP **Enable** radio button.

   ▶ **Entering a fixed address:** If you are using routing services on you LAN such as DHCP and NAT, you will want to assign a fixed LAN IP address and mask. This ensures that your LAN computers have a fixed address that they use to communicate with the device.

   The IP address you assign must be on the same subnet as your LAN computers that connect to this port (that is, the network ID portion of their IP addresses and their subnet masks must be the same). See Appendix A for an explanation of IP addresses and network masks.

   You may need to update the DHCP configuration so that the addresses that the DHCP server dynamically assigns to your computers are on the same subnet as the new LAN IP address. See Chapter 7 for instructions on changing the pool of dynamically assigned addresses. In addition, if you change the DHCP pool, you will also need to update the NAT configuration so the new IP addresses are translated properly. See Chapter 8 for instructions on NAT.

   ▶ **Enabling DHCP:** If another computer on your LAN provides DHCP services for your network, you can click the Use DHCP checkbox to enable the LAN port to accept a dynamically assigned address from the server.

   When you click the Enable radio button, the LAN Network Mask field will be dimmed (made unavailable for entry). The LAN IP Address field will remain editable, however. The address that you specify here will be used as a requested IP address from the DHCP server. This is referred to as a "Configured IP Address" in the program. If the configured IP address is not available from the DHCP server, the server will distribute another address to the LAN port. Even if another number is assigned, the same configured IP address will continue to display in this field.

For a description of how DHCP works, see Chapter 7.

3. Click Submit.
    - If you were using an Ethernet connection for the current session, and changed the IP address, the connection will be terminated.
    - If you enabled the DHCP service, the ADSL/Ethernet router will initiate a request for an IP address from your LAN's DHCP server. Assuming a different IP address is assigned, your current connection will be terminated.
4. Reconfigure your PCs, if necessary, so that their IP addresses place them in the same subnet as the new IP address of the LAN port. See the Quick Start chapter, "Part 2 — Configuring Your Computers," for instructions.
5. Log into Configuration Manager by typing the new IP address in your Web browser's address/location box.

    If you enabled DHCP, you may need to check the DHCP server on your LAN to determine the IP address actually assigned to the LAN port.
6. If the new settings work properly click the Admin tab, and then click **Commit & Reboot** in the task bar.
7. Click Commit to save your changes to permanent memory.

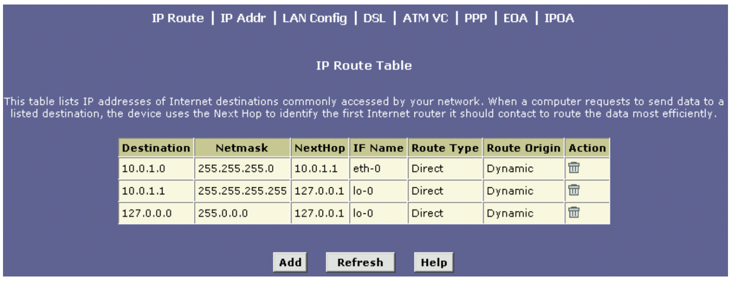
6 Viewing System IP Information and Performance Statistics

The interfaces on the Neobit 1012VAthat communicate with other network and Internet devices are identified by unique Internet protocol (IP) addresses. You can use the Configuration Manager to view the list of IP addresses that your device uses, and to view other system and network performance data.

See Appendix A for a description of IP addresses and masks.

Viewing the Neobit 1012VA's IP addresses

To view the Neobit 1012VA's IP addresses, click the Routing tab, and then click **IP Addr** in the task bar. The IP Address Table page displays, as shown in Figure 9:


IP Route | IP Addr | LAN Config | DSL | ATM VC | PPP | EOA | IPOA
Add
Refresh
Help

IP Route Table

This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently.

Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
10.0.1.0	255.255.255.0	10.0.1.1	eth-0	Direct	Dynamic	🗑
10.0.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	🗑
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	🗑

Figure 9. IP Address Table Page

The table lists the IP addresses, network masks ("Net Mask"), and interface names ("IF Name") for each of its IP-enabled interfaces.

The listed IP addresses may include:

- The IP address of the device's LAN (Ethernet) port, called *eth-0*. See Chapter 5 for instructions on configuring this address.
- The IP address of the WAN (ADSL line) interface, which your ISP and other external devices use to identify your network. It may be identified in the Configuration Manager by the names *ppp-0* or *eoa-0*, or *ipoa-0*, depending on the protocol your device uses to communicate with your ISP. Your ISP may assign the same address each time, or it may change each time you reconnect.
- The "loop back" IP address, named *lo-0*, of 127.0.0.1. This special address enables the device to keep any data addressed directly to it, rather than route the data through the WAN or LAN ports.

If your device has additional IP-enabled interfaces, the IP addresses of these will also display

7 Configuring Dynamic Host Configuration Protocol

You can configure your network and Neobit 1012VAto use the Dynamic Host Configuration Protocol (DHCP). This chapter provides an overview of DHCP and instructions for implementing it on your network.

Overview of DHCP

What is DHCP?

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device — such as the Neobit 1012VAor a router located with your ISP — to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a *DHCP server*, and the receiving device is a *DHCP client*.

Note

> *If you used the Quick Start instructions, you either configured each LAN PC with an IP address, or you specified that it will receive IP information dynamically (automatically). If you chose to have the information assigned dynamically, then you configured your PCs as DHCP clients that will accept IP addresses assigned from a DCHP server such as the Neobit 1012VA.*

The DHCP server draws from a defined pool of IP addresses and “leases” them for a specified amount of time to your computers when they request an Internet session. It monitors, collects, and redistributes the addresses as needed.

On a DHCP-enabled network, the IP information is assigned *dynamically* rather than *statically* A DHCP client can be assigned a different address from the pool each time it reconnects to the network.

Why use DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from a central computer. Without DHCP, you would have to configure each computer separately with IP addresses and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated.

Neobit 1012VADHCP modes

The device can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP client.

- If you configure the device as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation service, so that the private addresses can be translated to your public IP address on the Internet. Both DHCP server and NAT are enabled in the default configuration.
- If your ISP performs the DCHP server function for your network, then you can configure the device as a DHCP relay agent. When the Neobit 1012VAreceives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.
- If you have another PC or device on your network that is already performing the DHCP server function, then you can configure the LAN port on the Neobit 1012VAto be a DHCP client of that server (as are your PCs). This configuration is not discussed in this chapter. See Chapter 5 for instructions.

Note

You can input settings for both DHCP server and DHCP relay mode, and then activate either mode at any time. De-activated settings are retained for your future use.

Configuring DHCP Server

Note

By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.1.3 through 192.168.1.20 (subnet mask 255.255.255.0). To change this range of addresses, see "Viewing, modifying, and deleting address pools" on page 46.

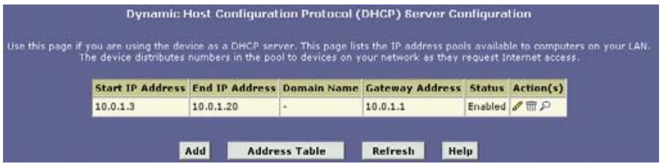
First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Open the Windows Control Panel and display the computer's Networking properties. Configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system). For detailed instructions, see the Quick Start chapter, "Part 2 — Configuring Your Computers."

Next, you define the pools of IP addresses you want to make available for distribution to your computers. These addresses can be multiple public addresses that you have purchased from your ISP, but are typically private addresses that you create. (LAN administrators often create private IP addresses for use only on their networks. See "Overview of NAT" on page 51.)

