EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch

Use this guide to install: BEFVP41

User Guide

LINKSYS®

LIMITED WARRANTY
Linksys guarantees that every Instant Broadband EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch will be free from physical defects in material and workmanship for one year from the date of purchase, when used within the limits set forth in the Specifications section of this User Guide. If the product proves defective during this warranty period, call Linksys Technical Support in order to obtain a Return Authorization Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. When returning a product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. All customers located outside the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT. Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

Linksys P.O. Box 18558, Irvine, CA 92623.

FCC STATEMENT
This Instant Broadband EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch has been tested and complies with the specifications 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 according to 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 is found 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 or devices
• Connect the equipment to an outlet other than the receiver's
• Consult a dealer or an experienced radio/TV technician for assistance

UG-BEFVP41-010603G-KL

Table of Contents

Chapter 1: Introduction

The EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch

Congratulations on your purchase of an Instant Broadband® EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch. The Instant Broadband™ EtherFast® Cable/DSL VPN Router from Linksys is the perfect solution for sharing a high-speed broadband Internet connection while still maintaining the ultimate in network security.

Utilizing 56-bit DES and 168-bit 3DES encryption, Encapsulated Secure Payload (ESP), and IKE key exchange access control, the EtherFast® Router's full IPSec Virtual Private Network (VPN) capability provides complete data privacy.

The EtherFast® Cable/DSL VPN Router also boasts an impressive array of features including PPPoE support, NAT firewall, and a convenient web management interface. Since the Router is compatible with virtually all major operating systems, it's easy to set up and use, making the Instant Broadband™ EtherFast® Cable/DSL VPN Router the perfect solution for your broadband needs.

Features

- Full IPSec Virtual Private Network (VPN) capability
    - Supports (56-Bit) DES and (168-Bit) 3DES Encryption Algorithms
    - Supports MD5 and SHA Authentication
    - Supports IKE Key Management
- Hardware Security Co-Processor Inside
- Supports Up to 70 Simultaneous Tunnels
- Compatible with other IPSec VPN Software/Hardware Products
- Acts as a DHCP Server for Your Existing Network
- NAT, PPPoE, IP Filter, and MAC Filter Support
- Free Technical Support—24 Hours a Day, 7 Days a Week, Toll-Free US Calls
- 1-Year Limited Warranty

Chapter 2: Your Virtual Private Network (VPN)

Why Do I Need a VPN?

Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when emails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs are called Virtual Private Networks because they secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network - when you send data to someone via email or communicate with an individual over the Internet - the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

Data "sniffing" is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the middle attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a "man in the middle" attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose.

What is a Virtual Private Network?

A VPN, or Virtual Private Network, is a connection between two endpoints - a VPN Router, for instance - in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a "tunnel". A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Router using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:
• VPN Router to VPN Router
• Computer (using VPN client software that supports IPSec) to VPN Router

The VPN Router creates a "tunnel" or channel between two endpoints, so that data transmissions between them are secure. A computer with VPN client software that supports IPSec can be one of the two endpoints. Any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Router to create a VPN tunnel using IPSec (refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the VPN Router"). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

VPN Router to VPN Router

An example of a VPN Router-to-VPN Router VPN would be as follows. (See Figure 2-1.) At home, a telecommuter uses his VPN Router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.

Figure 2-1

> ⚠️ **Important:** You must have at least one VPN Router on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second VPN Router or a computer with VPN client software that supports IPSec.

Computer (using VPN client software that supports IPSec) to VPN Router

The following is an example of a computer-to-VPN Router VPN. (See Figure 2-2.) In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software that supports IPSec and connects to the VPN Router at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.

Figure 2-2

For additional information and instructions about creating your own VPN, please visit Linksys's website at *www.linksys.com* or refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the VPN Router."

Chapter 3: Getting to Know the EtherFast® Cable/DSL VPN Router with 4-Port 10/100 Switch

The Cable/DSL VPN Router's Rear Panel

The rear panel of the VPN Router, shown in Figure 3-1, is where all of the Router's connections are made.

Figure 3-1

WAN   The WAN (Wide Area Network) Port is where you will connect your Cable or DSL modem.

Ports 1-4   These four LAN (Local Area Network) ports are where you will connect networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network.

Crossover Switch The Crossover Switch (X ll) toggles Port 4 between crossover mode (X) and straight-through mode (ll). If you are connecting the Router directly to a computer or to an Uplink port, choose straight-through (ll). For anything else, please refer to the chart shown in "Chapter 4: Connecting the Cable/DSL VPN Router to Your Network", Figure 4-2.

Power   The Power Port is where you will connect the included AC power adapter.

> **Important: The Reset Button***
>
> The **Reset** button can be used in one of two ways.
>
> **1.** If the VPN Router is having problems connecting to the Internet, press the **Reset** button for just a moment with a paper clip or a pencil tip. This clears up any jammed connections, and is similar to pressing the **Reset** button on your PC to reboot it.
>
> **2.** If you are experiencing extreme problems with the VPN Router and have tried all other troubleshooting measures, press the **Reset** Button, and hold it down until the red **Diag** LED on the front panel turns on and off completely.
>
> This will restore factory defaults and clear all of the Router's settings, including the IP addresses you entered.
>
> * The **Reset** Button is located on the Router's rear panel.

The Cable/DSL VPN Router's Front Panel LEDs

The VPN Router's LEDs, shown in Figure 3-2, provide a graphic display of activity.

Figure 3-2

The LAN Indicators

Power   *Green*. The Power LED illuminates when the Router is powered on.

Link/Act *Green*. The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port (1-4). If the LED is flickering, the Router is actively sending or receiving data over that port.

Full/Col   *Green*. The Full/Col LED also serves two purposes. If this LED is continuously illuminated, the connection made through the corresponding port is successfully running in Full Duplex mode. If the LED is flickering, the connection is experiencing collisions. Infrequent collisions are normal. If this LED is flickering too often, there may be a problem with your connection. Check the Troubleshooting section if you think there is a problem.

100   *Orange*. The 100 LED illuminates when a successful 100Mbps connection is made through the corresponding port.

The WAN Indicators

Link   *Green*. The Link LED illuminates when a successful connection is made between the Router and your Broadband device or network.

Act   *Green*. The Act LED flickers when the Router is sending or receiving data over the broadband port.

Diag   *Red*. The Diag LED illuminates when the Router goes through its self-diagnosis mode during boot-up. It will turn off upon successful completion of the diagnostic. If this LED stays on for an abnormally long period of time, refer to "Appendix A: Troubleshooting."

Chapter 4: Connecting the Cable/DSL VPN Router to Your Network

Overview

Unlike a simple hub or switch, the VPN Router's setup consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them.

You may need the following values from your ISP in order to install the Router:

• Your broadband-configured PC's fixed Internet IP Address (if applicable)
• Your broadband-configured PC's Computer Name and Workgroup Name
• Your Subnet Mask (if applicable)
• Your Default Gateway (if applicable)
• Your Primary DNS IP Address (if applicable)

Whoever installed your broadband access should have left this information with you. If not, call your ISP and they will be able to supply you with it.

About Static & Dynamic IP Addresses

Static IP Addresses A static IP address is an IP address permanently assigned to a computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices which are consistently accessed by multiple users, such as Server PCs, or printers. If you are using the VPN Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during the Router's configuration.

Dynamic IP Addresses A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

DHCP (Dynamic Host Configuration Protocol) DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as routers.

Connecting Everything Together & Booting Up

Once you are sure that you have the above values on hand, you can begin the installation and setup of the VPN Router.

> **Note:** Some ISPs—most notably some cable providers—configure their networks so that you do not have to enter a full Internet address into your web browser or e-mail application to reach your home page or receive your e-mail. If your Internet home page address is something very simple, such as "www", rather than "www.linksys.com", or your e-mail server's address is something similar to "e-mail" or "pop3", rather than "pop.mail.linksys.com", you won't be able to properly configure the VPN Router until you determine the actual Internet addresses of your Web and e-mail connections.
>
> You **must** obtain this information prior to connecting the Router to your network. You can obtain this information by contacting your ISP, or turn to "Appendix E: How to Ping Your ISP's E-mail and Web Addresses."

1. Power everything down, including your **PCs**, your **Cable** or **DSL** modem and the **Router**.

2. Connect a network cable from one of the LAN ports on the back of the Router to one of your PCs' Ethernet ports, as shown in Figure 4-1. Do the same with all the PCs you wish to connect to the Router.

Figure 4-1

3. If you are using Port 4 to connect to a PC, set the Crossover Switch to straight-through mode (II). If you are connecting the Router to a hub or switch, please refer to the chart shown in Figure 4-2 when setting the Crossover Switch.

Switch Position	Straight Through Cable	Crossover Cable
X	Port 4 on Router to Regular Port on Switch or Hub	Port 4 on Router to Uplink Port on Switch or Hub
II	Port 4 on Router to Uplink Port on Switch or Hub	Port 4 on Router to Regular Port on Switch or Hub

Figure 4-2

> **Note:** The diagram above is for reference purposes only. Every network is different. If you do not make a connection to a hub or switch by using the settings above, change the position of the Crossover Switch.

4. Connect the network cable from your cable or DSL modem to the **WAN** port on the Router's rear panel, as shown in Figure 4-3. This is the only port that will work for your modem connection.

Figure 4-3

5. Connect the power adapter to the **Power** port on the Router's rear panel, as shown in Figure 4-4, and then plug the power adapter into a power outlet.

   • The **Power** LED on the front panel will light up green as soon as the power adapter is connected properly.

   • The **Diag** LED will light up red for a few seconds when the Router goes through its self-diagnostic test. This LED will turn off when the self-test is complete.

Figure 4-4

> **Important:** You should always plug the Router into a power strip with surge protection.

6. Turn on the cable or DSL modem.

7. Press the Reset button on the Router's front panel with a paper clip or a pencil. Hold the button in until the **Diag** LED lights up and then turns off. This will restore the Router's factory default settings.

The Hardware Installation is complete.

Chapter 5: Configuring Your Network

Configuring Your PCs to Connect to the Cable/DSL VPN Router

Note: Make sure that a Network Card or Adapter has been successfully installed into each PC on your network.

You must now configure your other PCs to accept the IP addresses that the VPN Router will provide.

Note: These instructions apply only to Windows 95, Windows 98, and Windows ME machines. For TCP/IP setup under Windows NT, 2000 and XP, please refer to your Windows manual.

1. Click the **Start** button. Select **Settings** and open the **Control Panel**.

2. Double-click the **Network** icon.

3. In the **Configuration** window, shown in Figure 5-1, select the **TCP/IP** protocol line that has been associated with your network card/adapter. If there is no TCP/IP line listed, go to "Appendix F: Installing the TCP/IP Protocol" to install the TCP/IP protocol now.
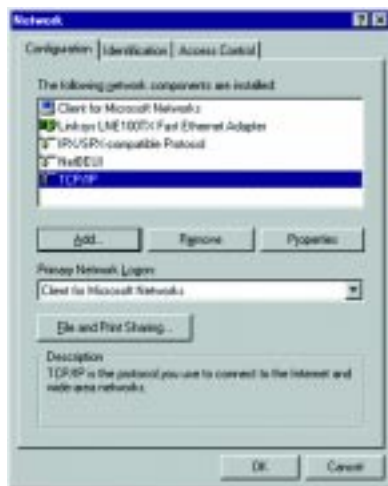

Figure 5-1

4. Click the **Properties** button, and then choose the **IP Address** tab, as shown in Figure 5-2. Select **Obtain an IP address automatically**. Click the **OK** button. You have completed the client settings.

Figure 5-2
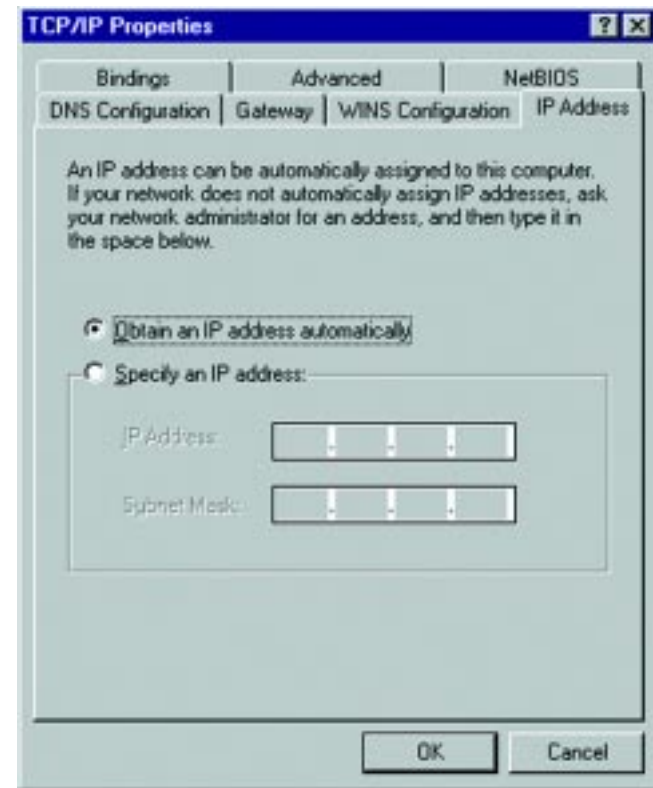
5. Click the **OK** button. Windows may ask for original Windows installation files. Supply them as needed (i.e.: D:\win98, D:\win95, D:\win9x, c:\windows\options\cabs).

6. Windows will ask you to restart the PC. Click the **Yes** button.

Repeat these steps for each PC on your network. When all of your PCs are configured, proceed to the next page, "Configuring the Cable/DSL VPN Router."

Configuring the Cable/DSL VPN Router

Now that the VPN Router is wired into your network, you can begin configuring your system.

