VisionNet

202ER ADSL Ethernet Router
User's Manual

Revision 1.1
February 27, 2003

Table of Contents

1 Introduction 9

Features 9

System Requirements 9

Using this Document 10

Notational conventions 10

Typographical conventions 10

Special messages 10

2 Getting to Know the VisionNet 202ER 11

Parts Check 11

Front Panel 12

Rear Panel 13

3 Quick Start 15

Part 1 — Connecting the Hardware 15

Step 1. Connect the ADSL cable and optional telephone. 16

Step 2. Connect the Ethernet cable 17

Step 3. Attach the power connector. 17

Step 4. Turn on the VisionNet 202ER and power up your systems. 17

Part 2 — Configuring Your Computers 18

Before you begin 18

Windows® 95, 98 PCs: 18

Windows NT 4.0 workstations: 19

Windows 2000 PCs: 20

Windows Me PCs 21

Assigning static Internet information to your PCs 22

Part 3 — Configuring the VisionNet 202ER 23

Logging in to the VisionNet 202ER Quick Setup 23

Operation Mode 24

DNS Settings 24
PPP Settings 24
Default Router Settings 25
Testing Your Installation 26
Using VisionNet's Diagnostic Utilities 27

4 Getting Started with the Configuration Manager 29
Accessing the Configuration Manager 29
Functional Layout 31
Commonly used buttons 31
The Home Tab and System View Table 32
Changing the System Date and Time 34
Changing the System Date and Time 34
Changing Your Login Password 35
Committing Your Changes and Rebooting the Device 36
Committing your changes 36
Rebooting the device using Configuration Manager 37

5 Setting the LAN IP Address 39
Configuring the LAN IP Address 39

6 Viewing System IP Information and Performance Statistics 43
Viewing the VisionNet 202ER's IP addresses 43
Viewing IP Global Statistics 44

7 Configuring Dynamic Host Configuration Protocol 45
Overview of DHCP 45
What is DHCP? 45
Why use DHCP? 45
VisionNet 202ER DHCP modes 46

Configuring DHCP Server 47

Viewing, modifying, and deleting address pools, and excluding IP addresses from a pool 50

Viewing current DHCP address assignments 50

Configuring DHCP Relay 52

Setting the DHCP Mode 53

8 Configuring Network Address Translation 55

Overview of NAT 55

Your Default NAT Setup 56

Viewing NAT Global Settings and Statistics 57

Viewing NAT Rules and Rule Statistics 60

Viewing Current NAT Translations 61

Adding NAT Rules 63

The napt rule: Translating between private and public IP addresses 63

The rdr rule: Allowing external access to a LAN computer 65

The basic rule: Performing 1:1 translations 68

The filter rule: Configuring a basic rule with additional criteria 69

The bimap rule: Performing two-way translations 71

The pass rule: Allowing specific addresses to pass through untranslated 72

9 Configuring DNS Server Addresses 79

About DNS 79

Assigning DNS Addresses 79

Configuring DNS Relay 74

10 Configuring IP Routes 77

Overview of IP Routes 77

Comparing IP routing to telephone switching 77

Hops and gateways 78

Using IP routes to define default gateways 78

Do I need to define IP routes? 78
Viewing the IP Routing Table 79
Adding IP Routes 81

11 Configuring the Routing Information Protocol 89
RIP Overview 89
When should you configure RIP? 89
Configuring the VisionNet 202ER's Interfaces with RIP 84
Viewing RIP Statistics 86

12 Configuring the ATM VCC 87
Viewing Your ATM VC Setup 87
Adding ATM VCs 88
Modifying ATM VCs 90

13 Configuring PPP Interfaces 91
Viewing Your Current PPP Configuration 91
Viewing PPP Interface Details 99
Adding a PPP Interface Definition 96
Modifying and Deleting PPP Interfaces 97

14 Configuring EOA Interfaces 99
Overview of EOA 99
Viewing Your EOA Setup 100
Adding EOA Interfaces 102

15 Configuring IPoA Interfaces 105
Viewing Your IPoA Interface Setup 105
Adding IPoA Interfaces 106

16 Configuring Bridging 109

Overview of Bridges 109
Using the Bridging Feature 110
Defining Bridge Interfaces 111
Deleting a Bridge Interface 112

17 Configuring Firewall Settings 113

Configuring Global Firewall Settings 113
Managing the Black List 116

18 Configuring IP Filters 117

Overview 117
Viewing Your IP Filter Configuration 117
Configuring IP Filter Global Settings 118
Creating IP Filter Rules 119
IP filter rule examples 124
Viewing IP Filter Statistics 126
Managing Current IP Filter Sessions 126

19 Viewing DSL Parameters 129

A IP Addresses, Network Masks, and Subnets 132

IP Addresses 132
Structure of an IP address 132
Network classes 133
Subnet masks 133

B Binary Numbers 135

Binary Numbers 135
Bits and bytes 135

C Troubleshooting 137

Diagnosing Problem using IP Utilities.....139
ping 139
nslookup 140

D Glossary..... 141

FCC Compliance Statements

NOTE : This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures :

Reorient or relocate the receiving antenna

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Warning : Modifications not expressly approved by the manufacturer could void the user's authority to operated the equipment under FCC rules

4 Getting Started with the Configuration Manager

The VisionNet 202ER includes 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 VisionNet 202ER via the LAN port.

This chapter describes how to use the Configuration Manager.

Note

The VisionNet 202ER may already be configured to provide Internet connectivity for your network. If it works properly with the preconfigured settings, then you may not need to use the Configuration Manager. Contact your ISP to determine which settings you may need to change, if any.

Accessing the Configuration Manager

The Configuration Manager program is preinstalled into memory on the VisionNet 202ER. 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.
- An web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 6.2, or later versions.

You can access the program from any computer connected to the VisionNet 202ER.

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

   `http://10.0.0.2`

   These are the predefined IP addresses for the LAN ports on the VisionNet 202ER.

   A login screen displays, as shown in ***Figure 7***.

Figure 7. Login Screen

2. Enter your user name and password, and then click OK.
3. The first time you launch the program, use these defaults:

Default User Name:	admin
Default Password :	visionnet

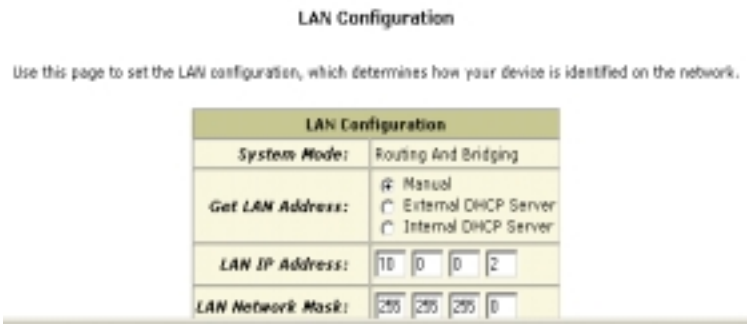
Note

You can change the password at any time (see Changing Your Login Password on page 35). The user name cannot be changed.

The System View page displays each time you launch the program (shown in ***Figure 8*** on page 31).

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, except for the Home tab which displays when you first log in, displays the available tasks horizontally the top of the page. You can click on these to display the specific configuration options.



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*
Save	Stores in *temporary* system memory any changes you have made on the current page. See "Committing your changes" on page 36 for instructions on storing changes permanently.
Refresh	Redisplays the current page with updated statistics.
Clear	When accumulated statistics are displaying, 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 Home Tab displays the System View table when you first access the program:

Figure 8. 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 the various sections of the system view table.

Table Heading	Description
Device	Displays basic information about the VisionNet 202ER hardware and software versions, the system uptime (since the last reboot), and the preconfigured operating mode.
DSL	Displays performance statistics for the DSL line. You can click the **DSL** link in the Advanced title bar 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 15, respectively) for more information about the interfaces defined on you 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 at least one Ethernet interface, named *eth-0*, and may include a USB interface named *usb-0*. You can configure some properties of these interfaces, as described in Chapter 5.
Services Summary	Displays the following service that the VisionNet 202ER performs to help you manage your network: o Translating private IP addresses to your public IP address (NAT, Chapter 8). o Setting up filtering rules that accept or deny incoming or outgoing data. (IP Filter, Chapter 16). o Enabling router-to-router communication (RIP, Chapter 9). o Dynamic assignment or receipt of IP information (DHCP, Chapter 7). o Message forwarding based on Internet Group assignment (IGMP, not configurable).

Changing the System Date and Time

The device keeps a record of the current date and time, which it uses to calculate and report various performance data.

Note

Changing the VisionNet 202ER date and time does not affect the date and time on your PCs.