2. Log into Configuration Manager, click the LAN tab, and then click **DHCP Server** in the task bar.

   The DHCP Server Configuration page displays:



Dynamic Host Configuration Protocol (DHCP) Server Configuration

Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
10.0.1.3	10.0.1.20	-	10.0.1.1	Enabled	✎ 🗑 🔍

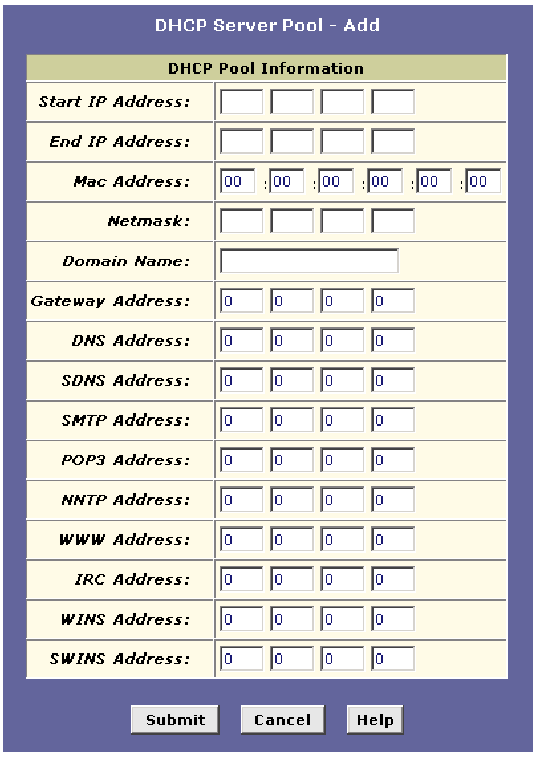
Figure 10. DHCP Configuration Page

   Each pool you create displays in a row on the table on this page.

   You can create up to eight pools; however, most users will need to create only one for their LAN

3. To add an IP address pool, click Add.

   The DHCP Server Pool – Add page displays.



DHCP Server Pool - Add

DHCP Pool Information

Start IP Address:	
End IP Address:	
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Netmask:	
Domain Name:	
Gateway Address:	0 0 0 0
DNS Address:	0 0 0 0
SDNS Address:	0 0 0 0
SMTP Address:	0 0 0 0
POP3 Address:	0 0 0 0
NNTP Address:	0 0 0 0
WWW Address:	0 0 0 0
IRC Address:	0 0 0 0
WINS Address:	0 0 0 0
SWINS Address:	0 0 0 0

Figure 11. DHCP Server Pool – Add Page

4. Enter the *Start IP Address*, *End IP Address*, *Net Mask*, and *Gateway Address* fields are required; the others are optional. The following table describes each field.

Field	Description
Start/End IP Addresses	Specify the lowest and highest addresses in the pool.
Mac Address	Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. (A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network.) If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.
Net Mask	Specifies which portion of each IP address in this range refers to the network and which portion refers to the host (computer). For a description of network masks and LAN network masks, see Appendix A. You can use the network mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (called a *subnet*).
Domain Name	A user-friendly name that refers to the group of computers (subnet) that will be assigned addresses from this pool.
Gateway Address	The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the IP address that the computers first contact to communicate with the Internet. Typically, it is the device's LAN port IP address. See "Hops and gateways" on page 74 for an explanation of gateway addresses.
DNS/SDNS Address	The IP address of the *Domain Name System* server and *Secondary Domain Name System* server to be used by computers that receive IP addresses from this pool. These DNS servers translate common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, these servers are located with your ISP.

Field	Description
SMTP...SWINS (optional)	The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as the SMTP, or *Simple Mail Transfer Protocol*, server which handles e-mail traffic). Contact your ISP for these addresses.

5. Click **Submit**.

   A confirmation page displays briefly to indicate that the pool has been added successfully. After a few seconds, the DHCP Server Pool – Add page displays with the newly added pool.

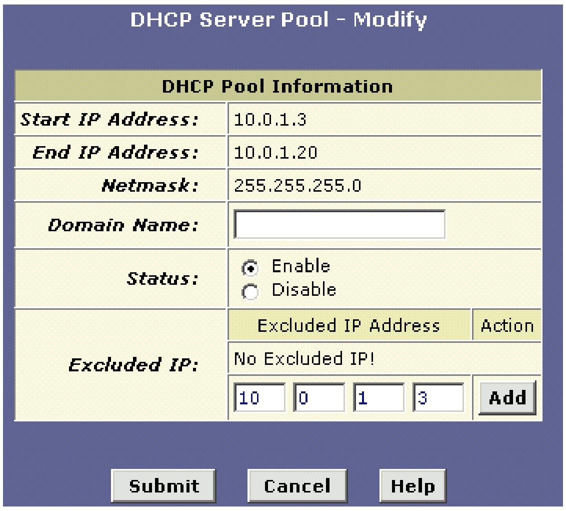
6. Follow the instructions in "Setting the DHCP Mode" on page 49 to set the DHCP mode to DHCP Server.

Viewing, modifying, and deleting address pools, and excluding IP addresses from a pool

To view, modify, or delete an existing address pool, display the DHCP Server Configuration page, and click the icons in the corresponding row in the address pool table.

- To delete an IP address pool, click 🗑, then submit and commit your changes.
- To view details on an IP address pool, click 🔍. A page displays with all the same information you entered when adding the pool.

  To modify the domain name associated with an IP address pool, or to exclude addresses from the pool, click ✎. The DHCP Server Pool – Modify page displays, as shown in Figure 12.



DHCP Server Pool - Modify

DHCP Pool Information		
Start IP Address:	10.0.1.3	
End IP Address:	10.0.1.20	
Netmask:	255.255.255.0	
Domain Name:		
Status:	● Enable ○ Disable	
Excluded IP:	Excluded IP Address	Action
	No Excluded IP!	
	10 . 0 . 1 . 3	Add

Figure 12. DHCP Server Pool – Modify Page

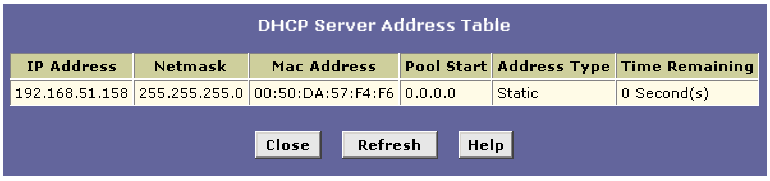
Excluded addresses are those that you have designated for fixed use with specific devices, or for some other reason do not want to make available to your network.

To exclude an address from distribution, type it in the fields provided and click Add. Click Submit after entering your changes. Be sure to use the Commit feature to save your changes to permanent memory, as described on page 33.

Viewing current DHCP address assignments

When the Neobit 1012VAfunctions as a DHCP server for your LAN, it keeps a record of any addresses, it has leased to your computers. To view a table of all current IP address assignments, display the DHCP Server Configuration page, and then click Address Table.

A page displays similar to that shown in Figure 13:



DHCP Server Address Table

IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
192.168.51.158	255.255.255.0	00:50:DA:57:F4:F6	0.0.0.0	Static	0 Second(s)

Figure 13. DHCP Server Address Table Page

The DHCP Server Address Table lists any IP addresses that are currently leased to LAN devices. For each leased address, the table lists the following information:

Field	Description
IP Address	The address that has been leased from the pool.
Netmask	The network mask associated with the leased address, which identifies the network ID and host ID portions of the address (see Appendix A).
Mac Address	A hardware ID for the device to which the number has been assigned.
Pool Start	The lower boundary of the address pool (provided to identify the pool from which the leased number came).
Address Type	Static or Dynamic. *Static* indicates that the IP number has been assigned permanently to the specific hardware device. *Dynamic* indicates that the number has been leased temporarily for a specified length of time.
Time Remaining	The amount of time left for the device to use the assigned address.

Configuring DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the device as a DHCP relay agent. When a computer on your network requests Internet access, the Neobit 1012VAcontacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer.

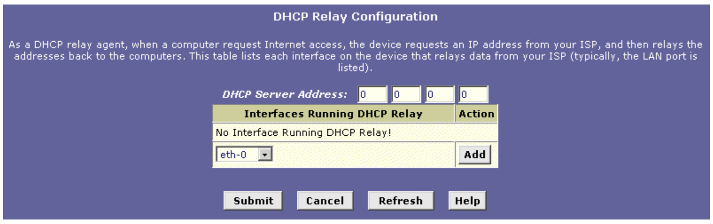
First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Open the Windows Control Panel and display the computer's Networking properties. Configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system). For detailed instructions, see the Quick Start chapter, "Part 2 — Configuring Your Computers."