> ⚠️ **Note:** If the TCP/IP protocol is not configured on your PC, go to "Appendix F: Installing the TCP/IP Protocol" for TCP/IP installation instructions now.

1. Open your web browser and type **http://192.168.1.1** in the browser's Address box, as shown in Figure 5-3. This number is the Router's default IP address. Press the **Enter** key.
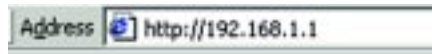
    | Address | 🔋 http://192.168.1.1 |

    Figure 5-3

2. A User Name and Password prompt will appear. Leave the User Name field empty, and type **admin** (the default password) in the **Password** field. (See Figure 5-4.) Click the **OK** button. If the screen does not appear, make sure your network adapter is working properly, the network cable is connected, and the Link LED is lit up on the Router. Restart the computer to obtain an IP address automatically.

    Figure 5-4

3. The Router configuration screen will appear with the Setup tab selected. Based on the setup instructions from your ISP, you may need to provide the following information.

    Host Name and **Domain Name**: These fields allow you to provide a host name and domain name for the Router. These fields are usually left blank. If requested by your ISP (usually cable ISPs), complete these two fields.

    Device IP Address and **Subnet Mask**: The values for the Router's IP Address and Subnet Mask are shown on the Setup screen. The default value is 192.168.1.1 for the IP Address and 255.255.255.0 for the Subnet Mask. Leave these settings alone.

4. The Router supports six connection types: DHCP (obtain an IP automatically), PPPoE, Static IP, RAS, and PPTP. These types are listed in the drop-down menu for the **WAN Connection Type** setting. Each Setup screen and available features will differ depending on what kind of connection type you select. Proceed to the instructions for the connection type you are using. When you are finished with the Setup tab, proceed to step 5.

> ⚠️ **Important:** If you have previously enabled an Internet Sharing Proxy Service on any of your PCs, you must disable it now.
>
> • If you are running Netscape Navigator, click **Edit** >> **Preference** >> **Advanced** >> **Proxies** >> **Direct Connection to the Internet**.
>
> • If you are running Internet Explorer v5 or better, click **Start** >> **Settings** >> **Control Panel** >> **Internet Options** >> **Connections** >> **LAN Settings**. Remove the checks from all three boxes. Click **OK** to continue.

DHCP

If your ISP says that you are connecting through DHCP or a dynamic IP address from your ISP, perform these steps:

A. Select **DHCP** as the WAN Connection Type. (Shown in Figure 5-5.)

B. Click the **Apply** and **Continue** buttons to save the setting, or click the **Cancel** button to clear the setting and start over. When you are finished, then proceed to step 5.

Figure 5-5

Static IP

If your ISP says that you are connecting through a static or fixed IP address from your ISP, perform these steps:

A. Select **Static IP** as the WAN Connection Type. (Shown in Figure 5-6.)

B. Enter the **IP Address**.

C. Enter the **Subnet Mask**.

D. Enter the **Gateway Address**.

E. Enter the **DNS** in the 1, 2, and/or 3 fields. You need to enter at least one DNS address.

F. Click the **Apply** and **Continue** buttons to save the settings, or click the **Cancel** button to clear the settings and start over. When you are finished, then proceed to step 5.

PPPoE

If your DSL provider says that you are connecting through PPPoE or if you nor-mally enter a user name and password to access the Internet, perform these steps:

A. Select **PPPoE** as the WAN Connection Type. (Shown in Figure 5-7.)

B. Enter the **User Name**.

C. Enter the **Password**.

Figure 5-6

Figure 5-7

D. Click the **Apply** and **Continue** buttons to save the settings, or click the **Cancel** button to clear the settings and start over.

E. When you are finished, click the **Status** tab, and then click the **Connect** button to start the connection. Proceed to step 5.

RAS

RAS is a service used in Singapore only. (Shown in Figure 5-8.) If you are using a RAS connection, check with your ISP for the neces-sary setup information.

When you are finished with the Setup tab, proceed to step 5.

Figure 5-8

PPTP

PPTP is a service used in Europe only. (Shown in Figure 5-9.) If you are using a PPTP connection, check with your ISP for the neces-sary setup information.

When you are finished with the Setup tab, proceed to step 5.

Figure 5-8

5. If you haven't already done so, click the **Apply** button and then the **Continue** button to save your Setup settings. Close the web browser.

6. Reset the power on your cable or DSL modem.

7. Restart your computers so that they can obtain the Router's new settings.

If you need advanced setting information, please refer to "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" or the Linksys support website at *support.linksys.com*.

Congratulations! You've suc-
cessfully configured the
Router. Test the setup by

Figure 5-9

opening your web browser from any computer and entering *www.linksys.com/registration*, as shown in Figure 5-9.

If you are unable to reach our website, you may want to review what you did in this section or refer to "Appendix A: Troubleshooting."

**Proceed to "Chapter 6: The Cable/DSL VPN Router's Web-based Utility"
for more details and advanced settings information.**

Chapter 6: The Cable/DSL VPN Router's Web-based Utility

Logging into the Web-Based Utility

The VPN Router uses a web-based interface to administer the Router. The interface can be accessed via Microsoft Internet Explorer or Netscape through use of a computer connected with a network cable to the Router.

To access the web-based interface of the Router, launch Internet Explorer or Netscape, and enter the Router's default IP address, **192.168.1.1** into the Address field, as shown in Figure 6-1. Then, press **Enter**.
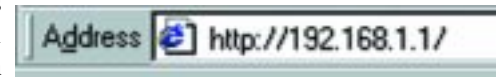

Figure 6-1

After entering the address value into the web browser, a password request page will pop up. Leave the User Name field empty, and type **admin** into the Password field. (See Figure 6-2.) Then, click the **OK** button.

Figure 6-2

In this section, you'll find brief descriptions of each webpage in the Utility and each page's key functions.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

Setup

The Setup screen is the first screen you will see when you access the Utility. If you have already installed and setup the VPN Router, you have already seen this screen and have already properly configured all of the screen's values.

- **Host Name & Domain Name** These fields allow you to supply a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your Broadband Internet service has been configured with a host and domain name. In most cases, these fields may be left blank.

- **Firmware Version** This entry shows the version of the firmware you are using. Future versions of the Router's Firmware may be available on the Linksys website at *www.linksys.com*.

- **Time Zone** Set your local time zone here.

- **Device IP Address and Subnet Mask** The values for the Router's IP Address and Subnet Mask are shown here. The default value is **192.168.1.1** for the IP address and **255.255.255.0** for Subnet Mask. If you change the Device IP Address, then reboot the computer so the new value takes effect.

- **WAN Connection Type** The Router supports five connection types: DHCP, PPPoE, Static IP Address, RAS, and PPTP. Each Setup screen and available features will differ depending on what kind of connection type you select. You can test and see if the above settings are correct by successfully connecting to the Internet.

Figure 6-3

DHCP

As shown in Figure 6-3, this is the Router's default setting. Tt should only be used if your ISP supports DHCP.

Static IP

If you are required to use a permanent IP address, then enable Static IP, as shown in Figure 6-4.

Specify WAN IP Address This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Address Your ISP will provide you with the Default Gateway Address.

DNS (Required) Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure 6-4

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish communications with an end-user. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable it, as shown in Figure 6-5.

Figure 6-5

User Name and Password Enter your ISP's User Name and Password.

Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (**Max Idle Time**). If you have been disconnected due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive Option and Redial Period This option keeps your PPPoE-enabled Internet access connected indefinitely, even when it sits idle. To use this option, click the radio button next to **Keep Alive** to select it. The default **Redial Period** is 30 seconds.

> **Important:** For DSL users, if you need to enable PPPoE support, choose **PPPoE**. If you do enable PPPoE, remember to remove any existing PPPoE applications already installed on any of your PCs.

RAS

Remote Access Service (RAS) is a service that applies for connections in Singapore only. (This setup is shown in Figure 6-6.) For users in Singapore, check with Singtel for information on RAS.

Figure 6-6

User Name and Password Enter the User Name and Password supplied by Singtel.

RAS Plan Select the type of plan you have.

Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (**Max Idle Time**). If you have been disconnected due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive Option and Redial Period This option keeps your PPPoE-enabled Internet access connected indefinitely, even when it sits idle. To use this option, click the radio button next to **Keep Alive** to select it. The default **Redial Period** is 30 seconds.

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies for connections in Europe only. (This setup is shown in Figure 6-7.)

Specify WAN IP Address This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

Figure 6-7

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Address Your ISP will provide you with the Default Gateway Address.

Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (**Max Idle Time**). If you have been disconnected due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive Option and Redial Period This option keeps your PPPoE-enabled Internet access connected indefinitely, even when it sits idle. Click the radio button next to **Keep Alive** to select it. The default **Redial Period** is 30 seconds.

VPN

Figure 6-8

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. This connection is very specific as far as its settings are concerned; this is what creates the security. The VPN screen, shown in Figure 6-8, allows you to configure your VPN settings to make your network more secure.

Note: Network security, while a desirable and often necessary aspect of networking, is complex and requires a thorough understanding of networking principles.

Establishing a Tunnel

The VPN Router creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure. To establish this tunnel, select the tunnel you wish to create in the **Select Tunnel Entry** drop-down box. It is possible to create up to 70 simultaneous tunnels.

Then check the box next to **Enable** to enable the tunnel.

Once the tunnel is enabled, enter the name of the tunnel in the **Tunnel Name** field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

Local Secure Group and Remote Secure Group

The **Local Secure Group** is the computer(s) on your LAN that can access the tunnel. The **Remote Secure Group** is the computer (s) on the remote end of the tunnel that can access the tunnel. Under Local Secure Group and Remote Secure Group, you may choose one of three options: Subnet, IP Address, and IP Range. Under Remote Secure Group, you have two additional options: Host and Any.

> **Note:** The IP Addresses and Subnet Mask values used here are for example only. ***Do not try to use them for your actual setup.*** Obtain the relevant information from your own network to accurately configure the Router.

- **Subnet** - If you select **Subnet** (which is the default), this will allow all computers on the local subnet to access the tunnel. In the example shown in Figure 6-9, all Local Secure Group computers with IP Addresses 192.168.1.xxx will be able to access the tunnel. All Remote Secure Group computers with IP Addresses 192.168.2.xxx will be able to access the tunnel (in your settings, use the IP Addresses appropriate for your VPN). When using the Subnet setting, the default values of **0** should remain in the last fields of the **IP** and **Mask** settings.

Figure 6-9

> **Note:** It is possible to set up the VPN Router using any combination of the three settings under Local Secure Group and the five settings under Remote Secure Group. For instance, when Subnet is chosen on the local end of the tunnel, Subnet does not have to be chosen at the remote end. So a single IP Address could be chosen to access the tunnel on the local end and a range of IP Addresses could be set at the remote end of the tunnel.

- **IP Address** - If you select **IP Address**, only the computer with the specific IP Address that you enter will be able to access the tunnel. In the example shown in Figure 6-10, only the computer with IP Address 192.168.1.10 can access the tunnel from this end. Only the computer with IP Address 192.168.2.12 can access the tunnel from the remote end (in your settings, use the IP Addresses appropriate for your VPN).

Figure 6-10

- **IP Range** - If you select IP Range, it will be a combination of Subnet and IP Address. You can specify a range of IP Addresses within the Subnet which will have access to the tunnel. In the example shown in Figure 6-11, all computers on this end of the tunnel with IP Addresses between 192.168.1.1 and 192.168.1.20 can access the tunnel from the local end. Only computers assigned an IP Address between 192.168.2.1 and 192.168.2.100 can access the tunnel from the remote end (in your settings, use the IP Ranges appropriate for your VPN).

Figure 6-11

Under **Remote Secure Group**, you have two additional options: Host and Any.

• **Host** - If you select Host for the Remote Secure Group, then the Remote Secure Group will be the same as the Remote Security Gateway setting: IP Address, FQDN (Fully Qualified Domain Name), or Any. (Remote Security Gateway settings are explained on the following page.) In the example shown in Figure 6-12, the Remote Secure Group is the same as the Remote Security Gateway, set to a specific IP Address.

Figure 6-12

• **Any** - If you select Any for the Remote Security Group, the local VPN Router will accept a request from any IP address. This setting, shown in Figure 6-13, should be chosen when the other endpoint is using DHCP or PPPoE on the WAN side.

Figure 6-13

Remote Security Gateway

The Remote Security Gateway is the VPN device, such as a second VPN Router, on the remote end of the VPN tunnel. Under **Remote Security Gateway**, you have three options: IP Address, FQDN, and Any.

• **IP Address** - If you select IP Address, as shown in Figure 6-14, enter the IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Router, but the IP Address of the remote VPN Router or device with which you wish to communicate.

Figure 6-14

• **FQDN** (Fully Qualified Domain Name) - If you select FQDN, as shown in Figure 6-15, enter the FQDN of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The FQDN is the host name and domain name for a specific computer on the Internet, for example, *vpn.myvpnserver.com*.

Figure 6-15

- **Any** - If you select Any for the Remote Security Gateway, as shown in Figure 6-16, the VPN device at the other end of the tunnel will accept a request from any IP address. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. If the remote user has an unknown or dynamic IP address (such as a professional on the road or a telecommuter using DHCP or PPPoE), then Any should be selected.

Figure 6-16

Encryption

Using **Encryption** also helps make your connection more secure. There are two different types of encryption: **DES** or **3DES** (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting **Disable**. In Figure 6-16, DES (which is the default) has been selected.

Authentication

Authentication acts as another level of security. There are two types of authentication: **MD5** and **SHA** (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication. In Figure 6-16, MD5 (the default) has been selected.

Key Management

In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a "key" to the encryption code. Under **Key Management**, you may choose automatic or manual key management.