Follow these instructions to change the date and time:

1. At the bottom of the System View page, click **Modify**.

   The System – Modify page displays in a separate browser window:

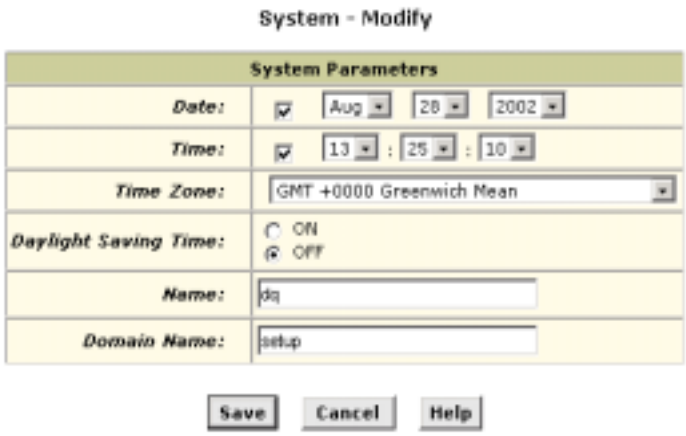


Figure 9. System – Modify Page

2. Use the drop-down lists to select a new date and time.
3. Click **Save**.

   A page displays to confirm your change.
4. Click **Close** to return to the System View page.
5. Click **Save and Reboot** in the Save Setting tab.
6. Click **Save** to save your changes to permanent memory.

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 **Password Configuration** in the Admin tab

   The User Password Configuration page displays by default.

Figure 10. 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 Save.
5. Click **Save and Reboot** in the Save Setting tab.
6. Click Save 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 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 **Save and Reboot** in the Save Setting tab.

   The Save and Reboot page displays:

   Figure 11. Save and Reboot Page

2. Click Save. (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 37).

Rebooting the device using Configuration Manager

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

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 VisionNet 202ER to activate new changes. This button resets the device settings to the manufacturer's default values. Any custom settings will be lost.

5 Setting the LAN IP Address

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

Configuring your LAN IP address

If you are using the ADSL/Ethernet router with multiple PCs on your LAN, you must connect the LAN via an Ethernet hub to the device's LAN port, called eth-0.

You must assign a unique IP address to each device port that you use.

Note

The instructions that follow assume that the device has been preconfigured to operate in Routing mode, which uses the IP protocol to determine how to exchange data among your PCs, the device, and your ISP. If your device is configured in Bridging mode, its ports do not require IP addresses. The operating mode displays at the top of the LAN Configuration page and cannot be changed by the user.

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 port on the network, such as the VisionNet 202ER'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 local 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. In this mode, the ADSL/Ethernet router is considered a *DHCP client* of your DHCP server.

Note

*The VisionNet 202ER itself 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. Launch Configuration Manager, and then click the LAN Config.

   The LAN Configuration page displays, as shown in ***Figure 12***.

Figure 12. LAN Configuration Page

The LAN Configuration table displays the following settings:

Setting	Description
System Mode	The preconfigured 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 preconfigured with a default network mask of 255.0.0.0.
Use DHCP	When checked, this setting instructs the device to accept LAN IP information assigned dynamically from another DHCP server already configured on your network. The VisionNet 202ER cannot 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 DHCP service for the LAN port. Check with your ISP to determine if this is advisable.

     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 Save.

   - 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 **Save and Reboot** in the Save Setting tab.
7. Click Save to save your changes to permanent memory.

6 Viewing System IP Information and Performance Statistics

The interfaces on the VisionNet 202ER that 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 VisionNet 202ER's IP addresses

To view the VisionNet 202ER's IP addresses, click **IP Address** in the System Status tab. The IP Address Table page displays, as shown in ***Figure 13***:

Figure 13. 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 "loopback" IP address, named *lo-0*, of 127.0.0.1. This is a special address that 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.

Viewing IP Global Statistics

You can view statistics on the processing of Internet protocol packets (a packet is a collection of data that has been bundled for transmission). You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

To view global IP statistics, click **Global Stats** on the IP Address Table page. ***Figure 14*** shows the IP Global Statistics page:

IP Global Statistics

IP Datagrams Statistic	Values
IP Received:	366173 Packets
IP Received w/ Header Error:	0 Packets
IP Received w/ Wrong Address:	0 Packets
IP Received w/ Unknown Protocol:	0 Packets
IP Routing Discarded:	0 Packets
IP Datagrams Forwarded	
Forwarded Datagrams:	362615 Packets
Input IP Datagrams	
Input IP Discarded:	0 Packets
Input IP Delivered To User-Protocol:	3552 Packets
Output IP Datagrams	
IP Requests For Transmission w/ User-Protocol:	2958 Packets
Output IP Discarded:	0 Packets
Output IP Discarded w/ No Route:	24 Packets
IP Datagrams / Reassemble	
Maximum # of Seconds IP Waits For Reassemble:	60 Second(s)
IP Received Which Needed To Be Reassembled:	0 Packets
IP Successfully Re-assembled:	0 Packets
IP Fails To Re-Assemble:	0 Packets
IP Datagrams / Fragment	
IP Successfully Fragmented:	0 Packets
IP Fails To Fragment:	0 Packets
IP Fragments Created:	0 Packets

Close Refresh Help

Figure 14. IP Global Statistics Page

To display updated statistics showing any new data since you opened the page, click **Refresh**.

7 Configuring Dynamic Host Configuration Protocol

You can configure your network and VisionNet 202ER to 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 VisionNet 202ER or 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 VisionNet 202ER.

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.

VisionNet 202ER DHCP 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 VisionNet 202ER receives 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 VisionNet 202ER to 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 10.0.0.4 through 10.0.0.15 (subnet mask 255.255.255.0). To change this range of addresses, see "Viewing, modifying, and deleting address pools" on page 50.

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 55.)

2. Launch Configuration Manager, click **DHCP Server** in the LAN tab.

   The DHCP Server Configuration page displays:

   Figure 15. 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:	10 0 1 1
End IP Address:	10 0 1 254
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Netmask:	255 255 255 0
Domain Name:	PoolName
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

Save Cancel Help

Figure 16. DHCP Server Pool – Add Page

4. The *Start IP Address*, *End IP Address*, *Net Mask*, and *Gateway Address* fields are required; the others are optional.

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 78 for an explanation of gateway addresses.
DNS	The IP address of the *Domain Name Server* to be used by computers that receive IP addresses from this pool. The DNS translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, this server is located with your ISP.
SDSN...SWINS (optional)	The IP addresses of devices that perform various services for computers that receive IP addresses from this pool. Typically, these devices are servers located with your ISP. See the glossary for a definition of each type of server.

5. Click Save.

   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 53 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.

  The DHCP Server Pool – Modify page is shown in ***Figure 17***.

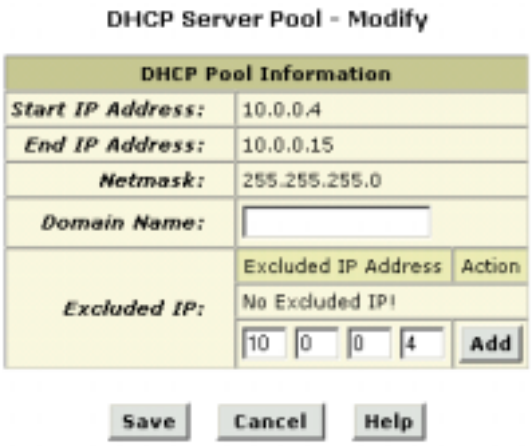


Figure 17. DHCP Server Pool – Modify Page

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 Save after entering your changes. Be sure to use the Commit feature to save your changes to permanent memory, as described on page 36.

Viewing current DHCP address assignments

When the VisionNet 202ER functions 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 the on shown in ***Figure 18***:

DHCP Server Address Table

IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
10.0.0.4	255.255.255.0	00:40:33:A3:A4:BF	10.0.0.4	Dynamic	2591842 Second(s)
10.0.0.5	255.255.255.0	00:50:DA:87:91:2E	10.0.0.4	Dynamic	2598932 Second(s)

Close Refresh Help

Figure 18. 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 VisionNet 202ER contacts 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. Launch the Configuration Manager, click **DHCP Relay** in the LAN tab.

   The DHCP Relay Configuration page displays:

Figure 19. 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 VisionNet 202ER has 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 **Save**.

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 53 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 47 or "Configuring DHCP Relay" on page 52 for additional instructions.

Follow these instructions to set the DHCP mode:

1. Click **DHCP Mode** in the LAN tab
2. Choose **DHCP Server**, **DHCP Relay**.

   If you choose none, your LAN computers must be configured with static IP addresses.
3. Click Save.
4. Click **Save and Reboot** in the Save Setting tab.
5. Click Save 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 VisionNet 202ER, 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 rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are coming from the computer assigned your public IP address (in this case, the VisionNet 202ER).

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 VisionNet 202ER changes 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. The VisionNet 202ER prevents external access your privately addressed computers (except when using an rdr rule discussed on page 65). In addition, the private addresses are replaced in all outbound data packets, so external computers never see the private addresses anyway.