Next, you specify the IP address of the DHCP server and select the interfaces on your network that will be using the relay service.

2. Log into the Configuration Manager, click the LAN tab, and then click **DHCP Relay** in the task bar.

   The DHCP Relay Configuration page displays:



DHCP Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP (typically, the LAN port is listed).

DHCP Server Address: 0 0 0 0

Interfaces Running DHCP Relay	Action
No Interface Running DHCP Relay!	
eth-0	Add

Figure 14. DHCP Relay Configuration Page

3. Type the IP address of your ISP's DHCP server in the fields provided.

   If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

4. If the interface named eth-0 is not already displaying, select it from the drop-down list and click Add.

   The eth-0 interface specifies that your default Ethernet (LAN) interface is running DHCP relay for your LAN. Typically, this is the only interface you need to specify here. If the Neobit 1012VAhas additional interfaces that you want to perform DHCP relay, you can select and add them.

   (You can also delete an interface from the table by clicking 🗑 in the right column.)

5. Click Submit.

A page displays to confirm your changes, and then the program returns to the DHCP Relay Configuration page.

6. Follow the instructions in "Setting the DHCP Mode" on page 49 to set the DHCP mode to DHCP Relay.

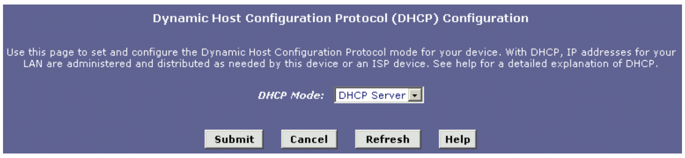
Setting the DHCP Mode

You should set the DHCP mode only after you have configured DHCP relay or DHCP server settings. See "Configuring DHCP Server" on page 43 or "Configuring DHCP Relay" on page 48 for additional instructions.

Follow these instructions to set the DHCP mode:

1. Click the LAN tab, and then click **DHCP Mode** in the task bar.

   The DHCP Configuration page displays, as shown in Figure 15.



Dynamic Host Configuration Protocol (DHCP) Configuration

Use this page to set and configure the Dynamic Host Configuration Protocol mode for your device. With DHCP, IP addresses for your LAN are administered and distributed as needed by this device or an ISP device. See help for a detailed explanation of DHCP.

DHCP Mode: DHCP Server

Figure 15. DHCP Configuration Page

2. From the DHCP Mode drop-down list, choose **DHCP Server**, **DHCP Relay**, or **none**.

   If you choose *none*, your LAN computers must be configured with static IP addresses.

3. Click Submit.

4. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

5. Click Commit to save your changes to permanent memory.

8 Configuring Network Address Translation

This chapter provides an overview of Network Address Translation (NAT) and instructions for modifying the default configuration on your device.

Overview of NAT

Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

Definitions

*A **private IP address** is created by a network administrator for use only on a LAN, whereas a **public IP address** is purchased from the Internet Corporation for Assigned Names and Numbers (ICANN) for use on the Internet. Typically, your ISP provides a public IP address for your entire LAN, and you define the private addresses for computers on your LAN.*

In a typical NAT setup, your ISP provides you with a single public IP address to use for your entire network. Then, you assign each computer on your LAN a unique private IP address. (Or, you define a pool of private IP addresses for dynamic assignment to your computers, as described in Chapter 7.) On the Neobit 1012VA, you set up a NAT rule to specify that whenever one of your computers communicates with the Internet, (that is, it sends and receives IP *data packets*) its private IP address—which is referenced in each packet—will be replaced by the LAN's public IP address.

Definitions

*An **IP data packet** contains bits of data bundled together in a specific format for efficient transmission over the Internet. Such packets are the building blocks of all Internet communication. Each packet contains header information that identifies the IP address of the computer that initiates the communication (the **source IP address**), the port number that the router associates with that computer (the **source port number**), the IP address of the targeted Internet computer (the **destination IP address**), and other information.*

When this type of NAT rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are actually originating from the computer assigned your public IP address (in this case, the Neobit 1012VA).

The NAT rule could further be defined to disguise the source port in the data packet (i.e., change it to another number), so that outside computers will not be able to determine the actual port from which the packet originated. Data packets that arrive in response contain the public IP address as the destination IP address and the disguised source port number. The Neobit 1012VAchanges the IP address and source port number back to the original values (having kept track of the changes it made earlier), and then routes the packet to the originating computer.

NAT rules such as these provide several benefits:

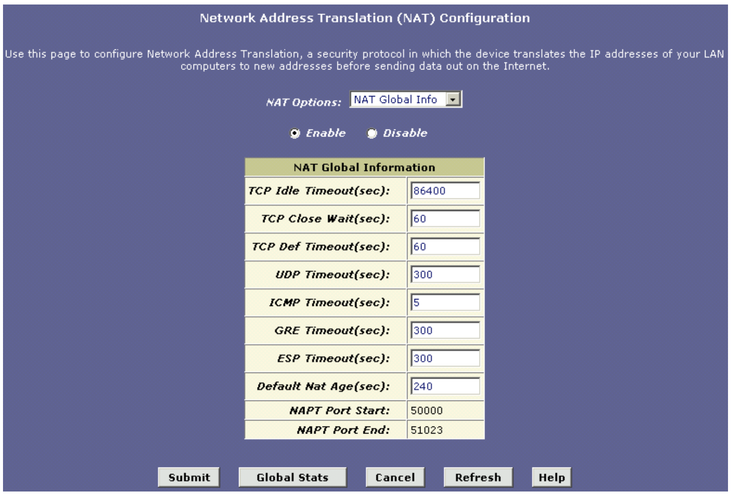
- They eliminate the need for purchasing multiple public IP addresses for computers on your LAN. You can make up your own private IP addresses at no cost, and then have them translated to the public IP address when your computers access the Internet.
- They provide a measure of security for you LAN by enabling you to assign private IP addresses and then have these and the source port numbers swapped out before your computers access the Internet.

The type of NAT function described above is called *network address port translation* (napt). You can use other types, called *flavors*, of NAT for other purposes; for example, providing outside access to your LAN or translating multiple private addresses to multiple public addresses.

By default, NAT is enabled, with an napt rule configured that translates any private address on the LAN side to your ISP-assigned public IP address on the WAN side. (For a description of napt rules, see page 58.)

Viewing NAT Global Settings and Statistics

To view your NAT settings, log into Configuration Manager, click the Services tab. The NAT Configuration page displays by default, as shown in Figure 16.



Network Address Translation (NAT) Configuration

Use this page to configure Network Address Translation, a security protocol in which the device translates the IP addresses of your LAN computers to new addresses before sending data out on the Internet.

NAT Options: NAT Global Info

● Enable ○ Disable

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
ESP Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

Figure 16. NAT Configuration Page

The NAT Configuration page contains the following elements:

- The NAT Options drop-down list, which provides access to the Global Information page (shown by default), the NAT

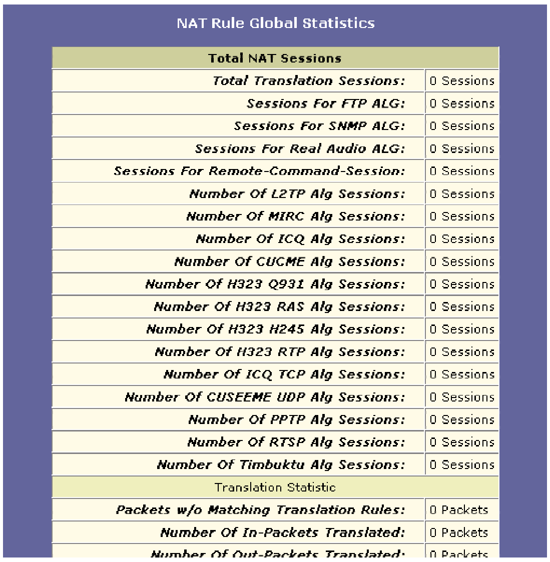
Rule Configuration page, and the NAT Translations page, which shows current translations.