Automatic Key Management

Select **Auto (IKE)** and enter a series of numbers or letters in the Pre-shared Key field. Check the box next to **PFS (Perfect Forward Secrecy)** to ensure that the initial key exchange and IKE proposals are secure. In the example shown in Figure 6-17, the word **MyTest** is used. Based on this word, which MUST be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.

Figure 6-17

Manual Key Management

Similarly, you may choose **Manual** keying, which allows you to generate the key yourself. Enter your **key** into the Encryption KEY field. Then enter an **Authentication KEY** into that field. These fields must both match the information that is being entered in the fields at the other end of the tunnel. The example in Figure 6-18 shows some sample entries for both the Encryption and Authentication Key fields. Up to 24 alphanumeric characters are allowed to create the Encryption Key. Up to 20 alphanumeric characters are allowed to create the Authentication Key.

The **Inbound SPI** and **Outbound SPI** fields are different, however. The Inbound SPI value set here must match the *Outbound SPI* value at the other end of the tunnel. The Outbound SPI here must match the *Inbound SPI* value at the other end of the tunnel. In the example (see Figure 6-18), the Inbound SPI and Outbound SPI values shown would be opposite on the other end of the tunnel. Only numbers can be used in these fields. After you click the Apply button, hexadecimal characters (series of letters and numbers) are displayed in the Inbound SPI and Outbound SPI fields.

Figure 6-18

Once you are satisfied with all your settings, click the **Apply** button. If you make any mistakes, clicking the **Cancel** button will exit the screen without saving any changes, provided that you have not already clicked the Apply button.

After the VPN device is set up at the other end of the tunnel, you may click the **Connect** button to use the tunnel. This assumes that both ends of the tunnel have a physical connection to each other (e.g., over the Internet, physical wiring, etc.). After clicking the Connect button, click the **Summary** button. If the connection is made, the screen shown in Figure 6-19 will appear:

Figure 6-19

Figure 6-20

Under **Status**, the word **Connected** should appear if the connection is successful. The other fields reflect the information that you entered on the VPN screen to make the connection.

If **Disconnected** appears under Status, as shown in Figure 6-20, some problem exists that prevents the creation of the tunnel. Make sure that all of your wiring is securely connected. Double-check all the values you entered on the VPN screen to make sure they are correct. If the other end of the tunnel is some distance from you (e.g., in another city, etc.), call to make sure that the settings on that end of the tunnel are correct as well.

If, for any reason, you experience a temporary disconnection, the connection will be re-established as long as the settings on both ends of the tunnel stay the same.

To get more details concerning your tunnel connection, click the **View Log** button. The screen in Figure 6-21 will appear:
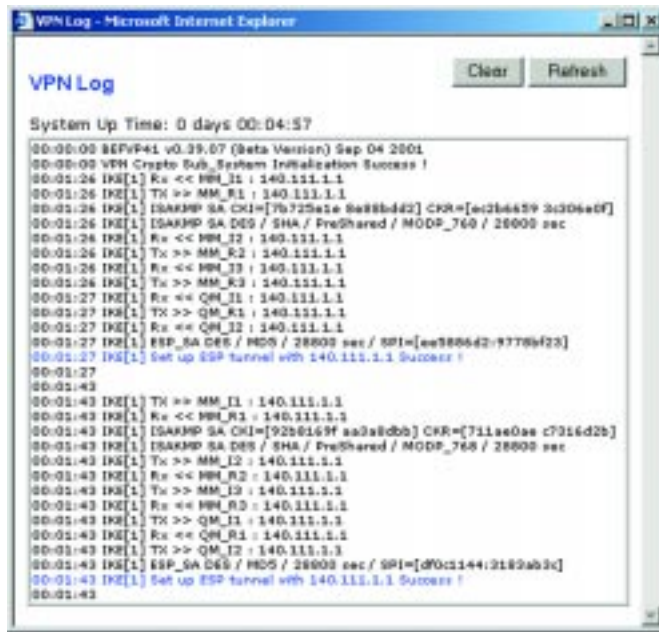
Figure 6-21

The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used.

Once you no longer have need of the tunnel, simply click the **Disconnect** button on the bottom of the VPN page.

To change advanced settings, select the **tunnel** whose advanced settings you wish to change. Then click on **more...** to change the Advanced Settings for a specific VPN tunnel.

Advanced Settings for Selected IPSec Tunnel

From the Advanced Settings screen, shown in Figure 6-22, you can adjust the settings for specific VPN tunnels.

Figure 6-22

Phase 1

Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.

Operation Mode
There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device.

Encryption
Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.

Authentication
Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.

Group

There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Lifetime

In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

Group

There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Lifetime

In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Other Settings

NetBIOS broadcast

Check the box next to NetBIOS broadcast to enable NetBIOS traffic to pass through the VPN tunnel.

Anti-replay

Check the box next to Anti-replay to enable the Anti-replay protection. This feature keeps track of sequence numbers as packets arrive, ensuring security at the IP packet-level.

Keep-Alive

Check the box next to Keep-Alive to re-establish the VPN tunnel connection whenever it is dropped. Once the tunnel is initialized, this feature will keep the tunnel connected for the specified amount of idle time.

Unauthorized IP Blocking

Check this box to block unauthorized IP addresses. Complete the on-screen sentence to specify how many times IKE must fail before blocking that unauthorized IP address for a length of time that you specify (in seconds).

Password

Figure 6-23

The Password screen, shown in Figure 6-23, allows you to change the password, set SNMP Community names, and restore default settings on the Router.

Router Password You should set a password for the Router, unique for you but that you will remember. When you first power up the Router, the default Password setting is **admin**.

If you do not change the password, all users on your network will be able to access the Router simply by entering the unit's IP address into their web browser's location window and entering **admin** to access the Router.

If you select the Restore Factory Default option and click the **Apply** button, you will clear all of the Router's settings.

Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration data.

SNMP Community allows a name to be assigned to any SNMP communities that have been setup in the network. Four different communities can be defined, including the two default communities—public and private. For each **SNMP Community** name, you can configure each community's accessibility, making it either **Read-Only** or **Read-Write**.

Restore Factory Default If you set this option to **Yes** and click the **Apply** button, you will clear all of the Router's settings. Do not restore to the factory defaults unless you are having difficulties with the Router. Once the Router is reset, you will have to re-enter your configuration information.

Status

The Status screen, shown in Figure 6-24, provides the current status of the device. All of the information provided is read-only.
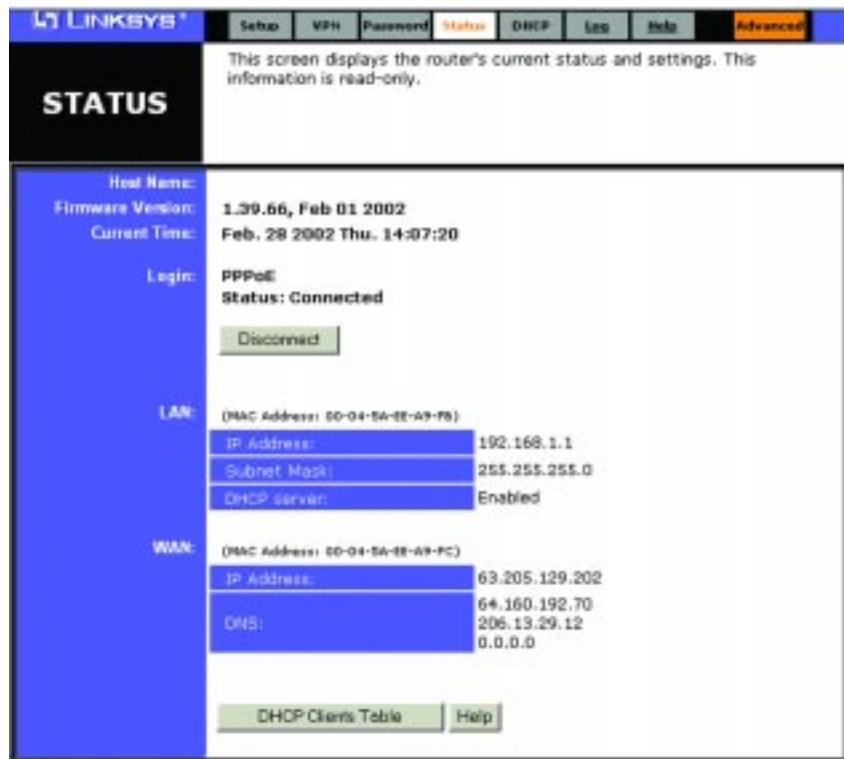
Figure 6-24

Host Name This field shows the name of this device. This entry is necessary for some ISPs.

Firmware Version This field shows the installed version of the firmware.

Login This field shows whether or not you have enabled the use of the Router's **PPPoE (Point-to-Point Protocol over Ethernet)** support. Click the **Connect** button if your PPPoE status is Disconnected. This will initiate a connection to your ISP. Click **Disconnect** if you want to cut your connection to your ISP.

LAN These fields display the Router's current IP Address and Subnet Mask, as seen by users on your internal network, as well as the status of the Router's DHCP server function. This option is either enabled or disabled.

WAN These fields display the Router's IP Address, Subnet Mask and Gateway IP as seen by external users on the Internet, as well as the IP Address of the DNS currently being used. Multiple DNS IP settings are common. The first available DNS entry is used in most cases.

DHCP Release Click on the **DHCP Release** button to delete your PC's current IP address.

DHCP Renew Click on the **DHCP Renew** button to replace your PC's current IP address with a new IP address.

DHCP Client Table Click on the **Client Table** button to show the current DHCP Client information. (This information is stored in temporary memory, so the list of clients could disappear.)

DHCP

Figure 6-25

From the DHCP screen, shown in Figure 6-25, you can configure the Router as a DHCP Server.

A DHCP (Dynamic Host Configuration Protocol) Server automatically assigns IP addresses to each computer on your network. Unless you already have one, you should set up the Router as a DHCP server.

DHCP Server Check the **Enable** option to enable the Router's DHCP server option. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**.

Starting IP Address Enter a numerical value for the DHCP server to start with when issuing IP addresses. Do not use 192.168.1.1 as the Router's starting IP address.

Number of DHCP users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to, with the absolute maximum being 253.

Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

DNS The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to utilize another, enter that **IP Address** in one of these fields. You can enter up to three DNS Server IP Addresses here. The Router will utilize these for quicker access to functioning DNS servers.

WINS Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's **IP Address** here. Otherwise, leave this blank.

DHCP Client Table Click on the **Client Table** button to show the current DHCP Client information. (This information is stored in temporary memory, so the list of clients could disappear.)

When finished, click the **Apply** button and then the **Continue** button.
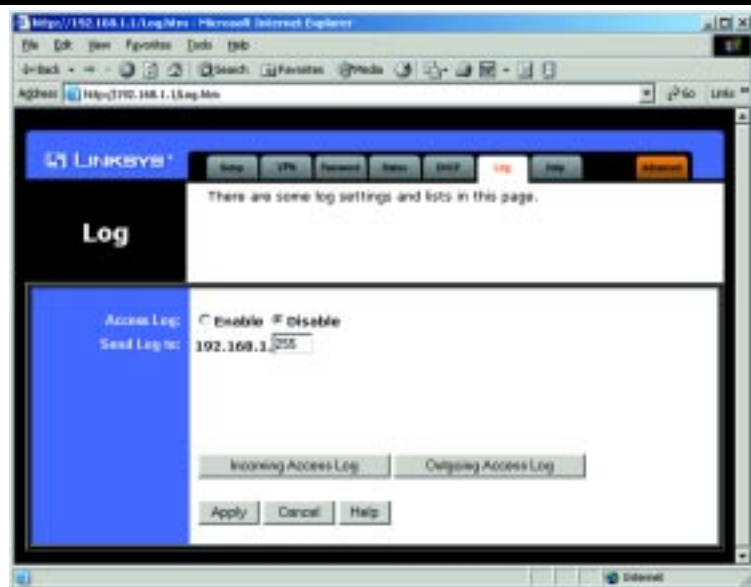
Log

Figure 6-26

The Log tab, shown in Figure 6-26, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

The Log feature provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection. The Logviewer keeps track of all incoming and outgoing activity that can be saved in a text file. The IP address points to the location where Logviewer is running.

The Outgoing Access Log lists all the URLs or IP addresses of Internet sites that users on your network have accessed, and the Incoming Access Log gives you a log of all incoming Internet traffic.

This data can also be accessed by other network users if the file is shared.

Access Log To activate logging, click the **Enable** button.

Send Log to Enter in the IP address of the PC that you want to send the log to (where your PC is running Logviewer). Make sure that this PC is using a static IP address. Click the **Apply** button and then the **Continue** button when you're done. You may download the Logview software at www.linksys.com.

Click on **Outgoing Access Log** or **Incoming Access Log** to view each log.

To disable Logging, click on **Disable** in the Log window, and then click the **Apply** button and the **Continue** button.

Help

Figure 6-27

On the Help screen, shown in Figure 6-27, you will find links to all of the Utility's internal support documentation, as well as the application that upgrades the Router's firmware.

Clicking on any of the topics in the bar on the left will give you help information about that topic.

Clicking on the **Linksys Website** link in the center area will take you to Linksys's website, provided you are connected to the Internet. If the link does not take you to the Linksys website, you may alternately type *www.linksys.com* in the address bar at the top of the screen.

Clicking on the **Online manual in PDF format** link will take you to the latest version of the manual for this product. The manual will be in Adobe Acrobat Portable Document File (.pdf) format. You will need the Adobe Acrobat Reader to view this version of the manual. If you do not have the Acrobat Reader, click on the **Adobe Website** link to get it.

For instructions on upgrading the Router's firmware, see the next page.