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.

Your Default NAT Setup

By default, NAT is enabled, with an napt rule configured to perform the following translation:

These private IP addresses:	...are translated to:
10.0.0.3 10.0.0.4 . . . 10.0.0.15	Your ISP-assigned public IP address

For a description of napt rules, see page 63. This default NAT setup assumes that, on each LAN computer, you configured TCP/IP properties as follows:

- You selected the check box that enables them to receive their IP addresses automatically (that is, to use a DHCP server);

  or,

- You assigned static IP addresses to your PCs in the range 10.0.0.3 through 10.0.0.32.

If your computers are not configured in one of these ways, you can either change the IP addresses on your computers to match the NAT setup (see the Quick Start instructions, Part 2), or delete this NAT rule and add a new one that matches the addresses you

assigned to your computers (see "Adding NAT Rules" on page 63 for instructions).

Viewing NAT Global Settings and Statistics

To view your NAT settings, launch the Configuration Manager, Click **NAT** in the Virtual Server tab. The NAT Configuration page displays by default, as shown in ***Figure 20***.

Figure 20. 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 settings that apply to all NAT rule translations.
- Buttons you use to submit or cancel changes, display global statistics, and access help.

The NAT Global Information table contains the following fields:

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 Save, and then click the Admin tab and commit your changes to permanent system memory (see page 36).

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 21*** 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
Number Of Fragments Processed:	0 Packets
Active NAT Sessions	
Active Translation Sessions:	0 Sessions

Figure 21. 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 22***.

Figure 22. 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 a rule of the specified flavor (pages 63 through 72).

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 23*** displays:

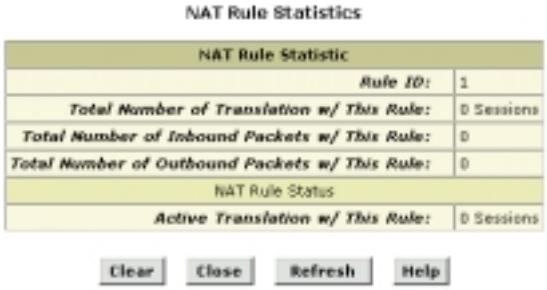
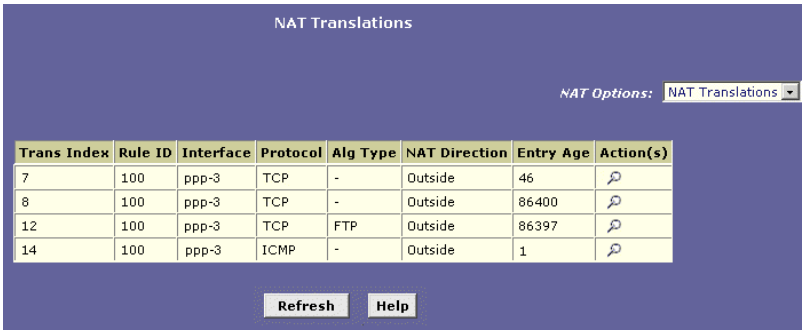


Figure 23. NAT Rule Statistics Page

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 24***:



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 24. 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 25***.

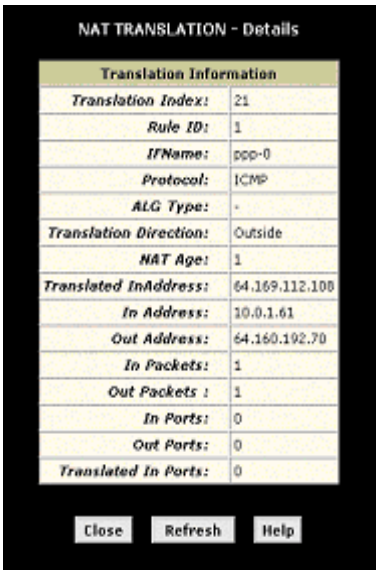


Figure 25. NAT Translation – Details Page

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 InAddress	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 57). The Introduction to NAT on page 55 describes how the napt rule works.

1. Click **NAT** in the Virtual Server 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 26***.

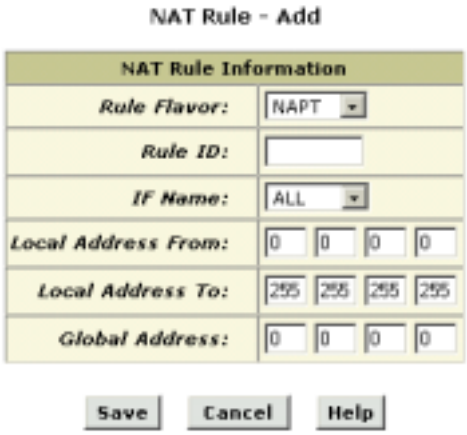


Figure 26. NAT Rule – Add Page (napt Flavor)

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 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 Save.

   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 Save.

   A page displays to confirm your changes.

10. Click **Save and Reboot** in the Save Setting tab.

11. Click Save 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 bimap rule described on page 71), the VisionNet 202ER blocks 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 27 shows the fields used to establish an rdr rule:

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

Follow these instructions to add an rdr rule (see steps 1-4 under "The napt rule" on page 63 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 4 and 5 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 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 63 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 28 shows the fields used for adding a basic rule.

Figure 28. NAT Rule – Add Page (basic Flavor)

Follow these instructions to add an basic rule (see steps 1-4 under "The napt rule" on page 63 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.

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

   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 to which to translate your private addresses. 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 63 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 68 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 29 shows the fields used to establish a filter rule.

Figure 29. NAT Rule—Add Page (filter Flavor)

Follow these instructions to add a filter rule (see steps 1-4 under "The napt rule" on page 63 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 63 to submit your changes.

The bimap rule: Performing two-way translations

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

In the incoming direction, when the specified VisionNet 202ER interface 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.

Bimap 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. Bimap 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 30 shows the fields used to establish a bimap rule.

Figure 30. NAT Rule – Add Page (bimap Flavor)

Follow these instructions to add a bimap rule (see steps 1-4 under "The napt rule" on page 63 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 63 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.

Figure 31. 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 63 for specific 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 63 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 47 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., 10.0.0.2). 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 that it receives on its LAN port to a DNS server at the ISP. It then relays the response to the PC.

When performing DNS relay, the VisionNet 202ER must 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, configure it to "Use DNS" 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. the WAN tab, and then click **DNS** in the task bar. The DNS Configuration page displays.

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 **Save**.

3. Click **Save and Reboot** in the Save Setting tab.

4. Click **Save** 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 an 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.

10 Configuring IP Routes

You can use Configuration Manager to define specific routes for your Internet and network data. This chapter describes basic routing concepts and provides instructions for creating routes.

Note that most users do not need to define IP routes.

Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to. When you define IP routes, you provide the rules that a device uses to make these decisions.

Comparing IP routing to telephone switching

IP routing decisions are similar to those made by switchboards that handle telephone calls.

When you dial a long distance telephone number, you are first connected to a switchboard operated by your local phone service carrier. All calls you initiate go first to this main switchboard.

If the phone number you dialed is outside your calling area, the switchboard opens a connection to a higher-level switchboard for long distance calls. That switchboard looks at the area code you dialed and connects you with another switchboard that serves that area. This new switchboard, in turn, may look at the prefix in the number you dialed (the middle set of three numbers) and connect to a more localized switchboard that handles numbers with that prefix. This final switchboard can then look at the last four digits of the phone number to open a connection with the person or company you dialed.

In comparison, when your computer initiates communication over the Internet, such as viewing a web page connecting to an web server, the data it sends out includes the IP address of the destination computer (the "phone number"). All your outgoing requests first go to the same router at your ISP (the first "switchboard"). That router looks at the network ID portion of the destination address (the "area code") and determines which next router to send the request to. After several such passes, the request arrives at a router for the destination network, which then uses the host ID portion of the destination IP address (the local "phone number") to route the request to the appropriate computer. (The network ID and host ID portions of IP addresses are explained in Appendix A..)

With both the telephone and the computer, all transactions are initially sent to the same switchboard or router, which serves as a gateway to other higher- or lower-level devices. No single device knows at the outset the eventual path the data will take, but each uses a specific part of the destination address/phone number to make a decision about which device to connect to next.

Hops and gateways

Each time Internet data is passed from one Internet address to another, it is said to take a *hop*. A hop can be a handoff to a different port on the same device, to a different device on the same network, or to a device on an entirely different network.

When a hop passes data from one type of network to another, it uses a *gateway*. A gateway is an IP address that provides initial access to a network, just as a switchboard serves as a gateway to a specific set of phone numbers. For example, when a computer on your LAN requests access to a company's web site, your ISP serves as a gateway to the Internet. As your request reaches its destination, another gateway provides access to the company's web servers.

Using IP routes to define default gateways

IP routes are defined on computers, routers, and other IP-enabled devices to instruct them which hop to take, or which gateway to use, to help forward data along to its specified destination.