- Enable/Disable radio buttons, which allow you to turn on or off the NAT feature.
- The NAT Global Information table, which displays the following settings that apply to all NAT rule translations:

Field	Description
TCP Idle Timeout (sec)	For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Close Wait (sec)	For a NAT translation on data using the TCP protocol, after a communication session has been closed, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Def Timeout (sec)	For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
UDP Timeout (sec)	Same as TCP Idle Timeout, but for UDP packets.
ICMP Timeout (sec)	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout (sec)	Same as TCP Idle Timeout, but for GRE packets.
Default Nat Age (sec)	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/End	When an napt rule is defined, the source ports will be translated to sequential numbers in this range.

If you change any values, click Submit, and then click the Admin tab and commit your changes to permanent system memory (see page 33).

You can click Global Stats to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one shown in Figure 17 displays.



NAT Rule Global Statistics

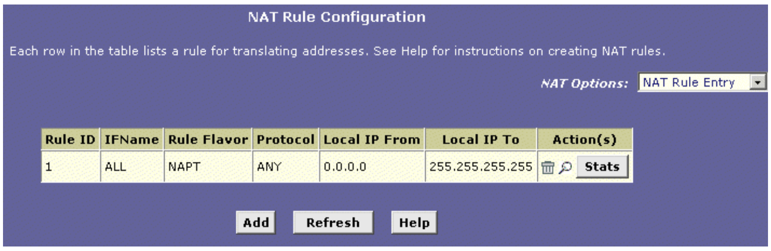
Total NAT Sessions	
Total Translation Sessions:	0 Sessions
Sessions For FTP ALG:	0 Sessions
Sessions For SNMP ALG:	0 Sessions
Sessions For Real Audio ALG:	0 Sessions
Sessions For Remote-Command-Session:	0 Sessions
Number Of L2TP Alg Sessions:	0 Sessions
Number Of MIRC Alg Sessions:	0 Sessions
Number Of ICQ Alg Sessions:	0 Sessions
Number Of CUCME Alg Sessions:	0 Sessions
Number Of H323 Q931 Alg Sessions:	0 Sessions
Number Of H323 RAS Alg Sessions:	0 Sessions
Number Of H323 H245 Alg Sessions:	0 Sessions
Number Of H323 RTP Alg Sessions:	0 Sessions
Number Of ICQ TCP Alg Sessions:	0 Sessions
Number Of CUSEEME UDP Alg Sessions:	0 Sessions
Number Of PPTP Alg Sessions:	0 Sessions
Number Of RTSP Alg Sessions:	0 Sessions
Number Of Timbuktu Alg Sessions:	0 Sessions
Translation Statistic	
Packets w/o Matching Translation Rules:	0 Packets
Number Of In-Packets Translated:	0 Packets
Number Of Out-Packets Translated:	0 Packets

Figure 17. NAT Rule Global Statistics Page

The table provides basic information for each NAT rule you have set up. You can click Clear to restart the accumulation of the statistics at their initial values.

Viewing NAT Rules and Rule Statistics

To view the NAT rules currently defined on your system, select **NAT Rule Entry** in the NAT Options drop-down list. The NAT Rule Configuration page displays, as shown in Figure 18.



NAT Rule Configuration

Each row in the table lists a rule for translating addresses. See Help for instructions on creating NAT rules.

NAT Options: NAT Rule Entry

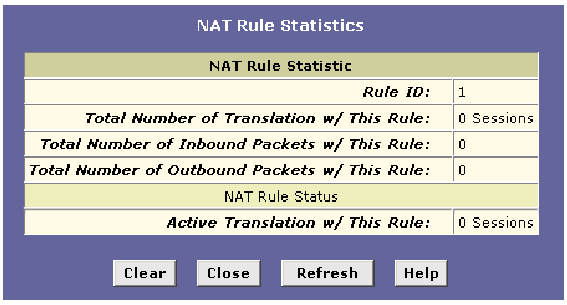
Rule ID	IFName	Rule Flavor	Protocol	Local IP From	Local IP To	Action(s)
1	ALL	NAPT	ANY	0.0.0.0	255.255.255.255	🗑 🔍 Stats

Figure 18. NAT Rule Configuration Page

The NAT Rule Configuration table displays a row containing basic information for each rule. For a description of these fields, refer to the instructions for adding rules (pages 58 through 67).

From the NAT Rule Configuration page, you can click **Add** to add a new rule, or use the icons in the right column to delete (🗑) or view details on (🔍) a rule.

To view data on how often a specific NAT rule has been used, click **Stats** in the Action(s) column. A page similar to the one show in Figure 19 displays:



NAT Rule Statistics

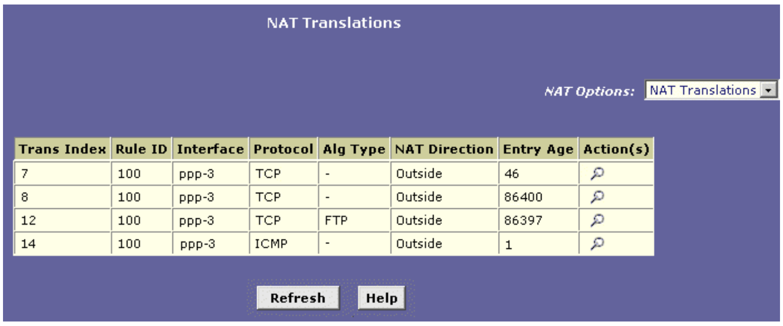
NAT Rule Statistic	
Rule ID:	1
Total Number of Translation w/ This Rule:	0 Sessions
Total Number of Inbound Packets w/ This Rule:	0
Total Number of Outbound Packets w/ This Rule:	0
NAT Rule Status	
Active Translation w/ This Rule:	0 Sessions

Figure 19. NAT Rule Statistics Page

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule. You can click **Clear** to reset the statistics to zeros and **Refresh** to display newly accumulated data.

Viewing Current NAT Translations

To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **NAT Translations** from the NAT Options drop-down list. The NAT Translations page displays, as shown in Figure 20:



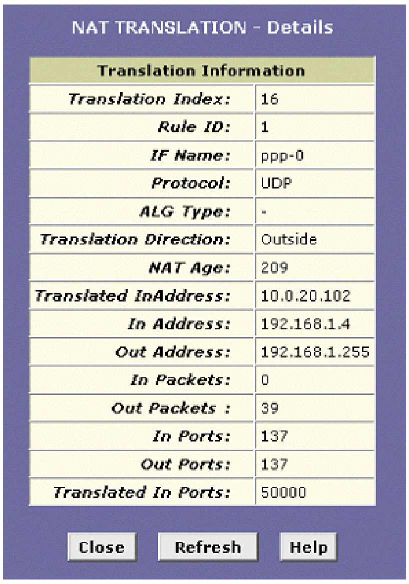
Trans Index	Rule ID	Interface	Protocol	Alg Type	NAT Direction	Entry Age	Action(s)
7	100	ppp-3	TCP	-	Outside	46	🔎
8	100	ppp-3	TCP	-	Outside	86400	🔎
12	100	ppp-3	TCP	FTP	Outside	86397	🔎
14	100	ppp-3	ICMP	-	Outside	1	🔎

Figure 20. NAT Translations Page

For each current NAT translation session, the table contains the following fields:

Field	Description
Trans Index	The sequential number assigned to the IP session used by this NAT translation session.
Rule ID	The ID of the NAT rule invoked.
Interface	The device interface on which the NAT rule was invoked (from the rule definition).
Protocol	The IP protocol used by the data packets that are undergoing translations (from the rule definition) Example: TCP, UDP, ICMP.
Alg Type	The *Application Level Gateway* (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).
NAT Direction	The direction (incoming or outgoing) of the translation (from the port definition).
Entry Age	The elapsed time, in seconds, of the NAT translation session.

You can click 🔎 in the Action(s) column to view additional details about a NAT translation session, as shown in Figure 21.