To upgrade the Router's firmware:

1. Download the latest firmware version from the Linksys website (*www.linksys.com*).

2. Go to the Help screen.

3. Click **Upgrade Firmware**. The page shown in Figure 6-28 will appear.

Figure 6-28

5. Click the **Browse** button to find the firmware upgrade file that you down-loaded from the Linksys website.

6. Double-click the **firmware file** you downloaded. Click the **Upgrade** button, and follow the instructions there.

To back up the Router's configuration file:

1. Go to the Help screen.

2. Click the **Backup** button and follow the instructions there.

> **Note:** Currently, the Backup & Restore Configuration feature supports only Internet Explorer 5.0 or higher.

Figure 6-29

To restore the Router's configuration file:

1. Go to the *Help* screen. Click the **Backup & Restore Configuration** link.

2. Click the **Browse** button (from the screen shown in Figure 6-29) to find and select the configuration file that you want to restore.

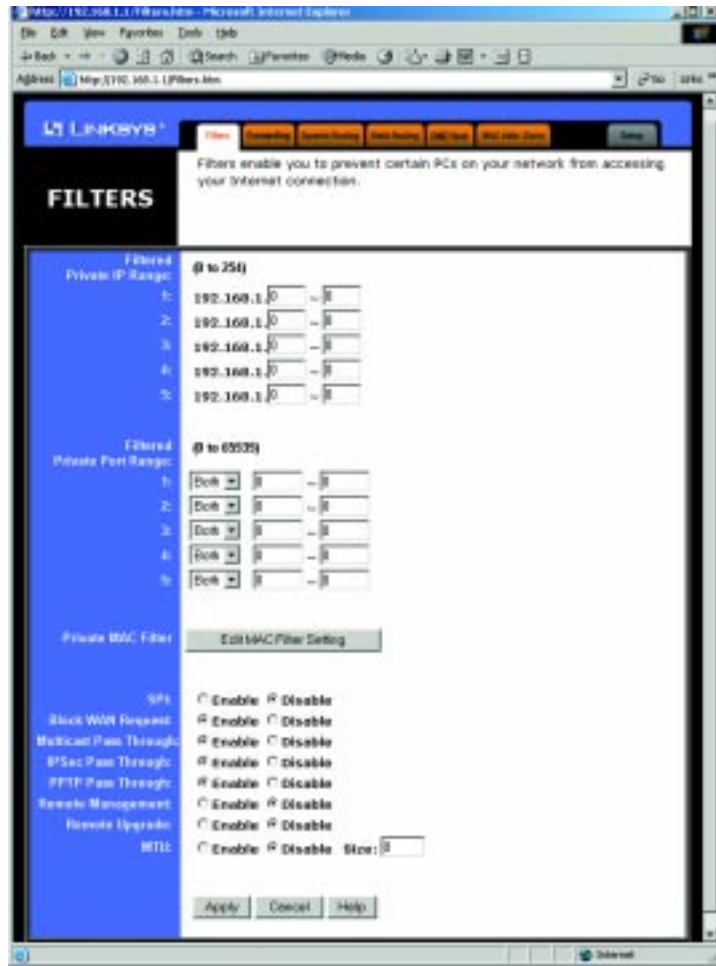3. Click the **Restore** button, and follow the instructions.

Filters

Figure 6-30

IP filters block specific internal users from accessing the Internet and enable VPN (Virtual Private Network) tunnels. This is handled from the Filters tab, shown in Figure 6-30. You can set up filters by using IP addresses or network port numbers (or a range of ports).

Setting Up Filters
- To set up a filter using IP addresses, enter the range of IP addresses you wish to filter into the IP address fields. Users who have filtered IP addresses will not be able to access the Internet at all. If you only want to filter one IP address instead of a range of IP addresses, enter the same value into both fields. For instance, if you wish to filter the PC with the IP address of 192.168.1.5, enter **5** into both fields on one line: 192.168.1.**5** ~ 192.168.1.**5**. Click the **Apply** button and **Continue** button when you're done.
- To filter users by network port number, enter a network port number or a range of network ports. Enter the port numbers you want to filter into the port numbers fields. Users connected to the Router will no longer be able to access any port number listed there.

Editing MAC Filter Setting
- This feature filters the network adapter's specific MAC address from going out to the Internet.
- To check your network adapter's MAC address, run **winipcfg** or **ipconfig** in the command prompt. To set the MAC filter, click the **Edit MAC Filter Setting** button. When a second window appears, select the range in the drop-down box, and at the MAC number prompt, enter the 12-digit MAC address you want to filter. Click the **Apply** button, followed by the **Continue** button, and then close the window.

SPI (Stateful Packet Inspection)
This feature checks the state of a packet to verify that the destination IP address matches the source IP of the original request. To use the firewall, select **Enable**; otherwise, select **Disable** to use the NAT firewall.

Blocking WAN Requests
- By enabling the *Block WAN Request* feature, you can prevent your network from being "pinged," or detected, by other Internet users. The *Block WAN Request* feature also reinforces your network security by hiding your network ports. Both functions of the *Block WAN Request* feature make it more difficult for outside users to work their way into your network.
- Click the **Apply** button and then the **Continue** button to save your changes.

Using Multicast Pass Through
This feature allows for multiple transmissions to specific recipients at the same time. Select **Enable** to support the feature, or **Disable** to keep the Router from multicasting.

Using IPSec Pass Through
- This feature lets you use IPSec Pass Through. To use this feature, select **Enable** next to IPSec Pass Through, and then click the **Apply** button and **Continue** button.
- To disable IPSec Pass Through, select **Disable**, and then click the **Apply** button and **Continue** button.

Using PPTP Pass Through
- Point-to-Point Tunneling Protocol is the method used to enable VPN (Virtual Private Networking) tunnels. To enable this feature, click on **Enable** next to PPTP Pass Through, and then click **Apply** and **Continue** button.
- To disable this feature, select **Disable** next to PPTP Pass Through, and then click the **Apply** button and **Continue** button.

Using Remote Management
- This feature allows you to manage the Router from a remote location, via the Internet. To enable this feature, select **Enable,** and then click the **Apply** button and **Continue** button.
- To disable Remote Management, select **Disable**, and then click the **Apply** button and **Continue** button. If you wish to use this feature on the browser, enter **http://<WAN IP Address>:8080**.

Using Remote Upgrade
This feature allows you to "flash," or upgrade, the Router's firmware from a remote location. To enable Remote Upgrade, select **Enable**, and then click the **Apply** button and **Continue** button.

Using MTU (Maximum Transmission Unit)
This feature specifies the largest packet size permitted for network transmission. Select **Enable** and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use **1492**. By default, MTU is set at **1500** when disabled.

Forwarding
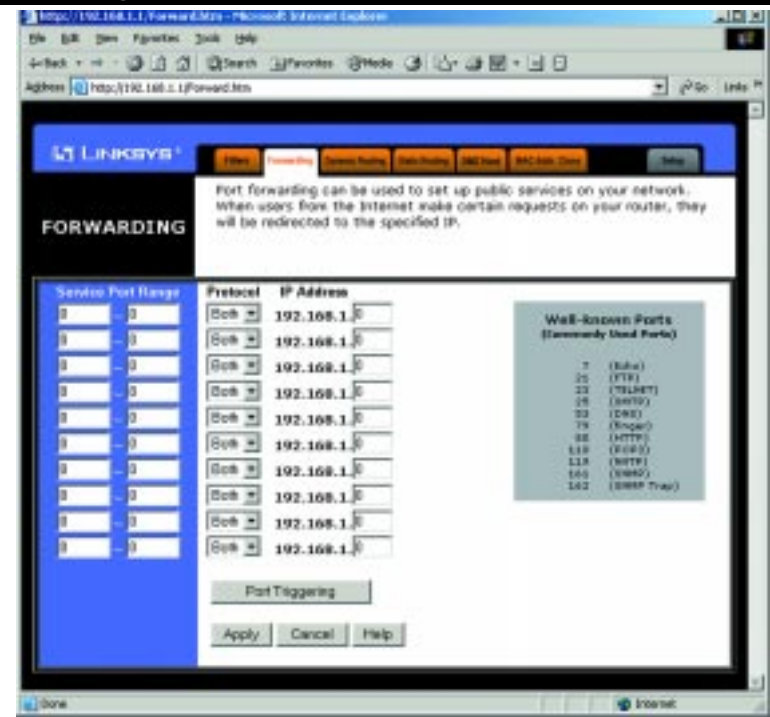
Figure 6-31

From the Forwarding tab, shown in Figure 6-31, you can set up public services on your network, such as web servers, ftp servers, or e-mail servers. When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Before using Forwarding, you must disable the Router's DHCP function from the DHCP tab and assign the Router a new static LAN IP address, as the IP address may change when using the DHCP server.

If you need to forward all ports for one PC, see the section on DMZ hosting.

To add a server using Forwarding:

1. Enter the port number or range of ports used by the server. On the same line, select the protocol **UDP**, **TCP**, or **Both**, and enter the LAN IP address of the server that you want the Internet user to access.

2. Configure as many entries as needed—the Router supports up to ten ranges of ports. Click the **Apply** button and **Continue** button when finished.

Using Port Triggering

Figure 6-32

From the Forwarding screen, click the **Port Triggering** button to open the Port Triggering screen, shown in Figure 6-32. Port triggering allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the firewall, the data is pulled back to the proper computer by way of IP address and port mapping rules.

1. Enter the **Application Name** of the trigger.

2. Enter the **Trigger Port Range** used by the application.

3. Enter the **Incoming Port Range** used by the application.

4. Click the **Apply** button and **Continue** button to finish.

Dynamic Routing

Figure 6-33

With Dynamic Routing (set from the Dynamic Routing screen, shown in Figure 6-33), you can automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network. To set up Dynamic Routing:

1. Choose the correct working mode. **Gateway Mode** should be used if the Router is hosting your network's connection to the Internet. **Router Mode** should be selected if the Router exists on a network with other routers.

2. Choose the **protocol** by which you transmit **(TX)** data on the network.

3. Choose the **protocol** by which the Router receives **(RX)** network data.

4. Click the **Apply** button and **Continue** button to save your changes.

Static Routing

Figure 6-34

If the Router is connected to more than one network, it may be necessary to set up a static route between them. This can be done from the Static Routing screen, shown in Figure 6-34. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Click the **Show Routing Table** button to view the current static routing configuration.

To create a static route entry:

1. Select **Static Route Entry** from the drop-down list. The Router supports up to 20 static route entries.

2. Enter the following data to create a new static route:

   Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. If you are building a route to an entire network, be sure that the network portion of the IP address is set to zero. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the network to which the Router is connected is 192.168.1, with the last digit (1, in this case) determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router.

   Network Mask The Network Mask (also known as the Subnet Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. In the example above, the Network Mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of an network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.

   Gateway IP This IP address should be the IP address of the gateway device that allows for contact between the Router and the remote network or host.

3. Click the **Apply** button and **Continue** button to save your changes.

DMZ Host

Figure 6-35

From the DMZ Host screen, shown in Figure 6-35, you can allow one local user to be exposed to the Internet to use a special-purpose service such as Internet gaming or videoconferencing.

Whereas IP Forwarding can only forward a maximum of ten ranges of ports, DMZ hosting forwards all the ports for one PC simultaneously.

• To expose one PC, enter the computer's IP address and click the **Apply** button and **Continue** button.

• Deactivate DMZ by entering **0** in the field and clicking the **Apply** button and **Continue** button.

MAC Address Cloning

Figure 6-36

From the MAC Address Clone screen, shown in Figure 6-36, you can change the Router's WAN Mac Address.

The Router's **MAC address** is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. Some ISPs require that you register the MAC address of your network card/adapter, which was connected to your cable or DSL modem during installation. If your ISPs require MAC address registration, find your adapter's MAC address by doing the following:

1. Click the **Start** button, and select **Run**. Run **winipcfg**, and then click **more info**. Or at the command prompt, run **ipconfig/all**, and look at your adapter's physical address.

2. Enter those 12 digits into the WAN MAC Address fields, and click the **Apply** button followed by the **Continue** button. This "clones" your network adapter's MAC address onto the Router, and prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address.

Appendix A: Troubleshooting

Common Problems and Solutions

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems regarding the installation and operation of the Router. If your situation is described here, the problem should be solved by applying the corresponding solution. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

1. I need to set a static IP address on a PC.

The Router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.150 using the DHCP server on the Router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

For Windows 95, 98, and Me:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
B. In *The following network components are installed* box, select the **TCP/IP->** associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.
C. In the *TCP/IP properties* window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Make sure that each IP address is unique for each PC or network device.
D. Click the **Gateway** tab, and in the *New Gateway* prompt, enter **192.168.1.1**, which is the Router's default IP address. Click the **Add** button to accept the entry.
E. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Enter the **DNS entry** provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the Network window.
G. Restart the computer when asked.

For Windows 2000:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
C. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
D. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the **Preferred DNS server** and **Alternative DNS server** (provided by your ISP). Contact your ISP or go on its website to find the information.
H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
I. Restart the computer if asked.

For Windows NT 4.0:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
B. Click the **Protocol** tab, and double-click **TCP/IP Protocol**.
C. When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter.
D. Select **Specify an IP address**, and enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Click the **DNS** tab, and enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Under DNS Service Search Order, click the **Add** button. Enter the **DNS IP address** in the DNS Server field, and click the **Add** button. Repeat this action for all DNS IP addresses given by your ISP.
H. Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
I. Restart the computer if asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

A. Click **Start** and **Control Panel**.
B. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
C. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
D. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
E. Select the *use the following IP address* radio button. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
F. Enter the Subnet Mask, **255.255.255.0**.
G. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
H. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the **Preferred DNS server** and **Alternative DNS server** (provided by your ISP). Contact your ISP or go on its website to find the information.
I. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window. Click the **OK** button in the *Local Area Connection Properties* window.