If no IP route is defined for a destination, then IP data is passed to a predetermined *default gateway*. The default gateway serves like a higher-level telephone switchboard; it may not be able to connect directly to the destination, but it will know a set of other devices that can help pass the data intelligently. If it cannot determine which of these devices provides a good next hop (because no such route has been defined), then that device will forward the data to *its* default gateway. Eventually, a high level device, using a predefined IP route, will be able to forward the data along a path to its destination.

Do I need to define IP routes?

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the VisionNet 202ER provide the most appropriate path for all your Internet traffic.

- On your LAN computers, a default gateway directs all Internet traffic to the LAN port on the VisionNet 202ER. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in the Quick Start instructions, Part 2.)
- On the VisionNet 202ER itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection. (The process for adding a default route is described on page 81.)

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

Viewing the IP Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these *destination IP addresses*, the table lists the IP address of the first hop the data should take. This table is known as the device's *routing table*.

To view the VisionNet 202ER's routing table, the System Status tab, and then click **Routing Table** in the task bar. The IP Route page displays by default, as shown in ***Figure 32. IP Route Table Page***:

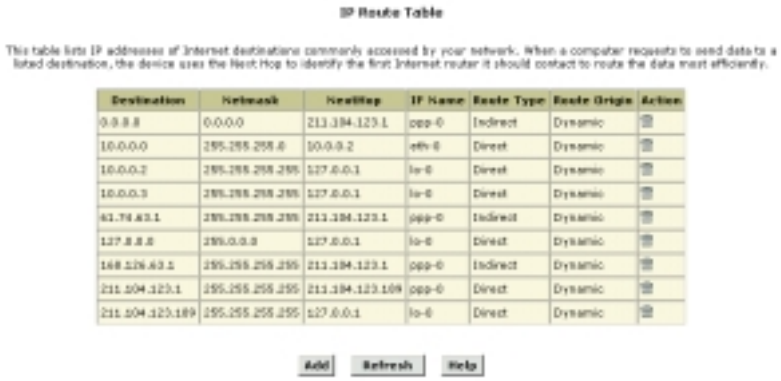


Figure 32. IP Route Table Page

The IP Route Table displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

The following table defines the fields in the IP Routing Table.

Table 3. IP Routing Table Fields

Field	Description
Destination	Specifies the IP address of the destination computer. The destination can specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Netmask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to Appendix A, for an explanation of network masks. The default gateway uses a netmask of 0.0.0.0.
NextHop	Specifies the *next* IP address to send data to when its final destination is that shown in the destination column.
IFName	Displays the name of the interface on the device through which data is forwarded to the specified next hop.
Route Type	Displays whether the route is direct or indirect. In a *direct* route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an *indirect* route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.
Route Origin	Displays how the route was defined. *Dynamic* indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled *Local*. Other routes can be created automatically (using RIP, as described in Chapter 9), or defined remotely through various network management protocols (LCL or ICMP).
Action	Displays an icon ( ) you can click on to delete a route.

Adding IP Routes

Follow these instructions to add an IP route to the routing table.

1. From the IP Route Table page, click **Add**.

   The IP Route – Add page displays, as shown in ***Figure 33***.

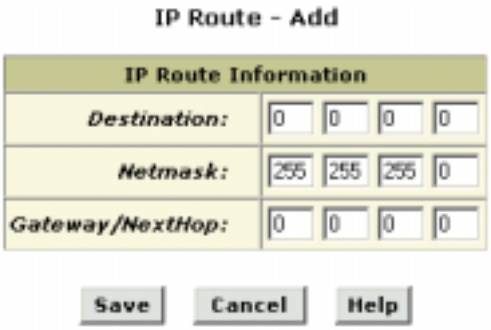


   Figure 33. IP Route – Add Page

2. Specify the destination, network mask, and gateway or next hop for this route.

   For a description of these fields, refer to Table 3 on page 80.

   To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination and Net Mask fields. Enter your ISP's IP address in the Gateway/NextHop field.

   Note that you cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3. Click **Save**.

4. On the confirmation page, click **Close** to return to the IP Route table page.

The IP Routing Table will now display the new route.

5. Click **Save and Reboot** in the Save Setting tab.

6. Click **Save** to save your changes to permanent memory.

11 Configuring the Routing Information Protocol

The VisionNet 202ER can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. Routing devices communicate this information using a variety of IP protocols. This chapter describes how to configure the VisionNet 202ER to use one of these, called the Routing Information Protocol (RIP).

RIP Overview

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Generally, RIP is used to enable communication on *autonomous* networks. An autonomous network is one in which all of the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closest neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

When should you configure RIP?

Most small home or office networks do not need to use RIP; they have only one router, such as the VisionNet 202ER, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the VisionNet 202ER). The VisionNet 202ER and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should *both* be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

Configuring the VisionNet 202ER's Interfaces with RIP

The following instructions describe how to enable RIP on the VisionNet 202ER.

Note

In order for the VisionNet 202ER to communicate with other devices using RIP, you must also enable the other devices to use the protocol. See the product documentation for those devices.

1. Launch the Configuration Manager, the Security tab, and then click **RIP** in the task bar.

   The RIP Configuration page displays, as shown in ***Figure 34***.

   Figure 34. RIP Configuration Page

   The page contains radio buttons for enabling or disabling the RIP feature and a table listing interfaces on which the protocol is currently running. The first time you open this page, the table may be empty.

2. If necessary, change the Age and Update Time.

   These are global settings for all interfaces that use RIP.

   - *Age* is the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.
   - *Update Time* specifies how frequently the VisionNet 202ER will send out its routing table its neighbors.

3. In the IFName column, select the name of the interface on which you want to enable RIP.

   For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface.

   For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

   (See page 43 for a description of various interfaces and their names.)

4. Select a metric value for the interface.

   RIP uses a "hop count" as a way to determine the best path to a given destination in the network. The hop count is the sum of

the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.

For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others.

You can select any integer from 1 to 15.

5. Select a Send and Receive Modes.

   The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices.

   The Receive Mode setting indicates the RIP version(s) in which information must be passed to the VisionNet 202ER in order for it to be accepted into its routing table.

   RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

   RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.

6. Click Add.

   The new RIP entry will display in the table.

7. Click the **Enable** radio button to enable the RIP feature.

Note

If you disable the RIP feature, the interface settings you have configured will remain available for future activation.

8. When you are finished defining RIP interfaces, click Save.

   A page displays to confirm your changes.

9. Click **Save and Reboot** in the Save Setting tab.

10. Click Save to save your changes to permanent memory.

Note

You can delete an existing RIP entry by clicking in the Action column.

Viewing RIP Statistics

From the RIP Configuration page, you can click **Global Stats** to view statistics on attempts to send and receive route table data over RIP-enabled interfaces on the VisionNet 202ER.

RIP Global Statistics

RIP Active Sessions	
Request Sent:	0 Packets
Response Sent:	0 Packets
Request Received:	0 Packets
RIP Packets w/ Error	
Packets Received w/ Bad Version:	0 Packets
Packets Received w/ Bad Address Family:	0 Packets
Packets Received w/ Bad Request Format:	0 Packets
Packets Received w/ Bad Metrics:	0 Packets
Packets Received w/ Bad Response Format:	0 Packets
Packets Received w/ Invalid Port:	0 Packets
Packets Rejected:	0 Packets
Response Received:	0 Packets
Unknown Packets Received:	0 Packets
Packets Received from Non-Neighbor Router:	0 Packets
Packets Rejected for Authentication Failure:	0 Packets
Packets w/ Route Changed:	0 Packets

Clear Close Refresh Help

Figure 35. RIP Global Statistics Page

You can click **Clear** to reset all statistics to 0 and **Refresh** to display any newly accumulated data.

12 Configuring the ATM VCC

As your LAN computers access the Internet via the VisionNet 202ER, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called *Asynchronous Transfer Mode* (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

This chapter describes how to configure the ATM *virtual channel* (VC). The VC properties define the path the VisionNet 202ER uses to communicate with your ISP over the ATM network.

Viewing Your ATM VC Setup

To view your current configuration, launch Configuration Manager, the WAN tab, and then click **ATM VC** in the task bar. The ATM VC Configuration page displays, as shown in ***Figure 36***.