NAT TRANSLATION - Details

Translation Information	
Translation Index:	16
Rule ID:	1
IF Name:	ppp-0
Protocol:	UDP
ALG Type:	-
Translation Direction:	Outside
NAT Age:	209
Translated InAddress:	10.0.20.102
In Address:	192.168.1.4
Out Address:	192.168.1.255
In Packets:	0
Out Packets :	39
In Ports:	137
Out Ports:	137
Translated In Ports:	50000

Figure 21. NAT Translation – Details Page

In addition to the information displayed in the NAT Translations table, this table displays the following for the selected current translation sessions:

Field	Description
Translated In Address	The public IP address to which the private IP address was translated.
In Address	The private IP address that was translated.
Out Address	The IP address of the outside destination (web, ftp site, etc.)
In/Out Packets	The number of incoming and outgoing IP packets that have been translated in this translation session.
In Ports	The actual port number corresponding to the LAN computer.
Out Ports	The port number associated with the destination address.
Translated In Ports	The port number to which the LAN computer's actual port number was translated.

Adding NAT Rules

This section explains how to create rules for the various NAT flavors

Note

You cannot edit existing NAT rules. To change a rule setup, delete it and add a new rule with the modified settings.

The napt rule: Translating between private and public IP addresses

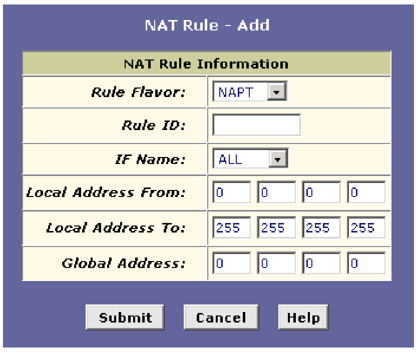
Follow these instructions to create a rule for translating the private IP addresses on your LAN to your public IP address. This type of rule uses the NAT flavor napt, which was used in your default configuration. The napt flavor translates private source IP addresses to a single public IP address. The napt rule also translates the source port numbers to port numbers that are defined on the NAT Global Configuration page (see page 52). The Introduction to NAT on page 51 describes how the napt rule works.

1. Click the NAT tab, then select **NAT Rule Entry** from the NAT Options drop-down list on the right side of the page.

   The NAT Rule entry page displays a row for each currently configured NAT rule.

2. Click Add to display the NAT Rule – Add page.

   The NAPT flavor displays by default in the Rule Flavor drop-down list. The NAT Rule – Add page displays, as shown in Figure 22.



NAT Rule - Add

NAT Rule Information				
Rule Flavor:	NAPT			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address:	0	0	0	0

Figure 22. NAT Rule – Add Page (napt Flavor)

3. Enter a Rule ID.

   The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the Rule ID so that the higher priority rules are invoked before lower-priority rules. It is recommended that you select rule IDs as multiples of 5 or 10 so that, in the future, you can insert a rule between two existing rules.

Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the IFName drop-down list, select the interface on the device to which this rule applies.

   Typically, NAT rules are used for communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named *ppp-0* or *eoa-0*) to connect your LAN to your ISP, it is the usual IFName selection.

5. In the Local Address From field and Local Address To fields, type the starting and ending IP addresses, respectively, of the range of private address you want to be translated. Or, type the same address in both fields to specify a single value.

   To specify that data from all LAN addresses should be translated, type 0 (zero) in each From field and 255 in each To field.

   If you have several non-sequential private addresses, you can create an additional napt rule for each address.

   These addresses should correspond to private addresses already in use on your network (either assigned statically to your PCs, or assigned dynamically using DHCP, as discussed in the Quick Start).

6. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP.

   If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on other PPP interfaces.

   If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

7. When you have completed entering all information, click Submit.

   A page displays to confirm the change.

8. Click Close to return to the NAT Configuration page.

   The new rule should display in the NAT Rule Configuration table.

9. Ensure that the Enable radio button is selected, and then click Submit.

   A page displays to confirm your changes.

10. Click the Admin tab, and then click **Commit and Reboot** in the task bar.

11. Click Commit to save your changes to permanent memory.

The rdr rule: Allowing external access to a LAN computer

You can create an rdr rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer's private IP address is translated to your public IP address in all incoming and outgoing data packets.

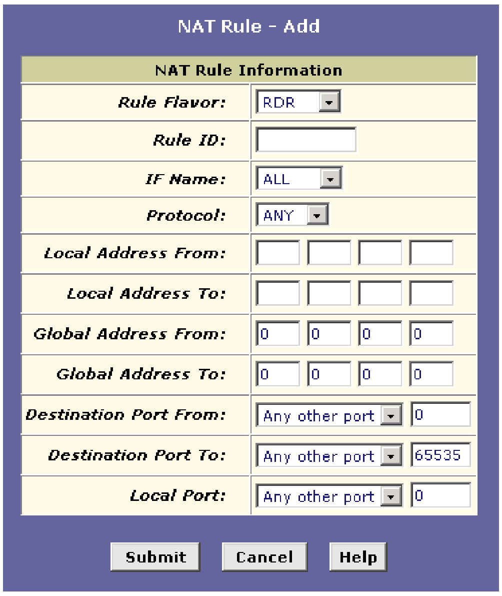
Note

Without an rdr rule (or bitmap rule described on page 66), the Neobit 1012VAblocks attempts by external computers to access your LAN computers.

The following example illustrates using the rdr rule to provide external access to your web server:

> Your ADSL/Ethernet router receives a packet containing a request for access to your Web server. The packet header contains the public address for your LAN as the destination IP address, and a destination port number of 80. Because you have set up an rdr rule for incoming packets with destination port 80, the device recognizes the data as a request for Web server access. The device changes the packet's destination address to the private IP address of your Web server and forwards the data packet to it.
>
> Your Web server sends data packets in response. Before the ADSL/Ethernet router forwards them on to the Internet, it changes the source IP address in the data packets from the Web server's private address to your LAN's public address. To an external Internet user then, it appears as if your Web server uses your public IP address.

Figure 23 shows the fields used to establish an rdr rule:



NAT Rule - Add

NAT Rule Information

Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	
Local Address To:	
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535
Local Port:	Any other port 0

Figure 23. NAT Rule – Add Page (rdr Flavor)

Follow these instructions to add an rdr rule (see steps 1-4 under "The napt rule" on page 58 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **RDR** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.
4. In the Local Address From and Local Address To fields, type the same private IP address, or the lowest and highest addresses in a range:

   - If you type the same IP address in both fields, incoming traffic that matches the criteria you specify in steps 5 and 6 will be redirected to that IP address.
   - If you type a range of addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers to help ensure efficient network performance.

   These addresses should correspond to private addresses already in use on your network (either assigned statically to your PCs or assigned dynamically using DHCP, as discussed in the Quick Start, Part 2).
5. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP.

   If you have multiple WAN (PPP) interfaces, this rule will not be enforced for data that arrives on other PPP interfaces. This rule will not be enforced for data that arrives on WAN interfaces not specified here.

   If you have multiple WAN interfaces and want the rule to be enforced on more than one of them (or all), type the starting and ending IP addresses of the range.
6. In the Destination Port From and Destination Port To fields, enter the port ID (or a range) that you expect to see on incoming packets destined for the LAN computer for which this rule is being created.

   Incoming traffic that meets this criteria will be redirected to the Local Port number you specify in the next field.

   For example, if you grant public access to a Web server on your LAN, you would expect that incoming packets destined for that computer would contain the well-known web server port number, 80. This setting serves as a filter; data packets not containing this port number would not be granted access to you local computer.

7. If the LAN computer that you are making publicly available is configured to use a non-standard port number for the type of traffic it receives, type the non-standard port number in the Local Port field.