2. I want to test my Internet connection.
A. Check your TCP/IP settings.

For Windows 95, 98, and Me:
Refer to "Appendix F: Installing the TCP/IP Protocol" and "Chapter 5: Configuring Your Network" for details. Make sure **Obtain IP address automatically** is selected in the settings.

For Windows 2000:
• Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
• Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
• In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure

---

that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
• Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the Local Area Connection Properties window.
• Restart the computer if asked.

For Windows XP:
The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

• Click **Start** and **Control Panel**.
• Click the **Network and Internet Connections** icon and then the **Network Connections** icon.• Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
• In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
• Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
• Restart the computer if asked.

For Windows NT 4.0:
• Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
• Click the **Protocol** tab, and double-click on **TCP/IP Protocol**.
• When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter and set it for **Obtain an IP address from a DHCP server**.
• Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
• Restart the computer if asked.

B. Open a command prompt.
• For **Windows 95, 98,** and **Me**, please click **Start** and **Run**. In the Open field, type in **command**. Press the **Enter** key or click the **OK** button.
• For **Windows NT, 2000,** and **XP**, please click **Start** and **Run**. In the Open field, type **cmd**. Press the **Enter** key or click the **OK** button.

C. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
  • If you get a reply, the computer is communicating with the Router.
  • If you do NOT get a reply, please check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

D. In the command prompt, type **ping** *followed by your WAN IP address* and press the **Enter** key. The WAN IP Address can be found in the Router's Web-based Utility. For example, if your WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.
  • If you get a reply, the computer is connected to the Router.
  • If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E. In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.
  • If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
  • If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the WAN with my Internet connection.

A. Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
B. If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix G: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the MAC Address Clone section of "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" for details.
C. Make sure you are using the right WAN settings. Contact your ISP to see if your WAN connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" for details on WAN settings.
D. Make sure you have the right cable. Check to see if the WAN column has a solidly lit Link LED.
E. Make sure the cable connecting from your cable or DSL modem is connected to the Router's WAN port. Verify that the Status page of the Router's Web-based Utility shows a valid IP address from your ISP.

F. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's Web-based Utility to see if you get an IP address.

4. I am not able to access the Web-based Utility's Setup page.

A. Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
B. Refer to "Appendix G: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
C. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."
D. Refer to "Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

5. I can't get my Virtual Private Network (VPN) working through the Router.

Open the Router's Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" and go to the **Advanced => Filter** tab. Make sure you have IPsec pass-through and/or PPTP pass-through enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions *may* be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the Router's IP address to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

Check the Linksys website for more information at *www.linksys.com*.

6. I need to set up a server behind my Router.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the Router's Web-based Utility. We will be setting up web, ftp, and mail servers.

A. Open the Router's Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" and go to the **Advanced => Filter** tab.
B. Enter any **name** you want to use for the Customized Application.
C. Enter the **Ext. Port range** of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
D. Check the **protocol** you will be using, TCP and/or UDP.
E. Enter the **IP address** of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	Ext. Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X	X	192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X	X	192.168.1.102	X
POP3 (incoming)	110 to 110	X	X	192.168.1.102	X

When you have completed the configuration, click the **Apply** button and then the **Continue** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

A. Open the Router's Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" and go to the **Advanced => Filter** tab.
B. Enter any **name** you want to use for the Customized Application.
C. Enter the **Ext. Port range** of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
D. Check the **protocol** you will be using, TCP and/or UDP.
E. Enter the **IP address** of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	Ext. Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

When you have completed the configuration, click the **Apply** button and then the **Continue** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.) Follow these steps to set DMZ hosting:

A. Open the Router's Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility" and go to the **Advanced => Filter** tab.
B. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
C. Click the **DMZ Host** tab.
D. Enter the Ethernet adapter's **IP address** of the computer you want exposed to the Internet. This will bypass the NAT firewall for that computer. Please refer to "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Once completed with the configuration, click the **Apply** button and then the **Continue** button.

9. I forgot my password, or the password prompt always appears when saving settings to the Router.

Reset the Router to factory default by pressing the **Reset** button for 30 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

A. Open the Router's Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility". Enter the default password **admin**, and click the **Password** tab.
B. Enter a **different password** in the Web-based Utility's Password field, and enter the same password in the second field to confirm the password.
C. Click the **Apply** and **Continue** buttons.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:
A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Internet Options**.
B. Click the **Connections** tab.
C. Click the **LAN settings** button and remove anything that is checked.
D. Click the **OK** button to go back to the previous screen.
E. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:
A. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
B. Make sure you have **Direct connection to the Internet** selected on this screen.
C. Close all the windows to finish.

11. How do I set the Router to factory default?

Hold the **Reset** button for up to 30 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at *www.linksys.com*. Follow these steps:

A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware.
B. To upgrade the firmware, follow the steps in the Help section found in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility."

13. The firmware upgrade failed, and/or the Diag LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Diag LED stop flashing:

A. If the firmware upgrade failed, use the **TFTP** program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
B. Set a **static IP address** on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

> IP Address: 192.168.1.50
> Subnet Mask: 255.255.255.0
> Gateway: 192.168.1.1

C. Perform the upgrade using the TFTP program or the Router's Web-based Utility through its Help tab.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

A. To connect to the Router, go to the Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility"
B. Enter the **password**, if asked. (The default password is **admin**.)
C. In the Setup tab, select the option **Keep Alive**, and set the **Redial Period** option at **20** (seconds).
D. Click the **Apply** and **Continue** buttons.
E. Click the **Status** tab, and click the **Connect** button.
F. You may see the login status display as **Connecting**. Press the **F5** key to refresh the screen, until you see the login status display as **Connected**.
G. Click the **Apply** and **Continue** buttons to continue.

If the connection is lost again, follow steps E to G to re-establish connection.

15. I can't access my email, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. Most DSL users should use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Router, go to the Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility".
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Advanced => Filter** tab.
D. Look for the MTU option, and select **Enable**. In the Size field, enter **1492**.
E. Click the **Apply** and **Continue** buttons to continue.

If your difficulties continue, change the **Size** to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
> 1462
> 1400
> 1362
> 1300

16. I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the Router to open a specific port, depending on which port an Internet application uses. Follow these steps:

A. To connect to the Router, go to the Web-based Utility, as shown in "Chapter 6: The Cable/DSL VPN Router's Web-based Utility".
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Advanced => Forwarding** tab, and click the **Port Trigger** button.
D. Enter any **name** you want to use for the Application Name.
E. Enter the **Triggered Port Range**. Check with your Internet application provider for more information on which outgoing port services it is using.
F. Enter the **Incoming Port Range**. Check with your Internet Application provider for more information on which incoming port services are required by the Internet application.

17. The Diag LED stays lit continuously.

The Diag LED lights up when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED turns off to show that the system is working fine. If the LED remains lit after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

18. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

A. Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.

B. If the PCs are configured correctly, but still not working, check the Router. Verify that it is connected and ON. (If you cannot connect to it, check the LAN and power connections.)

C. If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.

D. Manually configure the TCP/IP with a DNS address provided by your ISP.

E. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

19. The Full/Col LED keeps flickering continuously.

A. Check the Category 5 Ethernet cable and its RJ-45 connectors.

B. There may be interference with other network devices. Try removing other PCs or network devices to see if the problem persists. Eliminate each network device one at a time to determine the cause.

Frequently Asked Questions

What is MIB? MIB (Management Information Base) is a data file that works in tangent with third-party SNMP software in managing the Router. To use MIB files in tangent with third-party SNMP software, follow the instructions that come with the thirty-party SNMP software. MIB data files will be available on the Linksys web site: www.linksys.com.

Can I use firmware for other routers with the BEFVP41? No. If you attempt to use other router's firmware, you could damage the Router. Only use firmware specifically written for the BEFVP41 as posted on the Linksys web site: *www.linksys.com*.

What is SNMP? SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) is a widely-used network monitoring and control protocol. For more information on SNMP, see "Appendix D: SNMP Functions."

What is the maximum number of IP addresses that the Router will support? The Router will support up to 253 IP addresses.

Does the Router support IPSec Pass-Through? Yes, it is a built-in feature that the Router automatically enables.

Where is the Router installed on the network? In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Does the Router support IPX or AppleTalk? No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from WAN to LAN.

Does the Router's WAN connection support 100 Mbps Ethernet? Because of the speed limitations of broadband Internet connections, the Router's WAN port supports 10 Mbps Ethernet. It does, of course, support 100 Mbps over its auto-sensing 10/100 ports.

What is **Network Address Translation** and what is it used for? Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Router support any operating system other than Windows 95, Windows 98, Windows 2000, Windows NT, or Windows XP? Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Router support ICQ send file? Yes, with the following fix: click **ICQ menu -> preference -> connections tab->**, and check **I am behind a firewall or proxy**. Then set the firewall time-out to **80** seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do? If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port (8080 usually works well but is used for remote admin. You may have to disable this.), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address? It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get *Half-Life: Team Fortress* to work with the Router? The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. *One problem:* Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

How can I block corrupted FTP downloads? If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do? Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at *www.linksys.com* for more information.

If all else fails in the installation, what can I do? Reset the Router by holding down the reset button until the Diag LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

How will I be notified of new Router firmware upgrades? All Linksys firmware upgrades are posted on the Linksys website at *www.linksys.com*, where they can be downloaded for free. The Router's firmware can be upgraded with TFTP programs. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment? Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to access the Router's Web-based Utility. What can I do? You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

What is DMZ Hosting? Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. You should set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Router? No.

Does the Router pass PPTP packets or actively route PPTP sessions? The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible? Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded? Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

Does the Router replace a modem? Is there a cable or DSL modem in the Router? No, this version of the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router? The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

What are the Router's advanced features? The Router's advanced features include IP Filtering, Port Range Forwarding, Dynamic Routing, Static Routing, DMZ hosting, and MAC Address Cloning.

What is the maximum number of VPN sessions allowed by the Router? The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions *may* be possible, depending on the specifics of your VPNs.

How big is the Router's memory buffer? It includes a 1MB buffer and 512KB flash.

How can I check whether I have static or DHCP IP Addresses? Consult your ISP to obtain this information.

How do I get mIRC to work with the Router? Under the Port Range Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

If your questions are not addressed here, refer to the Linksys website, *www.linksys.com***.**

Appendix B: Maximizing VPN Security

Just as you maximized your network security with a firewall router, you should also maximize security for your data with the VPN Router.

IPSec is compatible with most VPN endpoints and ensures privacy and authentication for data, while authenticating user identification. With IPSec, authentication is based upon the PC's IP Address. This not only confirms the user's identity but also establishes the secure tunnel at the network layer, protecting all data that passes through.

By operating at the network layer, IPSec is independent of any applications running on the network. This way, it doesn't harm your PC's performance and still allows you to do more with greater security. Still, it is important to note that IPSec encryption does create a slight slowdown in network throughput, due to encrypting and decrypting data.

Some VPNs will still leave the IP headers decrypted. These headers contain the IP Addresses for the users at both ends of the VPN tunnel and can be utilized by the hacker in future attacks. The VPN Router, however, does not leave the IP headers decrypted. Using a method called PFS (Perfect Forward Secrecy), not only are the IP headers encrypted but the secret keys used to secure the tunnel are encrypted as well.

All of this protection actually comes at a lower cost than most VPN endpoint software packages. The VPN Router will allow the users on your network to secure their data over the Internet without having to purchase the extra client licenses that other VPN hardware manufacturers and software packages will require. With VPN functions handled by the router, rather than your PC (which software packages would require), this frees up your PCs to perform more functions, more efficiently. An additional benefit is that you aren't required to reconfigure any of your network PCs.

As secure as the VPN Router makes your data, there are still more ways to maximize security. The following are a few suggestions on how to increase data security beyond the VPN Router.

1) Maximize security on your other networks. Install firewall routers for your Internet connections, and use the most up-to-date security measures for wireless networking.

2) Narrow the scope of your VPN tunnel as much as possible. Rather than allowing a range of IP Addresses, use the addresses specific to the endpoints required.

3) Do not set the Remote Security Group to Any, as this will open the VPN to any IP Address. Host a specific IP address.

4) Maximize encryption and authentication. Use 3DES encryption and SHA authentication whenever possible.

5) Manage your pre-shared keys. Change pre-shared keys regularly.

Data transmission over the Internet is a hole in network security that is often overlooked. With VPN maximized, along with the use of a firewall router and wireless security, you can secure your data even when it leaves your network.

Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the VPN Router

Introduction

This document demonstrates how to establish a secure IPSec tunnel using pre-shared keys to join a private network inside the VPN Router and a Windows 2000 or XP PC. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

Windows 2000 or Windows XP
IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

BEFSX41
WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0
LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

> **Note:** Keep a record of any changes you make. Those changes will be identical in the Windows "secpol" application and the Router's Web-Based Utility.

Step One: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the Open field. The Local Security Setting screen will appear as shown in Figure C-1.
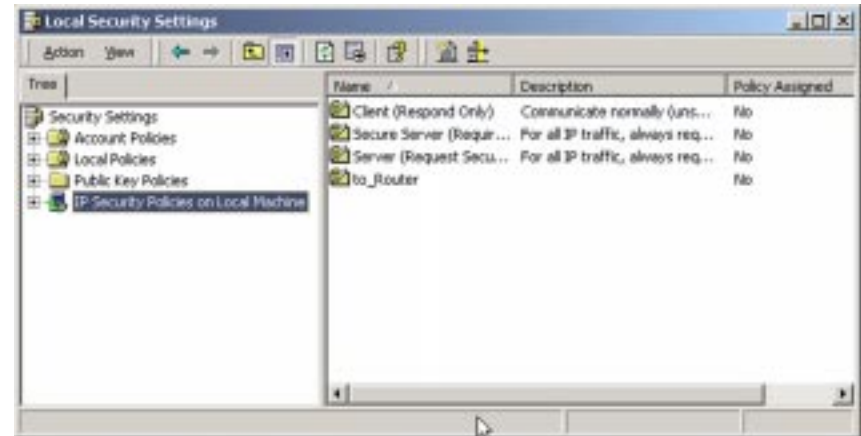

Figure C-1

2. Right-click **IP Security Policies on Local Computer**, and click **Create IP Security Policy**.

3. Click the **Next** button, and then enter a name for your policy (for example, **to_router**). Then, click **Next**.

4. Deselect the **Activate the default response rule** check box, and then click the **Next** button.

5. Click the **Finish** button, making sure the **Edit** check box is checked.

Step Two: Build Filter Lists

Filter List 1: win->router

⚠️ **Note:** The references in this section to "win" are references to Windows 2000 and XP.