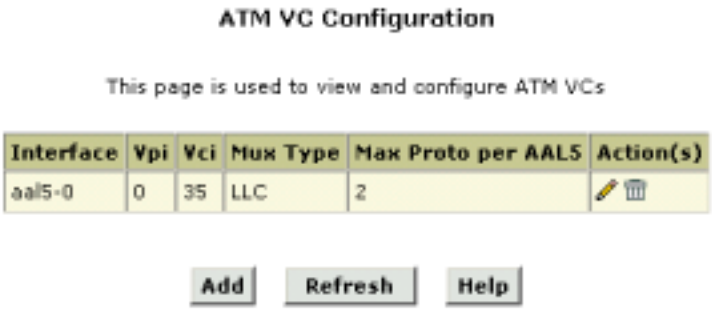


Figure 36. ATM VCC Configuration Page

The ATM VCC Configuration table displays the following fields (contact your ISP to determine these settings):

Field	Description
Interface	The name of the lower-level interface on which this VC operates. The low-level interface names are preconfigured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an AAL5-type interface.
Vpi, Vci, and Mux Type	These settings identify a unique ATM data path for communication between your ADSL/Ethernet router and your ISP.
Max Proto per AAL5	If you are using an AAL5-type of interface, this setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). Contact your ISP to determine which connection protocol(s) they require.
Actions	Displays an icon ( ) you can click on to delete the associated interface.

Adding ATM VCs

You may need to create a VC if none has been predefined on your system or if you use multiple services with your ISP. Each service may require its own VC. Follow these instructions to add a VC:

1. From the ATM VC Configuration page, click **Add**.

   The ATM VCC – Add page displays, as shown in ***Figure 37***.

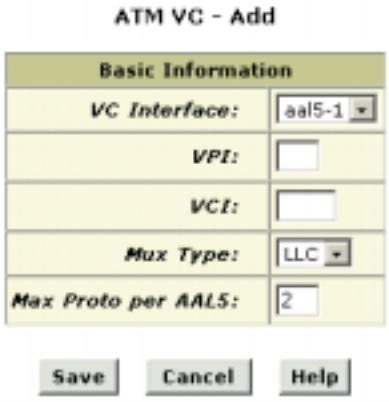


Figure 37. ATM VCC – Add Page

2. Select an interface name from the VCC Interface drop-down list.
3. Enter the VPI and VCI values assigned by your ISP, and select the mux type from the drop-down list.
4. Click Save.
5. On the confirmation page, click Close to return to the ATM VC Configuration page.
6. Click **Save and Reboot** in the Save Setting tab.
7. Click Save to save your changes to permanent memory.

   The new interface should now display in the ATM VCC Configuration table.

You may need to create a new WAN interface, or modify an existing interface, so that it uses the new VC. See the instructions for configuring a PPP (Chapter 12), EoA (Chapter 14), or IPoA (Chapter 15) interfaces, depending on the type you use to communicate with your ISP.

You can verify that the new settings work by attempting to access the Internet from a LAN computer. Contact your ISP for troubleshooting assistance.

Modifying ATM VCs

Your device may already be preconfigured with the necessary ATM VC properties, or the table may contain placeholder values that you must change before using the device. Contact your ISP to determine your ATM VC values. Follow these instructions to modify a preconfigured VC:

1. From the ATM VC Configuration page, click in the Actions column for the interface you want to modify.

   The ATM VCC Interface – Modify page displays, as shown in ***Figure 37***.

   ATM VC Interface - Modify

Basic Information	
VC Interface:	aal5-0
VPI:	0
VCI:	35
Mux Type:	LLC
Max Proto per AAL5:	2

   Save Cancel Help

   Figure 38. ATM VCC Interface – Modify Page

2. Enter the new VPI and VCI values, select the MUX type, or change the maximum number of protocols that the VC can carry, as directed by your ISP.

   You cannot modify the interface type over which an existing VC operates (aal5-0, for example). If you want to change the interface type, you must delete the existing interface, create a new one, and select the desired interface type.

3. Click Save.

4. On the confirmation page, click Close to return to the ATM VC Configuration page.

5. Click **Save and Reboot** in the Save Setting tab.

6. Click Save to save your changes to permanent memory.

You can verify that the new settings work by attempting to access the Internet from a LAN computer. Contact your ISP for troubleshooting assistance.

13 Configuring PPP Interfaces

When powered on, the VisionNet 202ER initiates a connection through your DSL line to your ISP.

The PPP protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password
- Enabling the ISP to assign Internet information to the customer's computers

Your ISP may or may not use the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

Viewing Your Current PPP Configuration

To view your current PPP setup, launch the Configuration Manager, the WAN tab, and then click **PPP** in the task bar. The PPP Configuration page displays a table with basic information about your PPP setup, as shown in ***Figure 39***.

Figure 39. PPP Configuration Page

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the VisionNet 202ER can be defined with more than one group of PPP settings. Each group of settings is called a *PPP interface* and is given a name, such as *ppp-0*, *ppp-1*, etc.

You can configure the following settings on the PPP Configuration page:

- **Inactivity TimeOut (mins)**: The time in minutes that must elapse before a PPP connection times out due to inactivity.
- **Ignore WAN to LAN traffic**: When enabled, data traffic traveling in the incoming direction—from the WAN port to the LAN port—will not count as activity on the WAN port; i.e., it will not prevent the connection from being terminated if inactive for the specified time.

The PPP Configuration Table displays the following fields:

Field	Description
Interface	The predefined name of the PPP interface.
VCC	The Virtual Channel Connection over which this PPP data is sent. The VCC identifies the physical path the data takes to reach your ISP. See Chapter 12 for more information.
IPF Type	The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ): o A public interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. o A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. o The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPoE) or PPP-over-ATM (PPoA).
WAN IP	The IP address currently assigned to your WAN (DSL) port by your ISP.
Gateway IP	The IP address of the server at your ISP that provides you access to the Internet. See "Hops and gateways" on page 78 for a description of gateway addresses.
Default Route	Indicates whether the ADSL/Ethernet router should use the IP address assigned to this connection as its default route. Can be Enabled or Disabled. See Chapter 10 for an explanation of default routes.

Field	Description
Use DHCP	When set to *Enable*, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. With Use DHCP enabled, the device will acquire IP addresses for various other server types (WINS, SMTP, POP3, etc. -- these server types are listed on the DHCP Server Configuration page).
User DNS	When set to *Enable*, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the ADSL/Ethernet Router is configured to act as a DHCP Server for your LAN. When set to *Disable*, LAN hosts will use the DNS address(es) preconfigured in the DHCP pool (see "Configuring DHCP Server" on page 47) and in the DNS feature (see Chapter 9, "Configuring DNS Server Addresses").
Oper. Status	Indicates whether the link is currently up or down or if a specific type of data exchange is under way (e.g., password authorization or DHCP).
Actions	You can use these icons to modify ( ), delete ( ), and view additional details on ( ) the PPP interface.

Viewing PPP Interface Details

When you click to view additional details, the PPP Interface - Detail page displays, as shown in ***Figure 40***.

PPP Interface - Detail

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
IPF Type:	Public
Status:	Start
Protocol:	PPPoE
Service Name:	-
Use Dhcp:	Disable
Use DNS:	Enable
Default Route:	Enable
Oper. Status:	Link Down
Last Fail Cause:	Unknown
PPP IP Status	
WAN IP Address:	0.0.0.0
Gateway IP Address:	0.0.0.0
DNS:	0.0.0.0
SDNS:	0.0.0.0
Security Information	
Security Protocol:	PAP
Login Name:	guest

Close Refresh Help

Figure 40. PPP – Detail Page

In addition to the properties defined on page 92, the PPP Interface – Detail table displays these fields:

Field	Description
Status	Indicates whether the interface has been specified in the system as: o Enabled: A connection will be established for use when the device is turned on or rebooted. o Disabled: The PPP interface cannot currently be used. o Start On Data: The PPP connection will be made only when data is sent to the interface (e.g., when a LAN user attempts to use the internet).
Service Name	The name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties.

Field	Description
Last Fail Cause	Indicates the action that ended the previous PPP session: o No Valid PADO Recvd: The unit initiated a PPoE handshake but did not receive a packet in reply from the ISP. o No Valid PADS Recvd: After the initial handshake, the unit did not receive a confirmation packet from the ISP. o Stopped by User: The user stopped the connection (for example, by changing the Configuration Manager settings for the PPP interface.) o No Activity: The PPP communication timed out, in accordance with the timeout period specified on the PPP Configuration page. o Auth Failure: The ISP could not authorize the connection based on the user name and/or password provided. o PADT recvd: The ISP issued a special packet type to terminate the PPP connection. o VC down: The Virtual Circuit between the unit and the ISP is down. o Internal failure: A system software failure occurred.
DNS	The IP address of the DNS server (located with your ISP) used on this PPP connection.
SDNS	The IP address of the secondary DNS server (located with your ISP) used on this PPP connection.
Security Protocol	The type of PPP security your ISP uses: *PAP* (Password Authentication Protocol) or *CHAP* (Challenge Handshake Authentication Protocol).
Login Name	The name you use to log in to your ISP each time this PPP connection is established.

Adding a PPP Interface Definition

If you intend to use more than one type of service from your ISP, the device may be configured with multiple PPP interfaces, each with unique logon and other properties. Follow this procedure to define properties for a PPP interface:

1. From the PPP Configuration Page, click **Add**.

   The PPP Interface – Add page displays, as shown in ***Figure 41***.