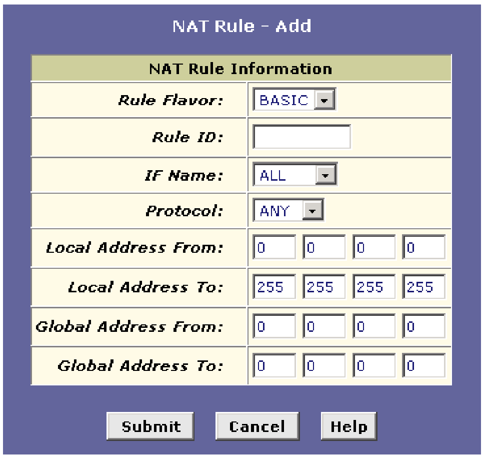
   This option translates the standard port number in packets destined for your LAN computer to the non-standard number you specify. For example, if your Web server uses (non-standard) port 2000, but you expect incoming data packets to refer to (standard) port 80, you would enter 2000 here and 80 in the Destination Port fields. The headers of incoming packets destined for port 80 will be modified to refer to port 2000. The packet can then be routed appropriately to the web server.

8. Follow steps 7-12 under "The napt rule" on page 58 to submit your changes.

The basic rule: Performing 1:1 translations

The basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like napt rules. However, unlike napt rules, basic rules do not also translate the port numbers in the packet header; they are passed through untranslated. Therefore, the basic rule does not provide the same level of security as the napt rule.

Figure 24 shows the fields used for adding a basic rule.



NAT Rule - Add

NAT Rule Information

Rule Flavor:	BASIC			
Rule ID:				
IF Name:	ALL			
Protocol:	ANY			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address From:	0	0	0	0
Global Address To:	0	0	0	0

Figure 24. NAT Rule – Add Page (basic Flavor)

Follow these instructions to add an basic rule (see steps 1-4 under "The napt rule" on page 58 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **BASIC** as the Rule Flavor, and enter a Rule ID.

2. Select the interface on which this rule will be effective.

3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.

4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 5).

   You can create a basic rule for each specific address translation to occur. The range of addresses should correspond to private addresses already in use on your network, whether assigned statically to your PCs, or assigned dynamically using DHCP.

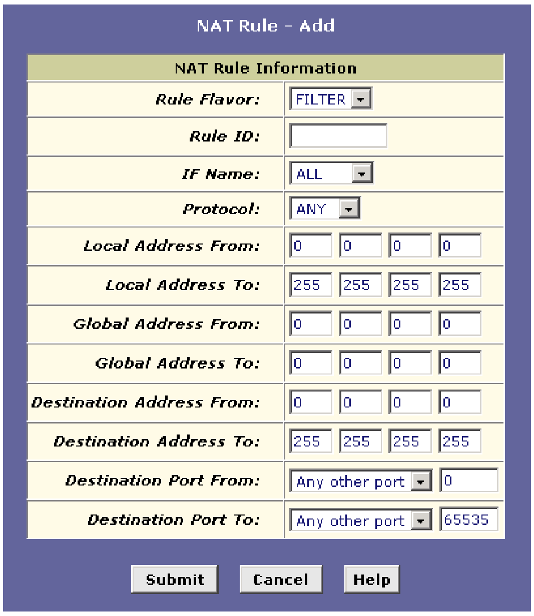
5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the pool of public IP addresses that the private addresses should be translated to. Or, type the same address in both fields (if you also specified a single address in step 4).
6. Follow steps 7-12 under "The napt rule" on page 58 to submit your changes.

The filter rule: Configuring a basic rule with additional criteria

Like the basic flavor, the filter flavor translates public and private IP addresses on a one-to-one basis. The filter flavor extends the capability of the basic rule. Refer to “The basic Rule” on page 63 for a general description.

You can use the filter rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, server type (such as FTP or Web server), or both.

Figure 25 shows the fields used to establish a filter rule.



NAT Rule - Add

NAT Rule Information

Rule Flavor:	FILTER
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Address From:	0 0 0 0
Destination Address To:	255 255 255 255
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535

Figure 25. NAT Rule—Add Page (filter Flavor)

Follow these instructions to add a filter rule (see steps 1-4 under "The napt rule" on page 58 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **FILTER** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.

4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 5).

   The address (or range of addresses) should correspond to a private addresses (or addresses) already in use on your network. These may be assigned statically to your PCs or assigned dynamically using DHCP, as discussed in the Quick Start.

5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the range of public IP addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 4).

6. Specify a Destination Address or addresses, Destination Port (or ports), or both. You can specify a single value by entering that value in both fields.

   - Specify a destination address (or range) if you want this rule to apply only to outbound traffic to the address (or range).

     If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on network.

   - Specify a destination ports (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.

     For example, if you do not specify a destination address, but specify a Destination Port From/To of 21, then this translation will occur on all accesses by your LAN to all external FTP servers. That is, when one of your LAN computers communicates with an external FTP server, the source IP address in the packet headers is changed to the public address, replacing the initiator's private IP address.

     Port number assignments are maintained in RFCs maintained by IANA. Common port numbers include:
     20, 21—FTP (file transfer protocol) server
     25—SMTP (simple mail transfer protocol) server
     80—HTTP (World Wide Web) server

   - Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to apply to accesses to the specified server type at the specified IP address or network.

7. Follow steps 7-12 under "The napt rule" on page 58 to submit your changes.

The bitmap rule: Performing two-way translations

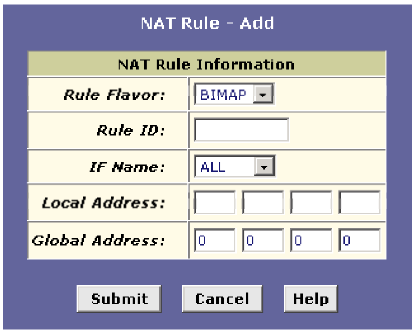
Unlike the other NAT flavors, the bitmap flavor performs address translations in both the outgoing and incoming directions.

In the incoming direction, when the specified Neobit 1012VAinterface receives a packet with your public IP address as the destination address, this address is translated to the private IP address of a computer on your LAN. To the external computer, it appears as if the access is being made to the public IP address, when, in fact, it is communicating with a LAN computer.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN's public IP address. To the rest of the Internet, it appears as if the data packet originated from the public IP address.

Bitmap rules can be used to provide external access to a LAN device. They do not provide the same level of security as rdr rules, because rdr rules also reroute incoming packets based on the port ID. Bitmap rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.

Figure 26 shows the fields used to establish a bitmap rule.


NAT Rule - Add

NAT Rule Information

Rule Flavor:	BIMAP
Rule ID:	
IF Name:	ALL
Local Address:	
Global Address:	0 0 0 0

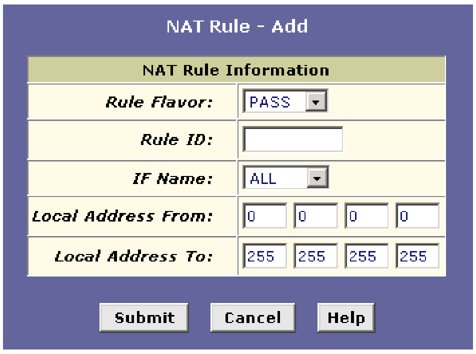
Figure 26. NAT Rule – Add Page (bimap Flavor)

Follow these instructions to add a bimap rule (see steps 1-4 under "The napt rule" on page 58 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **BIMAP** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. In the Local Address field, type the private IP address of the computer to which you are granting external access.
4. In the Global Address field, type the address that you want to serve as the publicly known address for the LAN computer.
5. Follow steps 7-12 under "The napt rule" on page 58 to submit your changes.

The pass rule: Allowing specific addresses to pass through untranslated

You can create a pass rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so



NAT Rule - Add

NAT Rule Information

Rule Flavor:	PASS
Rule ID:	
IF Name:	ALL
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255

Figure 27. NAT Rule – Add Page (pass Flavor)

The pass rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. In you want a specific IP address or range of addresses to not be subject to an existing rule, say rule ID #5, then you can create a pass rule with ID #1 through #4.

Follow these instructions to add a pass rule (see steps 1-4 under "The napt rule" on page 58 for detailed instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **PASS** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. In the Local Address From and Local Address To fields, type the lowest and highest IP addresses that define the range of private address you want to be passed without translation.

   If you want the pass rule to act on only one address, type that address in both fields.
4. Follow steps 7-12 under "The napt rule" on page 58 to submit your changes.

9 Configuring DNS Server Addresses

About DNS

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g., "yahoo.com") to the equivalent numerical IP addresses that are used for Internet routing.