1. In the new policy's properties screen, verify that the **Rules** tab is selected, as shown in Figure C-2. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.

Figure C-2

2. Make sure the **IP Filter List** tab is selected, and click the **Add** button.

Figure C-3

3. The *IP Filter List* screen should appear, as shown in Figure C-4. Enter an appropriate name, such as **win->router**, for the filter list, and de-select the **Use Add Wizard** check box. Then, click the **Add** button.

Figure C-4

4. The *Filters Properties* screen will appear, as shown in Figure C-5. Select the **Addressing** tab. In the Source address field, select **My IP Address**. In the Destination address field, select **A specific IP Subnet**, and fill in the IP Address: **192.168.1.0** and Subnet mask: **255.255.255.0**. (These are the Router's default settings. If you have changed these settings, enter your new values.)

Figure C-5

5. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

6. Click the **OK** button. Then, click the **OK** (for Windows XP) or **Close** (for Windows 2000) button on the *IP Filter List* window.

Filter List 2: router=>win

7. The *New Rule Properties* screen will appear, as shown in Figure C-6. Select the **IP Filter List** tab, and make sure that **win -> router** is highlighted. Then, click the **Add** button.
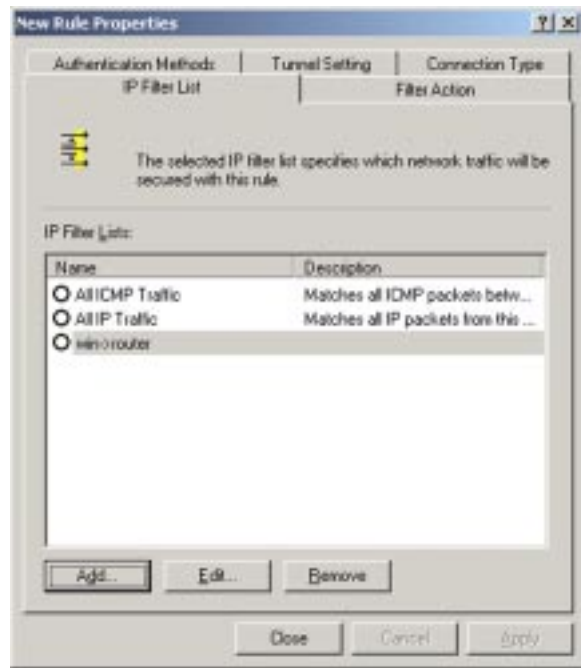
Figure C-6

8. The *IP Filter List* screen should appear, as shown in Figure C-7. Enter an appropriate name, such as **router->win** for the filter list, and de-select the **Use Add Wizard** check box. Click the **Add** button.
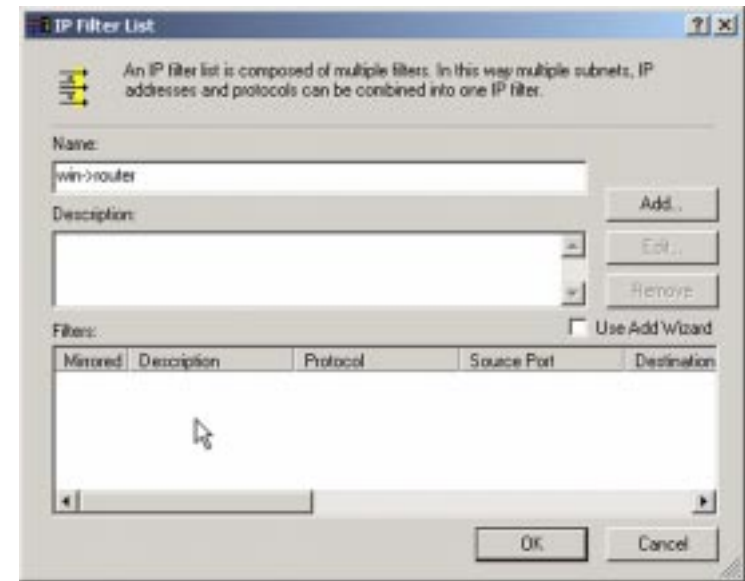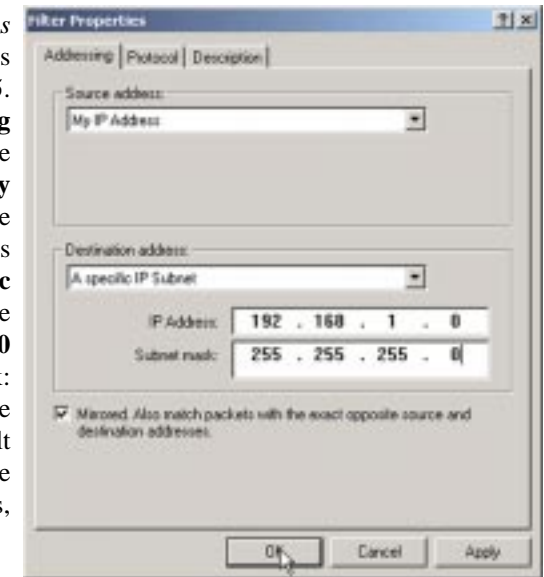
Figure C-7

9. The *Filters Properties* screen will appear, as shown in Figure C-8. Select the **Addressing** tab. In the Source address field, select **A specific IP Subnet**, and enter the IP Address: **192.168.1.0** and Subnet mask: **255.255.255.0**. (Enter your new values if you have changed the default settings.) In the Destination address field, select **My IP Address**.
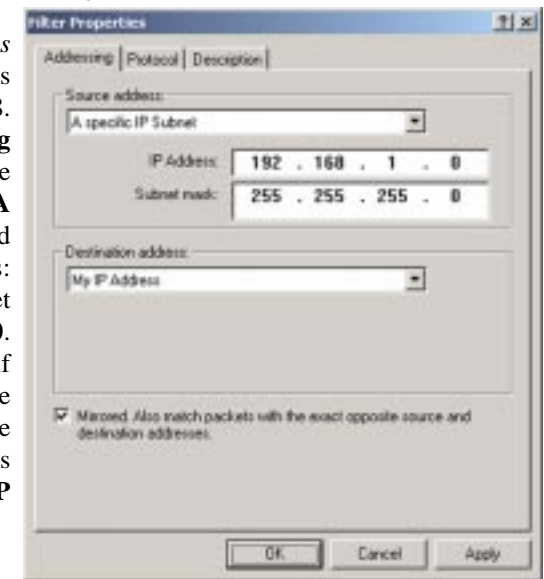
Figure C-8

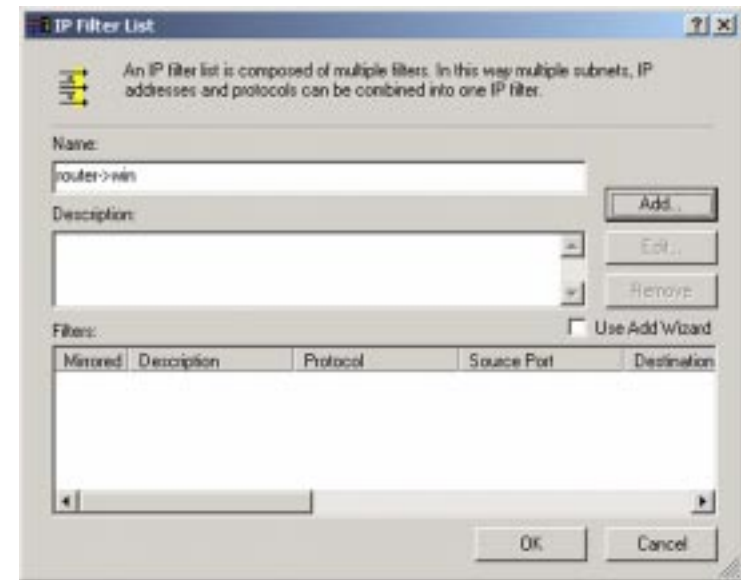10. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

11. Click the **OK** button and the *New Rule Properties* screen should appear with the IP Filer List tab selected, as shown in Figure C-9. There should now be a listing for "router -> win" and "win -> router". Click the **OK** (for WinXP) or **Close** (for Win2000) button on the *IP Filter List* window.

Figure C-9

Step Three: Configure Individual Tunnel Rules

Tunnel 1: win->router

1. From the *IP Filter List* tab, shown in Figure C-10, click the filter list **win->router**.
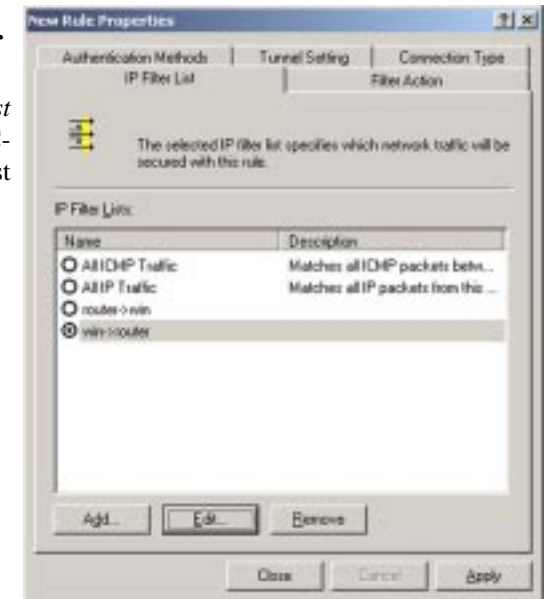
Figure C-10

2. Click the **Filter Action** tab (as in Figure C-11), and click the filter action **Require Security** radio button. Then, click the **Edit** button.
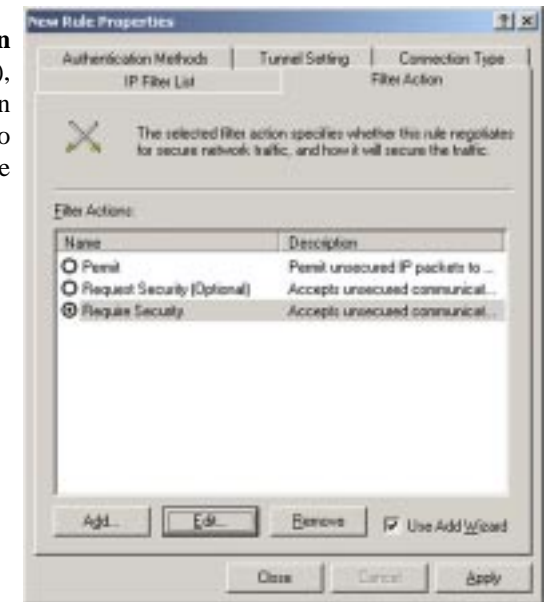
Figure C-11

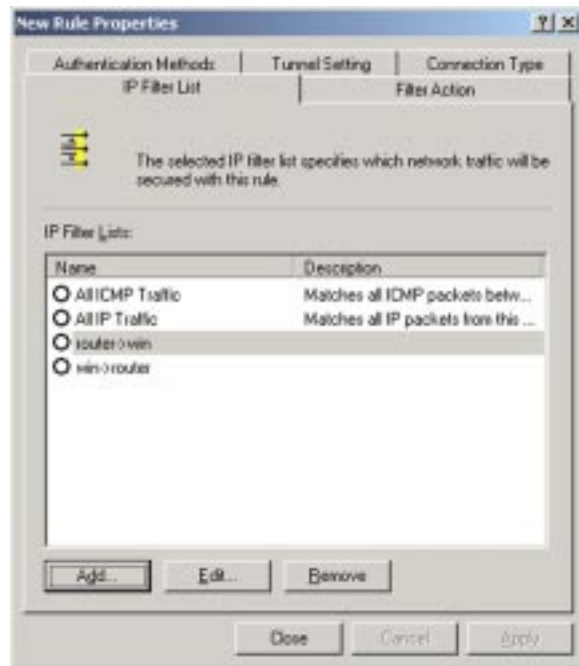3. From the *Security Methods* tab, shown in Figure C-12, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

Figure C-12

4. Select the **Authentication Methods** tab, shown in Figure C-13, and click the **Edit** button.

Figure C-13

5. Change the authentication method to **Use this string to protect the key exchange (pre-shared key)**, as shown in Figure C-14, and enter the preshared key string, such as **XYZ12345**. Click the **OK** button.

Figure C-14

6. This new Preshared key will be displayed in Figure C-15. Click the **OK** or **Close** button to continue.
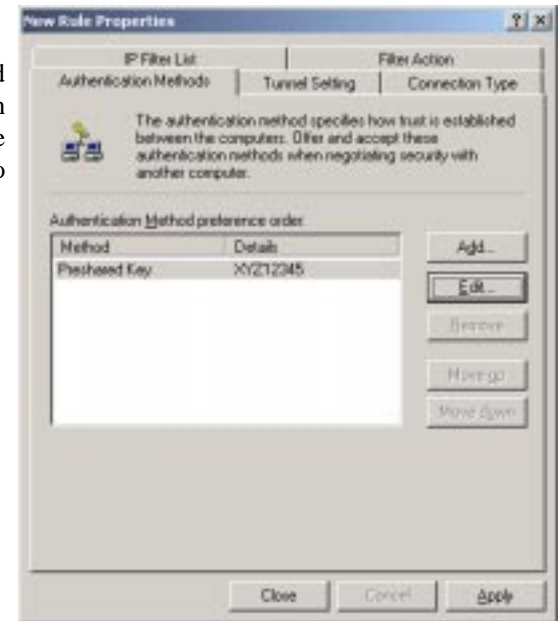
Figure C-15

7. Select the **Tunnel Setting** tab, shown in Figure C-16, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the Router's **WAN IP Address**.