Figure 41. PPP Interface – Add Page

2. Select a PPP interface name from the drop-down list, and then enter or select data for each field.

Note

You can create multiple PPP interfaces only if you are using the PPoA protocol; only one PPP interface can be define if you are using PPoE. Check with your ISP which version of the protocol they require.

   The fields are defined in the tables on page 92 and 94.

3. Click **Save**.

   A page displays to confirm your changes.

4. Click Close to return to the PPP page and view the new interface in the table.
5. Click **Save and Reboot** in the Save Setting tab.
6. Click Save to save your changes to permanent memory.

Modifying and Deleting PPP Interfaces

To modify a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to modify. The PPP Interface – Modify page displays, as shown in ***Figure 42***.

Figure 42. PPP Interface – Modify

You can change only the status of the PPP connection, the security protocol, your login name, and your password. To modify the other settings, you must delete the interface and create a new one. To modify the other settings, you must delete the interface and create a new one.

To delete a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to delete. You should not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you will not be able to connect to your ISP. You can recreate the PPP interface with the same name at a later time.

After modifying or deleting a PPP interface, click Save. Then, display the Save Setting tab, click **Save and Reboot** in the task bar, and click Save to save your changes to permanent memory.

Note

Bridges vs. Routers: *The essential difference between a bridge and a router is that a router uses a higher-level protocol (such as the IP) to determine how to pass data. IP data packets contain IP addresses that specifically identify the destination computer. Routers can read this information and pass the data to the destination computer, or determine which next router to send the data to if the destination is not on a connected network.*

Bridges cannot read or use IP information, but instead use the manufacturer-assigned hardware IDs to determine the port through which it should send the data packet.

Routers are considered more intelligent and flexible devices than bridges, and often provide a variety of security and network administration services.

Using the Bridging Feature

Although the VisionNet 202ER is preconfigured to serve as a router for providing Internet connectivity to you LAN, there are several instances in which you may also want to configure bridging:

- Your ISP may use protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- Your LAN may include computers that communicate using "layer-3" protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

In both cases, you need to specify the device's interfaces as bridge interfaces.

Defining Bridge Interfaces

To enable bridging, you simply specify the device interfaces on which you want to bridge data, and then enable bridging mode:

1. Launch Configuration Manager and click the **Bridging** in the WAN tab.

   The Bridge Configuration page displays, as shown in ***Figure 47***.

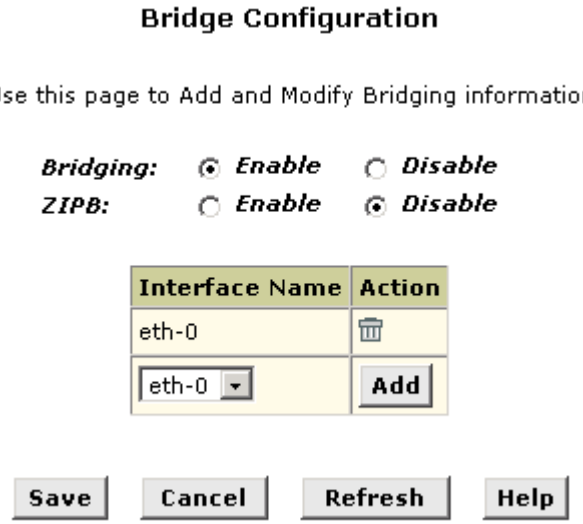


Figure 47. Bridge Configuration Page

   The table may be empty if bridging has not yet been established.

2. Select the interface names on which you want to perform bridging and click **Add**.

   For example, select *eth-0* (LAN) and *eoa-0* (WAN) interfaces.

Note

If you do not have an eoa-0 interface, but instead have an interface named ppp-0 *or* ipoa-0*, your device is not currently configured with a WAN interface that allows bridging with your ISP. You may want to check with your ISP to determine whether they use the eoa protocol. See Chapter 14 for instructions on creating an EOA interface.*

Note

If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.

You can determine whether the Ethernet (eth-0) has been assigned IP addresses by displaying the IP Address Table (display the Routing tab, and then click **IP Address***). These interfaces will display in the table only if they have been assigned IP addresses.*

You can check whether the eoa-0 interface has been assigned an IP address by displaying the EOA configuration table (display the WAN tab, and then click **EOA***). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.*

3. Click the **Enable** radio button to turn on bridging.
4. Click Save.

   A page will briefly display to confirm your changes, and will return you to the Bridge Configuration page.
5. Click **Save and Reboot** in the Save Setting tab.
6. Click Save to save your changes to permanent memory.

Deleting a Bridge Interface

To make an interface non-bridgeable, display the Bridge Configuration page and click next to the interface you want to delete. Click OK to confirm the deletion. The interface remains defined in the system, but is no longer capable of performing bridging.

17 Configuring Firewall Settings

Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

Configuring Global Firewall Settings

Follow these instructions to configure global firewall settings:

1. Launch Configuration Manager, click **Firewall** in the Security tab.

   The Firewall Configuration page displays, as shown in ***Figure 48***.

Figure 48. Firewall Configuration Page

Note that the Firewall Configuration page contains a drop-down list on the right side of the page that enables you to view Firewall settings, as discussed in this chapter, or configure IP Filters, as discussed in Chapter 18.

2. Configure any of the following settings that display in the Firewall Global Information table:

Field	Description
Black List Status	If you want the device to maintain and use a black list, click *Enable*. Click *Disable* if you do not want to maintain a list.
Black List Period(min)	Specifies the number of minutes that a computer's IP address will remain on the black list (i.e., all traffic originating from that computer will be blocked from passing through any interface on the ADSL/Ethernet router). For more information, see "Managing the Black List" on page 116.
Attack Protection	Click the *Enable* radio button to use the built-in firewall protections that prevent the following common types of attacks: o IP Spoofing: Sending packets over the WAN interface using an internal LAN IP address as the source address. o Tear Drop: Sending packets that contain overlapping fragments. o Smurf and Fraggle: Sending packets that use the WAN or LAN IP broadcast address as the source address. o Land Attack: Sending packets that use the same address as the source and destination address. o Ping of Death: Illegal IP packet length.
DoS Protection	Click the Enable radio button to use the following denial of service protections: o SYN DoS o ICMP DoS o Per-host DoS protection
Max Half open TCP Connection	Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
Max ICMP Connection	Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as the are initiated.
Max Single Host Connection	Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.

Field	Description
Log Destination	Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility Ethernet to (*Trace*) or can e-mailed to specified administrators.
E-mail ID of Admin 1/2/3	Specifies the e-mail addresses of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard internet e-mail address format, e.g., *jxsmith@onecompany.com*. The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3. Click Save.
4. Click **Save and Reboot** in the Save Setting tab.
5. Click Save to save your changes to permanent memory.

Managing the Black List

If data packets are received that violate the firewall settings or any of the IP Filter rules, then the source IP address of the offending packets can be blocked from such accesses for a specified period of time. You can enable or disable use of the black list using the settings described above. The source computer remains on the black list for the period of time that you specify.

To view the list of currently blacklisted computers, click **Black List** at the bottom of the Firewall Configuration page. The Black List page displays, as shown in ***Figure 49***.

Figure 49. Firewall Blacklisted Hosts Page

The table displays the following information for each entry:

Field	Description
Host IP Address	The IP address of the computer that sent the packet(s) that caused the violation
Reason	A short description of the type of violation. If the packet violated an IP Filter rule, the custom text from the Log Tag field will display. (See "Creating IP Filter Rules" on page 119.)
IPF Rule ID	If the packet violated an IP Filter rule, this field will display the ID assigned to the rule.
Action(s)	Displays an icon (🗑) you can click on to delete the entry from the list (if you want it to be removed prior to its automatic timed expiration.

18 Configuring IP Filters

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet. This chapter explains how to create IP filter rules.

Overview

The IP filter feature enables you to control the types of data being passed between the Internet and your network. You can create IP filter rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN.

When you define an IP filter rule and enable the feature, you instruct the VisionNet 202ER to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the size of the packet, the network or internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can be either accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

Viewing Your IP Filter Configuration

To view your current IP filter configuration, launch Configuration Manager, click **IP Filter** in the Security tab. The IP Filter page displays, as shown in ***Figure 50***.

Figure 50. IP Filter Page

The IP Filter Configuration page displays global settings that you can modify, and the IP Filter rule table, which shows all currently established rules. See "Creating IP Filter Rules" on page 119 for a

description of the items that make up a rule. When rules are defined, you can use the icons that display in the Actions column to ( ), delete ( ), and view details on ( ) the corresponding rule.