When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP address. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

Assigning DNS Addresses

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses. Your LAN PCs learn these DNS addresses in one of the following ways:

- **Statically:** If your ISP provides you with their DNS server addresses, you can assign them to each PC by modifying the PCs' IP properties.
- **Dynamically from a DHCP pool:** You can configure the DHCP Server feature on the ADSL/Ethernet router and create an address pool that specify the DNS addresses to be distributed to the PCs. Refer to Chapter 7, “Configuring DHCP Server” on page 43 for instructions on creating DHCP address pools.

In either case, you can specify the actual addresses of the ISP's DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN port on the ADSL/Ethernet router (e.g., 192.168.1.1). When you specify the LAN port IP address, the device performs *DNS relay*, as described in the following section.

Note

If you specify the actual DNS addresses on the PCs or in the DHCP pool, the DNS relay feature is not used.

Configuring DNS Relay

When you specify the device's LAN port IP address as the DNS address, then the ADSL/Ethernet automatically performs "DNS relay"; i.e., because the device itself is not a DNS server, it forwards domain name lookup requests from the LAN PCs to a DNS server at the ISP. It then relays the DNS server's response to the PC.

When performing DNS relay, the Neobit 1012VAmust maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

- **Learned through PPP:** If the device uses a PPP connection to the ISP, the primary and secondary DNS addresses can be learned via the PPP protocol. To use this method, the "Use DNS" checkbox must be selected in the PPP interface properties. (See Chapter 13 for instructions on configuring your PPP interface. Note that you cannot change this property by modifying an existing PPP interface; you must delete the interface and recreate it with the new setting.)

  Using this option provides the advantage that you will not need to reconfigure the PCs or the ADSL/Ethernet router if the ISP changes their DNS addresses.

- **Configured on the ADSL/Ethernet router:** You can use the device's DNS feature to specify the ISP's DNS addresses. If the device also uses a PPP interface with the "Use DNS" property enabled, then these configured addresses will be used in addition to the two addresses learned through PPP. If "Use DNS" is not enabled, or if a protocol other than PPP is used (such as EoA), then these configured addresses will be used as the primary and secondary DNS addresses.

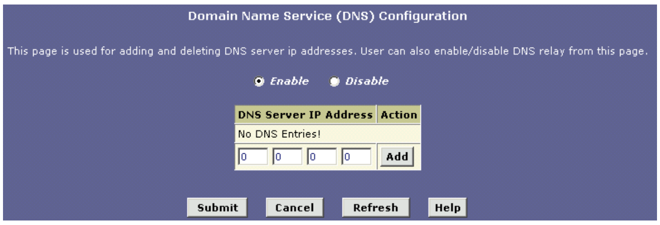
Follow these steps to configure DNS relay:

1. Configure the LAN PCs to use the ADSL/Ethernet router's LAN IP address as their DNS server address—by assigning the LAN IP address statically to each PC, or by inputting the LAN IP address or the address 0.0.0.0 as the DNS address in the DHCP server pool used by the PCs.
2. If using a PPP connection to the ISP, click the "Use DNS" check box so that the DNS server addresses it learns are used for DNS relay.

   Or, ...

   If not using a PPP connection (or if you want to specify DNS addresses in addition to those learned through PPP), configure the DNS addresses on the ADSL/Ethernet router as follows:

a. Click the Services tab, and then click **DNS** in the task bar. The DNS Configuration page displays.



Domain Name Service (DNS) Configuration

This page is used for adding and deleting DNS server ip addresses. User can also enable/disable DNS relay from this page.

● *Enable* ○ *Disable*

DNS Server IP Address	Action
No DNS Entries!	
0 . 0 . 0 . 0	Add

Figure 28. DNS Configuration Page

b. Type the IP address of the DNS server in an empty row and click Add.

You can enter only two addresses.

c. Click the **Enable** radio button, and then click Submit.

3. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

4. Click Commit to save your changes to permanent memory.

Note

DNS addresses that are assigned to LAN PCs prior to enabling DNS relay will remain in effect until the PC is rebooted. DNS relay will only take effect when a PC's DNS address is the LAN IP address.

Similarly, if after enabling DNS relay, you specify a DNS address (other than the LAN IP address) in a DHCP pool or statically on a PC, then that address will be used instead of the DNS relay address.

C Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the Neobit 1012VA, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the Neobit 1012VAand a wall socket/power strip.
DSL LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable like the one provided is securely connected to the ADSL port and your wall phone jack. Wait 30 seconds to allow the device to negotiate a connection with your ISP.
LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the Neobit 1012VA. Make sure the PC and/or hub is turned on. Verify that you are using a straight-through type Ethernet cable to the uplink port on a hub or a cross-over type cable to a stand-alone PC. If you connected the device to an ordinary hub port (not Uplink), you must use a straight-through cable. (Hold the connectors at each end of the cable side-by-side in the same position. If the order of their color-coded wire pairs is the same, it is a straight-through type.) Contact Customer Support if your cable is not the correct type. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.
Internet Access	
PC cannot access Internet	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the Neobit 1012VA's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: • Check that the gateway IP address on the computer is your public IP address (see the Quick Start chapter, Part 2 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. • Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. • Verify that a Network Address Translation rule has been defined on the Neobit 1012VAto translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules (see

Problem	Troubleshooting Suggestion
	Chapter 8). Or, configure the PC to accept an address assigned by another device (see the Quick Start, Part 2). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool (see the instructions in Chapter 7 to view the address pool).
PCs cannot display web pages on the Internet.	Verify that the DNS server specified on the PCs is correct for your ISP, as discussed in the item above. You can use the ping utility, discussed in the following section, to test connectivity with your ISP's DNS server.
Configuration Manager Program	
You forgot/lost your Configuration Manager user ID or password.	If you have not changed the password from the default, try using "root" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset button on the back panel of the device (using a pointed object such as a pen tip). Then, type the default User ID and password shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
Cannot access the Configuration Manager program from your browser.	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the Neobit 1012VA's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v4.7 or later. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the Neobit 1012VA.
Changes to Configuration Manager are not being retained.	Be sure to use the Commit function after any changes. This function is described on page 33.

Diagnosing Problem using IP Utilities

ping

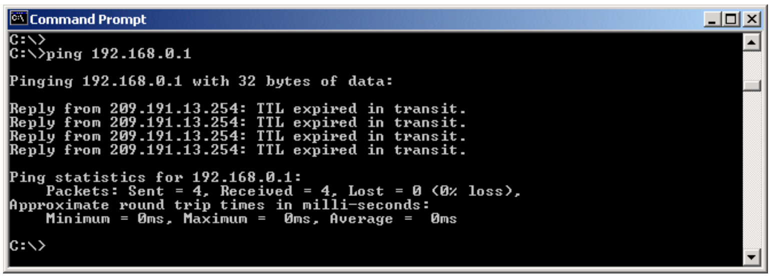
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

ping 192.168.1.1

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window displays like that shown in Figure 63.



```
C:\>
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Figure 63. Using the ping Utility

If the target computer cannot be located, you will receive the message “Request timed out.”

Using the ping command, you can test whether the path to the Neobit 1012VAis working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

nslookup

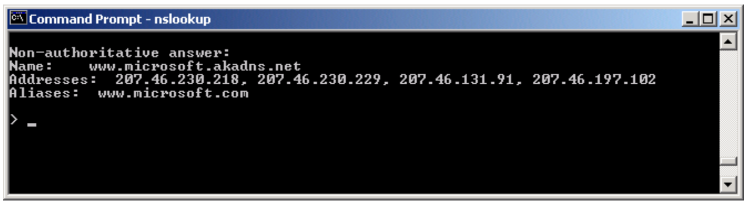
You can use the nslookup command to determine the IP address associated with an internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP’s DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

nslookup

Click OK. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the internet address your are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown in Figure 64.