Figure C-16

8. Select the **Connection Type** tab, as shown in Figure C-17, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

Figure C-17

Tunnel 2: router->win

9. In the new policy's properties screen, shown in Figure C-18, make sure that "win -> router" is select and deselect the **Use Add Wizard** check box. Then, click the **Add** button to create the second IP filter.
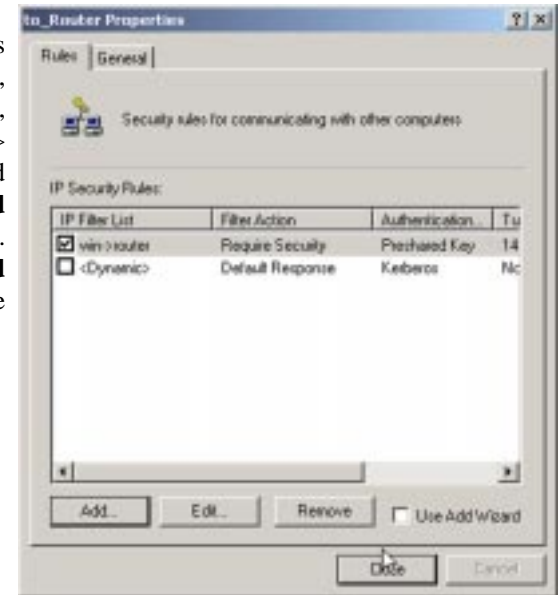
Figure C-18

10. Go to the **IP Filter List** tab, and click the filter list **router->win**, as shown in Figure C-19
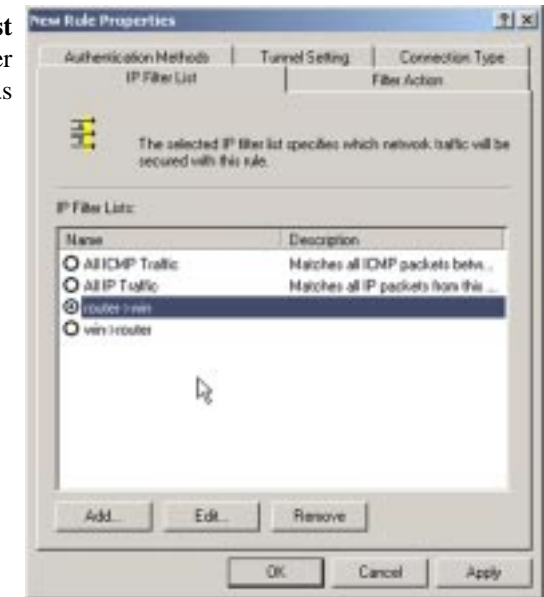
Figure C-19

11. Click the **Filter Action** tab, and select the filter action **Require Security**, as shown in Figure C-20. Then, click the **Edit** button.

Figure C-20

13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as **XYZ12345**, as shown in Figure C-22. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.
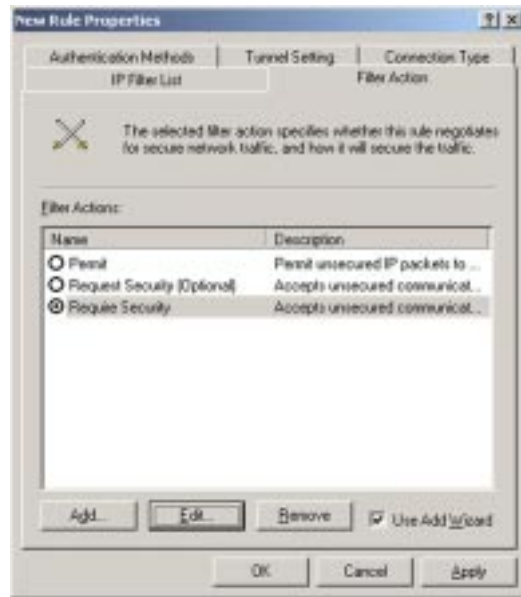
Figure C-22

12. Click the **Authentication Methods** tab, and verify that the authentication method *Kerberos* is selected, as shown in Figure C-21. Then, click the **Edit** button.
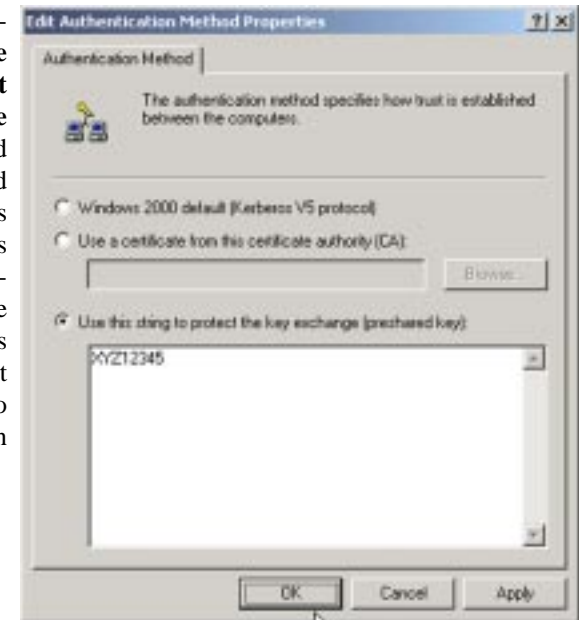
Figure C-21

14. This new Preshared key will be displayed in Figure C-23. Click the **OK** button to continue.

Figure C-23

15. From the Tunnel Setting tab, shown in Figure C-24, click the radio button for **The tunnel endpoint is specified by this IP Address**, and enter the Windows 2000/XP computer's IP Address.
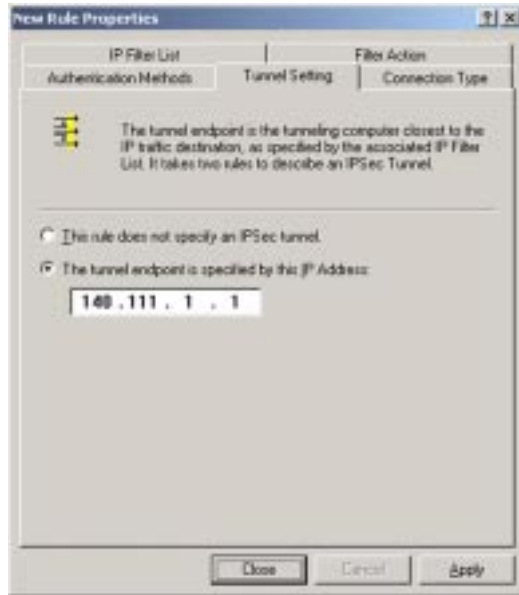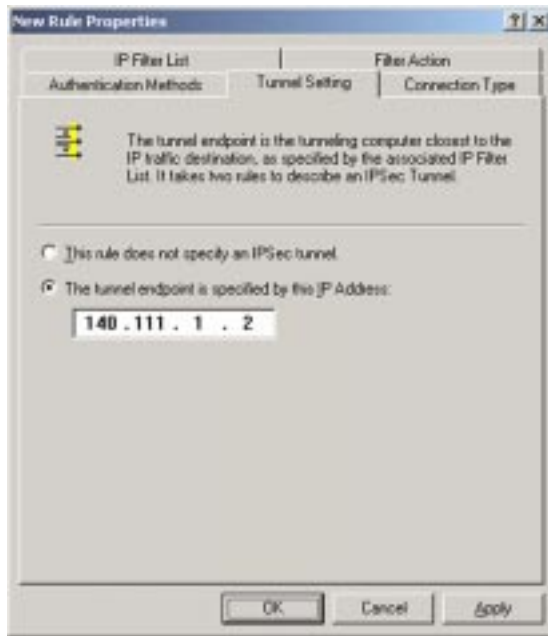

Figure C-24

16. Click the **Connection Type** tab, shown in Figure C-25, and select **All network connections**. Then click the **OK** (for Windows XP) or **Close** (for Windows 2000) button to finish.

Figure C-25

17. From the Rules tab, shown in Figure C-26, click the **OK** button to return to the secpol screen.
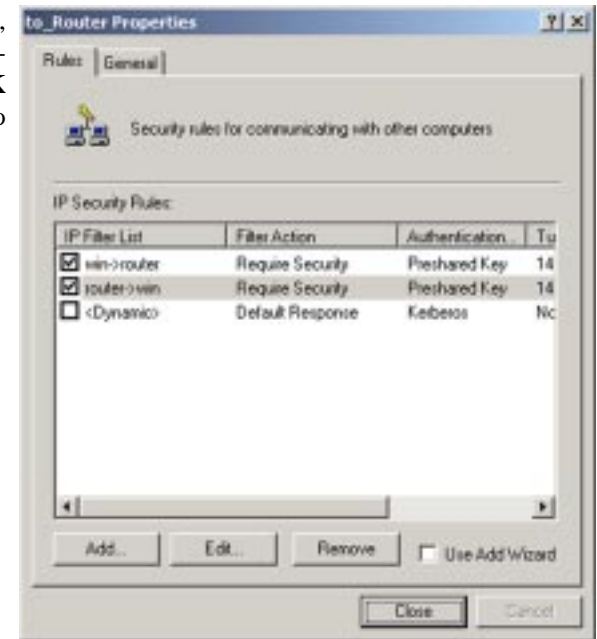
Figure C-26

Step Four: Assign New IPSec Policy

In the **IP Security Policies on Local Computer** window, shown in Figure C-27, right-click the policy named **to_router**, and click **Assign**. A green arrow appears in the folder icon.
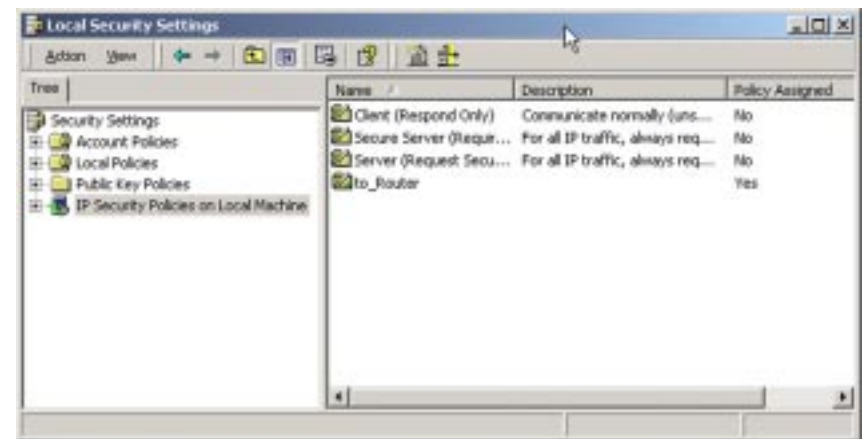
Figure C-27

Step Five: Create a Tunnel Through the Web-Based Utility

⚠️ **Note:** Further details on this step can be found in the VPN Tab section in "Chapter 6: The Cable/DSL VPN Router's Web-Based Utility".

1. Open your web browser, and enter **192.168.1.1** in the Address field. Press the **Enter** key.

2. When the User name and Password field appears, skip the user name and enter the default password **admin**. Press the **Enter** key.

3. From the Setup tab, shown in Figure C-28, click the **VPN** tab.

Figure C-28

4. From the VPN tab, shown in Figure C-29, select **Enable** beside This Table.

5. Enter a **Tunnel Name**. This name should be unique for this particular tunnel.

6. Select **Subnet** from the pull-down menu beside Local Secure Group. Then, enter the **IP Address** for this group. This would be the IP Address of the local endpoint, your endpoint.

7. Select **IP Addr.** from the pull-down menu beside Remote Secure Group. Then, enter the **IP Address** for this group. This would be the IP Address of the remote endpoint, the endpoint on the other side of the tunnel.

8. Select **IP Addr.** from the pull-down menu beside Remote Security Gateway. This would be the IP Address of your Internet connection as seen from the Internet. Enter this **IP Address** here.

9. Select a type of **encryption** and **authentication** for the tunnel your are establishing.

10. Check **PFS (Perfect Forward Secrecy)** and enter the **Pre-Shared Key** and **Key Lifetime**.

11. Click the **Apply** button followed by the **Continue** button.

12. Click the **Connect** button.

Your tunnel should now be established.

Figure C-29

Appendix D: SNMP Functions

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) is a widely-used network monitoring and control protocol. Data is passed from a SNMP agent, such as the VPN Router, to the workstation console used to oversee the network. The Router then returns information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

SNMP functions, such as statistics, configuration, and device information, are not available without third-party Management Software. The Router is compatible with all HP Openview compliant software.

Appendix E: How to Ping Your ISP's E-mail & Web Addresses

Virtually all Internet addresses are configured with words or characters (i.e., www.linksys.com, www.yahoo.com, etc.) In actuality, however, these Internet addresses are assigned to IP addresses, which are the true addresses on the Internet. For example, www.linksys.com is actually 206.135.116.3. Type it into your web browser and you will wind up at the Linksys home page every time.

IP and web addresses, however, can sometimes be long and hard to remember. Because of this, certain ISPs will shorten their server addresses to single words or codes on their users' web browser or e-mail configurations. If your ISP's E-mail and Web server addresses are configured with single words ("www", "e-mail", "home", "pop3", etc.) rather than whole Internet Addresses or IP Addresses, the Router may have problems sending or receiving mail and accessing the Internet. This happens because the Router has not been configured by your ISP to accept their abbreviated server addresses.