Configuring IP Filter Global Settings

The IP Filter Configuration page enables you to configure several global IP Filter settings, and displays a table showing all existing IP Filter rules. The global settings that you can configure are:

- **Security Level:** This setting determines which IP Filter rules take effect, based on the security level specified in each rule. For example, when *High* is selected, only those rules that are assigned a security value of *High* will be in effect. The same is true for the *Medium* and *Low* settings. When *None* is selected, IP Filtering is disabled.
- **Private/Public/DMZ Default Action:** This setting specifies a default action to be taken (Accept or Deny) on private, public, or DMZ-type device interfaces when they receive packets that *do not* match any of the filtering rules. You can specify a different default action for each interface type. (You specify and interface's type when you create the interface; see the PPP configuration page, for example.)
  - A *public* interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is *Deny*, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.
  - A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. Typically, the global setting for private interfaces is *Accept*, so that LAN computers have access to the ADSL/Ethernet routers' Internet connection.
  - The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface—a whether from a LAN or external source—are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to *Deny* so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

Creating IP Filter Rules

To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule, and refer to the examples on page 124 for assistance:

1. On the main IP Filter page, click **Add**.

   The IP Filter Rule – Add page displays, as shown in ***Figure 51***.

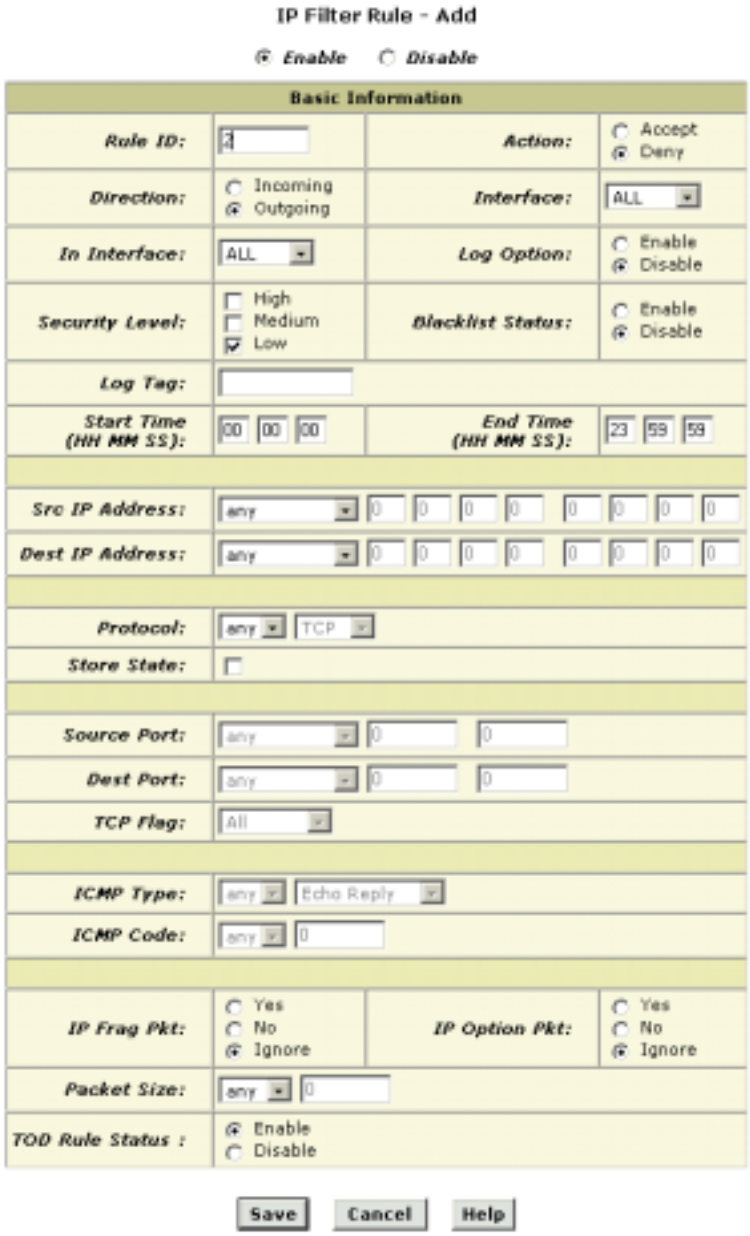


Figure 51. IP Filter Rule – Add Page

2. Enter or select data for each field that applies to your rule. The following table describes the fields:

Field	Description
Rule ID	Each rule must be assigned a sequential ID number. Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., *10*, *20*, *30*) so that you leave enough room between them for inserting a new rule if necessary.
Action	Specifies the action that will be taken when a packet matches the rule criteria. The action can be *Accept* (forward to destination) or *Deny* (discard the packet).
Direction	Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. *Incoming* refers to packets coming from the LAN, and *outgoing* refers to packets going to the Internet. You can use rules that specify the incoming direction to prevent outside accesses to your LAN.
Interface	Specifies the interface on the VisionNet 202ER on which the rule will take effect. See the examples on page 124 for suggestions on choosing the appropriate interface for various rule types.
In Interface	Specifies the interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction.
Log Option	When *Enabled* is selected, a log entry will be created on the system each time this rule is invoked. The log entry will include the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring in the previous x minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to designated administrators. See Chapter 17, "Configuring Firewall Settings" for instructions.
Security Level	Specifies the security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive.

Field	Description
Black List Status	Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the ADSL/Ethernet router from forwarding packets from that source for a specified period of time. See Chapter 17, "Configuring Firewall Settings" for instructions.
Log Tag	Specifies a description up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to *Enable* if you configure a Log Tag.
Start/End Time	The time range during which this rule is to be in effect, specified in military units.
Src IP Address	Specifies IP address criteria for the source computer(s) from which the packet originates. In the drop-down list, you can configure the rule to be invoked on packets containing: **any**: any source IP address. **lt**: *any* source IP address that is numerically *less than* the specified address. **lteq**: any source IP address that is numerically *less than or equal to* the specified address. **gt**: any source IP address that is numerically *greater than* the specified address. **eq**: any source IP address that is numerically *equal to* the specified address. **neq**: any source IP address that is *not equal to* the specified address. **range**: any source IP address that is within the specified range, inclusive. **out of range**: any source IP address that is outside the specified range. **self**: the IP address of the ADSL/Ethernet router interface on which this rule takes effect.
Dest IP Address	Specifies IP address rule criteria for the destination computer(s) (i.e., the IP address of the computer to which the packet is being sent). In addition to the options described for the Src IP Address field, the following option is available: **bcast**: Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select this option, you do not need to specify the address, so the address fields are dimmed.

Field	Description
Protocol	Specifies the basic IP protocol criteria that must be met for rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (*eq*), that they must not contain the specified protocol (*neq*), or that the rule can be invoked regardless of the protocol (*any*). TCP, UDP, and ICMP are commonly IP protocols; others can be identified by number from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).
Store State	If this option is enabled, then *stateful filtering* is performed and the rule is also applied in the other direction on the given interface during an IP session.
Source Port	Specifies port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) if you have not specified a protocol criteria. See the description of Src IP Address for the selection options.
Dest Port	Specifies port number criteria for the destination computer(s) (i.e., the port number of the type of computer to which the packet is being sent). This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.
TCP Flag	Specifies whether the rule should apply only to TCP packets that contain the synchronous (*SYN*) flag, only to those that contain the non-synchronous (*NOT-SYN*) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.
ICMP Type	Specifies whether the value in the type field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.

Field	Description
ICMP Code	Specifies whether the value in the code field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
IP Frag Pkt	Determines how the rule applies to IP packets that contain fragments. You can choose from the following options: o **Yes**: The rule will be applied only to packets that contain fragments. o **No**: The rule will be applied only to packets that do not contain fragments. o **Ignore**: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.
IP Option Pkt	Determines whether the rule should apply to IP packets that have options specified in their packet headers. o **Yes:** The rule will be applied only to packets that contain header options. o **No:** The rule will be applied only to packets that do not contain header options. o **Ignore:** (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.
Packet Size	Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criteria. (*lt* = less than, *gt* = greater than, *lteq* = less than or equal to, etc.)
TOD Rule Status	The Time of Day Rule Status determines how the Start Time/End Time settings are used. o **Enable:** (Default) The rule is in effect for the specified time period. o **Disable:** The rule is not in effect for the specified time period, but is effective at all other times.

3. When you are done selecting criteria, ensure that the Enable radio button is selected at the top of the page, and then click Save.

   After a confirmation page displays, the IP Filter Configuration page will redisplay with the new rule showing in the table.

   If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different than the globally configured level.

4. Ensure that the Security Level and Private/Public/DMZ Default Action settings on the IP Filter Configuration page are configured as needed, then click Save

   A page displays to confirm your changes.

5. Click **Save and Reboot** in the Save Setting tab.

6. Click Save to save your changes to permanent memory.

IP filter rule examples

Example 1. Blocking a specific computer on your LAN from using accessing web servers on the Internet:

1. Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0, for example).
2. Specify a source IP address of the computer you want to block.
3. Specify the Protocol = *TCP* and enable the Store State setting.
4. Specify a destination port = *80*, which is the well-known port number for web servers.
5. Enable the rule by clicking the radio button at the top of the page.
6. Click Save to create the rule.
7. On the IP Filter Configuration page, set the Security Level to the same level you chose for the rule, and set both the Private Default Action and the Public Default Action to *Accept*.
8. Click Save, and commit your changes.