```
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses:  207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases:  www.microsoft.com

> _
```

Figure 64. Using the nslookup Utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press **<Enter>** at the command prompt.

D Glossary

10BASE-T
A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. *See also data rate, Ethernet*.

100BASE-T
A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. *See also data rate, Ethernet*.

ADSL
Asymmetric Digital Subscriber Line
The most commonly deployed "flavor" of DSL for home users. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.

analog
Of data, having a form is analogous to the data's original waveform. The voice component in DSL is an analog signal. *See also digital*.

ATM
Asynchronous Transfer Mode
A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. *See also data rate*.

authenticate
To verify a user’s identity, such as by prompting for a password.

binary
The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. *See also bit, IP address, network mask*.

bit
Short for "binary digit," a bit is a number that can have two values, 0 or 1. *See also binary*.

bps
bits per second

bridging
Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The Neobit 1012VAcan perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See also *routing*.

broadband
A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.

broadcast
To send data to all computers on a network.

DHCP
Dynamic Host Configuration Protocol
DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address

from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.

DHCP relay Dynamic Host Configuration Protocol relay
A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the Neobit 1012VA's interfaces can be configured as a DHCP relay. *See DHCP*.

DHCP server Dynamic Host Configuration Protocol server
A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. *See DHCP*.

digital Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. *See also analog*.

DNS Domain Name System
The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. *See also domain name.*

domain name A domain name is a user-friendly name used in place of its associated IP address. For example, www.globespan.net is the domain name associated with IP address 209.191.4.240. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site, e.g., http://www.globespan.net/index.html. *See also DNS.*

download To transfer data in the downstream direction, i.e., from the Internet to the user.

DSL Digital Subscriber Line
A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.

Ethernet The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. *See also 10BASE-T, 100BASE-T, twisted pair*.

filtering To screen out selected types of data, based on filtering rules. Filtering can be applied in one direction (upstream or downstream), or in both directions.

filtering rule A rule that specifies what kinds of data the a routing device will accept and/or reject. Filtering rules are defined to operate on an interface (or multiple interfaces) and in a particular direction (upstream, downstream, or both).

firewall Any method of protecting a computer or LAN connected to the Internet from intrusion or attack from the outside. Some firewall protection can be provided by packet filtering and Network Address Translation services.

FTP

File Transfer Protocol
A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

GGP

Gateway to Gateway Protocol. An Internet protocol that specifies how gateway routers communicate with each other.

Gbps

Abbreviation for Gigabits ("GIG-uh-bits") per second, or one billion bits per second. Internet data rates are often expressed in Gbps.

hop

When you send data through the Internet, it is sent first from your computer to a router, and then from one router to another until it finally reaches a router that is directly connected to the recipient. Each individual "leg" of the data's journey is called a hop.

hop count

The number of hops that data has taken on its route to its destination. Alternatively, the maximum number of hops that a packet is allowed to take before being discarded (*see also TTL*).

host

A device (usually a computer) connected to a network.

HTTP

Hyper-Text Transfer Protocol
HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. *See also web browser, web site*.

ICMP

Internet Control Message Protocol
An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.

IGMP

Internet Group Management Protocol
An Internet protocol that enables a computer to share information about its membership in multicast groups with adjacent routers. A multicast group of computers is one whose members have designated as interested in receiving specific content from the others. Multicasting to an IGMP group can be used to simultaneously update the address books of a group of mobile computer users or to send company newsletters to a distribution list.

in-line filter

See micro filter.

Internet

The global collection of interconnected networks used for both private and business communications.

intranet

A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.

IP

See TCP/IP.

IP address

Internet Protocol address
The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a *network ID* that identifies the particular network the host belongs to, and a *host ID* uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. *See also domain name, network mask*.

ISP

Internet Service Provider
A company that provides Internet access to its customers, usually for a fee.

LAN

Local Area Network
A network limited to a small geographic area, such as a home, office, or small building.

LED

Light Emitting Diode
An electronic light-emitting device. The indicator lights on the front of the Neobit 1012VAare LEDs.

MAC address

Media Access Control address
The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of characters.

mask

See network mask.

Mbps

Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

micro filter

In splitterless deployments, a micro filter is a device that removes the data frequencies in the DSL signal, so that telephone users do not experience interference (noise) from the data signals. Micro filter types include *in-line* (installs between phone and jack) and *wall-mount* (telephone jack with built-in micro filter). *See also splitterless.*

NAT

Network Address Translation
A service performed by many routers that translates your network's publicly known IP address into a *private* IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.

NAT rule

A defined method for translating between public and private IP addresses on your LAN.

network

A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a *LAN*, or very large, such as the *Internet*.

network mask

A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. *See also binary, IP address, subnet, "IP Addresses Explained" section*.

NIC

Network Interface Card
An adapter card that plugs into your computer and provides the physical interface to your network cabling, which for Ethernet NICs is typically an RJ-45 connector. *See Ethernet, RJ-45*.

packet

Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).

ping
Packet Internet (or Inter-Network) Groper
A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

port
A physical access point to a device such as a computer or router, through which data flows into and out of the device.

POTS
Plain Old Telephone Service
Traditional analog telephone service using copper telephone lines. Pronounced "pots." *See also PSTN*.

POTS splitter
See splitter.

PPP
Point-to-Point Protocol
A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the Neobit 1012VAuses two forms of PPP called PPPoA and PPPoE. *See also PPPoA, PPPoE*.

PPPoA
Point-to-Point Protocol over ATM
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.

PPPoE
Point-to-Point Protocol over Ethernet
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.

protocol
A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.

remote
In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.

RIP
Routing Information Protocol
The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.

RJ-11
Registered Jack Standard-11
The standard plug used to connect telephones, fax machines, modems, etc. to a telephone jack. It is a 6-pin connector usually containing four wires.

RJ-45
Registered Jack Standard-45
The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.

routing
Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.

rule
See filtering rule, NAT rule.

SDNS
Secondary Domain Name System (server)
A DNS server that can be used if the primary DSN server is not available. *See DNS*.

SNMP Simple Network Management Protocol
The TCP/IP protocol used for network management.

splitter A device that splits off the voice component of the DSL signal to a separate line, so that data and telephone service each have their own wiring and jacks. The splitter is installed by your telephone company where the DSL line enters your home. The CO also contains splitters that separate the voice and data signals, sending voice to the PSTN and data on high-speed lines to the Internet. *See also CO, PSTN, splitterless, micro filter*.

splitterless A type of DSL installation where no splitter is installed, saving the cost of a service call by the telephone company. Instead, each jack in the home carries both voice and data, requiring a micro filter for each telephone to prevent interference from the data signal. ADSL is usually splitterless; if you are unsure if your installation has a splitter, ask your DSL provider. *See also splitter, micro filter*.

subnet A subnet is a portion of a network. The subnet is distinguished from the larger network by a *subnet mask* which selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. *See also network mask*.

subnet mask A mask that defines a subnet. *See also network mask*.

TCP *See TCP/IP*.

TCP/IP Transmission Control Protocol/Internet Protocol
The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.

Telnet An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.

TFTP Trivial File Transfer Protocol
A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.

TTL Time To Live
A field in an IP packet that limits the life span of that packet. Originally meant as a time duration, the TTL is usually represented instead as a maximum hop count; each router that receives a packet decrements this field by one. When the TTL reaches zero, the packet is discarded.

twisted pair The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category

5 (CAT 5) is used for 100BASE-T networks. *See also 10BASE-T, 100BASE-T, Ethernet*.

upstream
The direction of data transmission from the user to the Internet.

USB
Universal Serial Bus
A serial interface that lets you connect devices such as printers, scanners, etc. to your computer by simply plugging them in.

VC
Virtual Circuit
A connection from your ADSL router to your ISP.

VCI
Virtual Circuit Identifier
Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. *See also VC*.

VPI
Virtual Path Identifier
Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. *See also VC*.

WAN
Wide Area Network
Any network spread over a large geographical area, such as a country or continent. With respect to the Neobit 1012VA, WAN refers to the Internet.

Web browser
A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. *See also HTTP, web site, WWW*.

Web page
A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the *home page*. *See also hyperlink, web site*.

Web site
A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. *See also hyperlink, web page*.

WWW
World Wide Web
Also called *(the) Web.* Collective term for all web sites anywhere in the world that can be accessed via the Internet.