Figure 51 on page 119 shows the configuration for this rule. The specified computer will not be able to access the Web, but will be able to access FTP Internet sites (and any others that use destination port numbers other than 80).

Example 2. Blocking Telnet accesses to the VisionNet 202ER:

1. Add a new rule for incoming packets incoming on the ppp-0 interface.
2. Specify that the packet must contain the TCP protocol, and must be destined for port 23, the well-known port number used for the Telnet protocol.
3. Enable the rule by clicking the radio button at the top of the page.
4. Click Save to create the rule, and save your changes.

Figure 52 shows how this rule could be configured:

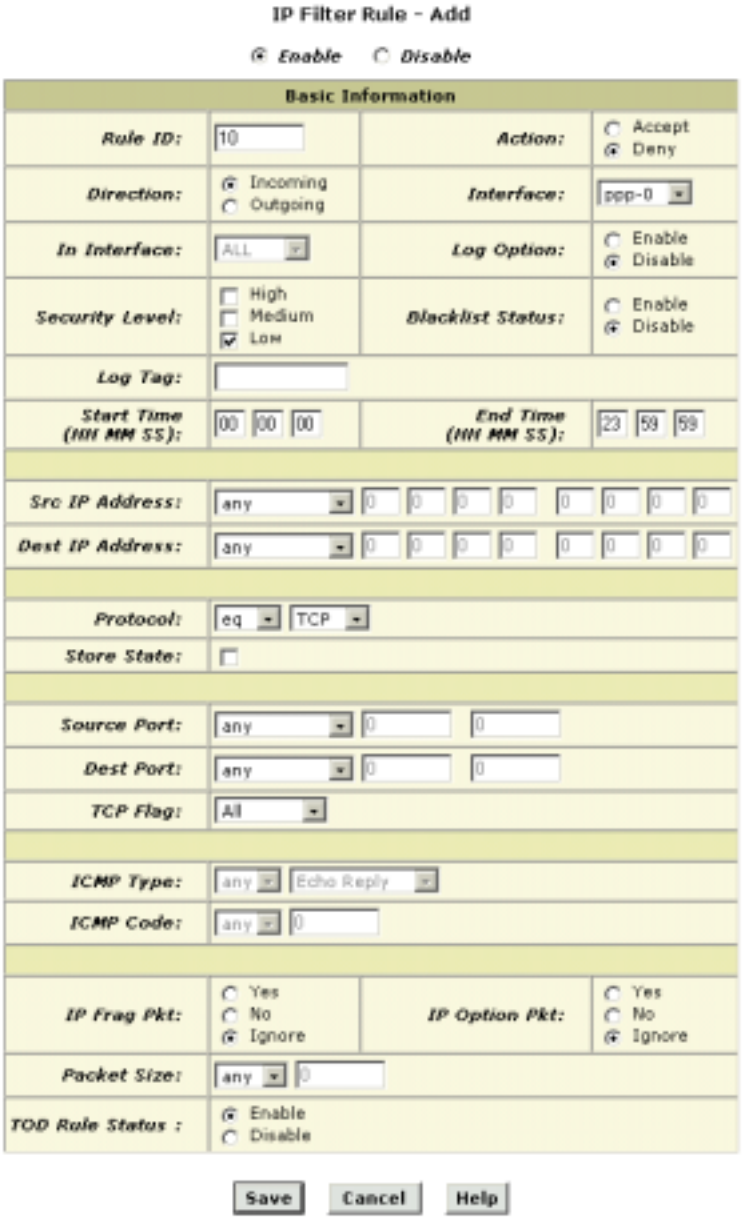


Figure 52. IP Filter Rule Example 2

Viewing IP Filter Statistics

For each rule, you can view statistics on how many packets were accepted or denied. Display the IP Filter Configuration page, and then click Stats in the corresponding row corresponding to the rule. A page such as the following displays:

IP Filter Rule - Statistics

IP Filter Rule Statistic	
Rule ID:	10
Number of Packets Maching this Rule:	0 Packets

Clear Close Refresh Help

Figure 53. IP Filter Rule – Statistics Page

You can click Clear to reset the count to zero and Refresh to display newly accumulated data.

Managing Current IP Filter Sessions

When two computers communicate using the IP protocol, an IP session is created for the duration of the communication. The ADSL/Ethernet router allows a fixed number of concurrent IP sessions. You can view information about each current IP session and delete sessions (for security reasons, for example).

To view all current IP sessions. display the IP Filters Configuration page, and then click Session. Figure 126 shows an example of an IP Filter Sessions page.

IP Filter Session

Session Index	Time to expire	Protocol	I/F	IP Address	Port	In Rule Index	In Action	Out Rule Index	Out Action	Action (s)
1	252	UDP	eth-0 Self	10.0.20.70 255.255.255.255	9830 69	30 0	Accept Unknown	30 0	Accept Unknown	
2	60	TCP	eth-0 Self	192.168.51.138 192.168.51.239	1721 80	30 0	Accept Unknown	30 0	Accept Unknown	
4	132	UDP	eth-0 Self	192.168.51.120 192.168.51.255	138 138	30 0	Accept Unknown	30 0	Accept Unknown	
8	12	UDP	eth-0 Self	192.168.51.162 192.168.51.255	138 138	0 0	Unknown Unknown	0 0	Unknown Unknown	
13	122	UDP	eth-0 Self	192.168.51.115 192.168.51.255	138 138	30 0	Accept Unknown	30 0	Accept Unknown	

Figure 54. IP Filter Sessions Page

The IP Filter Session table displays the following fields for each current IP session:

Field	Description
Session Index	The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP filter rule, are assigned a session index).
Time to expire	The number of seconds in which the connection will automatically expire
Protocol	The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.)
I/F	The interface on which the IP Filter rule is effective
IP Address	The IP addresses involved in the communication. The first one shown is the initiator of the communication.
Port	The hardware addresses of the ports involved in the communication
In/Out Rule Index	The number of the IP Filter rule that is applies to this session (assigned when the rule was created)
In/Out Action	The action (accept, deny, or unknown), being taken on data coming into or going out on the interface. This action is specified in the rule definition.
Actions	Provides a icon you can click on ( ) to delete the IP session. When you delete a session, the communication between is discontinued.

You can click **Refresh** to display newly accumulated data.

Problem	Troubleshooting Suggestion
	translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules (see 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 VisionNet 202ER's LAN IP address (by default 10.0.0.2). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v6.2 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 VisionNet 202ER.
Changes to Configuration Manager are not being retained.	Be sure to use the Commit function after any changes. This function is described on page 36.

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 you are trying to communicate with.

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 10.0.0.2

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 59***.

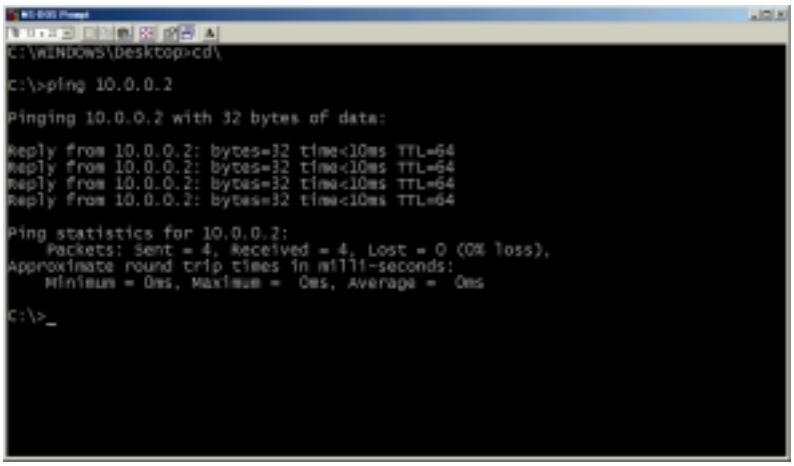


Figure 59. Using the ping Utility

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 VisionNet 202ER is working (using the preconfigured default LAN IP address 10.0.0.2) 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 60***.

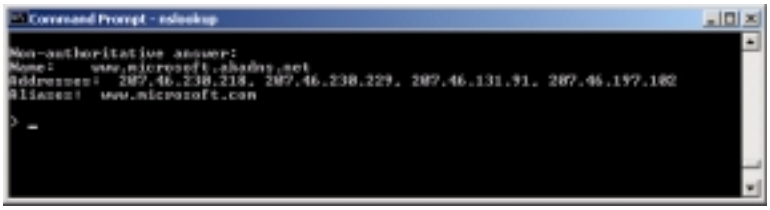


Figure 60. Using the nslookup Utility

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.