The solution is to determine the true web addresses behind your ISPs code words. You can determine the IP and web addresses of your ISP's servers by "pinging" them.

Important: If you don't have your ISP's web and e-mail IP Addresses, you *must* either get them from your ISP or follow these steps *prior* to connecting the Router to your network.

Step One: Pinging for an IP Address

The first step to determining your ISP's web and e-mail server address is to ping its IP Address.

1. **Power on the computer and the cable or DSL modem**, and restore the network configuration set by your ISP if you have since changed it.

2. **Click Start**, select **Run,** and type **command**. This will bring up the DOS Window.

3. **At the DOS command prompt**, type **ping mail** (assuming that the location for which you're trying to find an IP address is configured as "mail"). Press the **Enter** key. Information such as the following data, taken from a ping of Microsoft Network's e-mail server, will be displayed.

```
C:\>ping mail

Pinging mail [24.53.32.4] with 32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128

Ping statistics for 24.53.32.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
  loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure E-1

4. **Write down the IP address returned by the ping command**. (In the example above: 24.53.32.4.) This IP address is the actual IP address of the server "mail", or any other word or value you have pinged.

Step Two: Pinging for a Web Address

While the IP address returned above would work as your e-mail server address, it may not be permanent. IP Addresses change all the time. Web addresses, however, usually don't. Because of this, you're likely to have less problems by configuring your system with web addresses rather than IP addresses. Follow the instructions below to find the web address assigned to the IP address you just pinged.

1. **At the DOS command prompt**, type **ping -a 24.53.32.4**, where 24.53.32.4 is the IP address you just pinged. Information such as the following data will be displayed:

```
C:\>ping -a 24.53.32.4

Pinging mail.msnv3.occa.home.com [24.53.32.4] with 32
  bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127

Ping statistics for 24.53.32.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
  loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure E-2

2. **Write down the web address returned by the ping command**. (In the example above: mail.msnv3.occa.home.com.) This web address is the web address assigned to the IP address you just pinged. While the IP address of "mail" could conceivably change, it is likely that this web address will not.

3. **Replace your ISP's abbreviated server address** with this extended web address in the corresponding Internet application (web browser, e-mail application, etc.).

Once you have replaced the brief server address with the true server address, the Router should have no problem accessing the Internet through that Internet application.

Appendix F: Installing the TCP/IP Protocol

Follow these instructions to install the TCP/IP Protocol on one of your PCs *only* after a network card has been successfully installed inside the PC. These instructions are for Windows 95, 98, and Millennium. For TCP/IP setup under Windows NT, 2000, or XP, please refer to your Windows documentation.

1. Click the **Start** button. Choose **Settings**, and then **Control Panel**.

2. Double-click the **Network** icon. Your Network window should pop up. Select the **Configuration** tab.

Figure F-1

3. Click the **Add** button**.**

4. Double-click **Protocol**.

5. Highlight **Microsoft** under the list of manufacturers.

6. Find and double-click **TCP/IP** in the list to the right in Figure F-2.
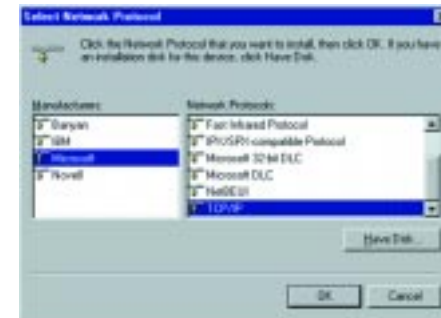
Figure F-2

7. After a few seconds you will be brought back to the main Network window. The TCP/IP Protocol should now be listed.

Figure F-3

8. Click **OK**. Windows may ask for original Windows installation files. Supply them as needed (e.g.: c:\windows\options\cabs., D:\win98, D:\win95, D:\win9x, etc.)

9. Windows will ask you to restart the PC. Click **Yes**.

The TCP/IP Installation is complete.

Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your Ethernet adapter to do either MAC Filtering or MAC Address Cloning for the Router and ISP. You can also find the IP address of your computer's Ethernet adapter. The IP address is used for filtering, forwarding, and DMZ. Follow the steps in this appendix to find the MAC address or IP address for your adapter in Windows 95, 98, Me, NT, 2000, and XP.

For Windows 95, 98, and Me:

1. Click on **Start** and **Run**. In the Open field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.

Figure G-1

2. When the IP Configuration window appears, select the Ethernet adapter you are using to connect to the Router via a CAT 5 Ethernet cable.

Figure G-2

3. Write down the Adapter Address as shown on your computer screen (see Figure G-3). This is the MAC address for your Ethernet adapter and will be shown as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC Address Cloning or MAC Filtering.

Figure G-3

The example in Figure G-3 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

> **Note**: The MAC address is also called the Adapter Address.

For Windows NT, 2000, and XP:

The following steps show an alternative way of obtaining the MAC address and IP address for your Ethernet adapter.

1. Click on **Start** and **Run**. In the Open field, enter **cmd**. Press the **Enter** key or click the **OK** button.
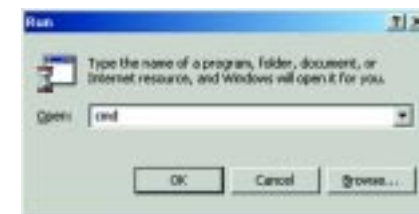
Figure G-4

2. In the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
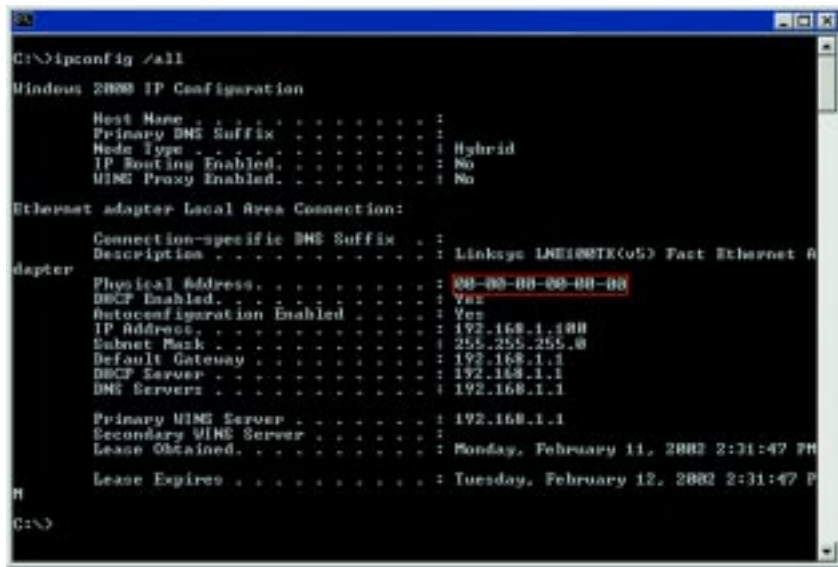
Figure G-5

3. Write down the Physical Address as shown on your computer screen; it is the MAC address for your Ethernet adapter. This will appear as a series of letters and numbers.

The MAC address/Physical Address is what you will use for MAC Address Cloning or MAC Filtering.

Note: The MAC address is also called the Physical Address.

The example in Figure G-5 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

When entering the information using the Router's Web-based Utility, you will type the **12-digit MAC address** in this format, XXXXXXXXXXXX *without the hyphens* for MAC Filtering. See Figure G-6.
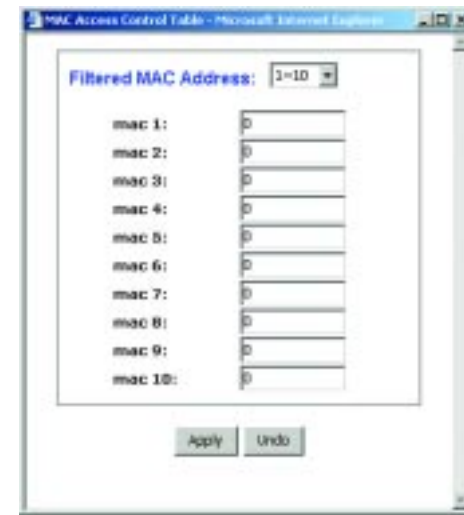
Figure G-6

When entering information for MAC Address Cloning, type the **12-digit MAC address** (see Figure G-7).

Figure G-7

Appendix H: Glossary

3DES - 3DES is a variation on DES that uses a 168-bit key.

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

AppleTalk - An Apple Computer networking system that supports Apple's proprietary local talk.

Auto-negotiate - To automatically determine the correct settings. The term is often used with communications and networking. For example, Ethernet 10/100 cards, hubs and switches can determine the highest speed of the node they are connected to and adjust their transmission rate accordingly.

Boot - To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it and pass control to it.

Broadband - A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

Buffer - A buffer is a shared or assigned memory area used by hardware devices or program processes that operate at different speeds or with different sets of priorities. The buffer allows each device or process to operate without being held up by the other. In order for a buffer to be effective, the size of the buffer and the algorithms for moving data into and out of the buffer need to be considered by the buffer designer. Like a cache, a buffer is a "midpoint holding place" but exists not so much to accelerate the speed of an activity as to support the coordination of separate activities.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

CAT 5 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

DES (**D**igital **E**ncryption **S**tandard) - Encryption used for data communication where both the sender and receiver must know the same secret key, used to encrypt and decrypt the data, or to generate and verify a message authentication code. Linksys DES encryption uses a 56-bit key.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DMZ (**De**militarized **Z**one) - Allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. You should set your computer with a static IP address if you want to use DMZ Hosting.

DNS - The domain name system (DNS) is the way that Internet domain name are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain - A subnetwork comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download - To receive a file transmitted over a network. In a communications session, download means receive, upload means transmit.

DSL (**D**igital **S**ubscriber **L**ine) - A technology that dramatically increases the digital capacity of ordinary telephone lines into the home or office and, by employing unused bandwidth, still allows for normal phone usage. DSL provides "always-on" operation, eliminating the need to dial in to the service.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Dynamic Routing - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - Standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

Firewall - A firewall is a set of related programs, located at a network gateway server, that protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

Basically, a firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

Firmware - Code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server using FTP.

FTP includes functions to log onto the network, list directories and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Unlike e-mail programs in which graphics and program files have to be "attached," FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

Full Duplex - The ability of a device or line to transmit data simultaneously in both directions.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to dis-

tinguish the "box" and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

Hop - The link between two network nodes.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a Web server and transmit HTML pages to the client browser.

Hub - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

ICQ - A conferencing program for the Internet that provides interactive chat, e-mail and file transfer and can alert you when someone on your predefined list has also come online.

IKE (**I**nternet **K**ey **E**xchange) - A negotiation and key exchange protocol specified by the Internet Engineering Task Force. An IKE security association (SA) automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass encrypted data over the Internet or any other network.

IP (**I**nternet **P**rotocol) - The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to be able to understand each other.

IP Address - In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IPSec (**I**nternet **P**rotocol **S**ecurity) - A suite of protocols used to implement secure exchange of packets at the IP layer. IPSec supports two basic modes: Transport and Tunnel. Transport encrypts the payload of each packet, leaving the header untouched, while Tunnel mode encrypts both the header and the payload and is therefore more secure. IPSec must be supported on both transmitter and receiver and must share a public key. Tunnel mode is widely deployed in VPNs (Virtual Private Networks).

IPX (**I**nternetwork **P**acket E**X**change) - A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides individuals and companies access to the Internet and other related services such as Web site building and virtual hosting.

LAN (**L**ocal **A**rea **N**etwork) - A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

MAC (**M**edia **A**ccess **C**ontrol) **Address** - A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Mbps (**M**ega**b**its **p**er **s**econd) - One million bits per second; unit of measurement for data transmission.

MD5 - A type of one-way authentication method that uses passwords. MD5 authentication is not as secure as the EAP-TLS or EAP/TTLS authentication methods.

MIB (**M**anagement **I**nformation **B**ase) - A set of database objects. This set contains information about a specific device for utilizing SNMP.

mIRC - mIRC runs under Windows and provides a graphical interface for logging onto IRC servers and listing, joining and leaving channels.

Multicasting - Sending data to a group of nodes instead of a single destination.

NAT (**N**etwork **A**ddress **T**ranslation) - The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

NetBIOS - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols.

NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server.

There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

Network - A system that transmits any combination of voice, video and/or data between users.

Network Mask - Also known as the "Subnet Mask".

Node - A network junction or connection point, typically a computer or work station.

Notebook (PC) - A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than five pounds and is three inches or less in thickness.

Packet - A unit of data routed between an origin and a destination in a network.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems and printers.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A protocol which allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol but rather describes a "tunneling service" for carrying PPP (a tunneling service is any network service enabled by tunneling protocols such as PPTP, L2F, L2TP, and IPSEC tunnel mode). One example of a tunneling service is secure access from a remote small office network to a headquarters corporate intranet via a Virtual Private Network (VPN) that traverses the Internet. However, tunneling services are not restricted to corporate environments and may also be used for personal (i.e., non-business) applications.

RIP (**R**outing **I**nformation **P**rotocol) - A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.

RJ-45 (**R**egistered **J**ack-**45**) - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

Router - Protocol-dependent device that connects subnetworks together. Routers are useful in breaking down a very large network into smaller subnetworks; they introduce longer delays and typically have much lower throughput rates than bridges.

Security Association - A group of security settings related to a specific VPN tunnel.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user.

A common misconception is that software is data. It is not. Software tells the hardware how to process the data.

SPI (**S**tateful **P**acket **I**nspection) - A firewall technology that monitors the state of the transaction so that it can verify that the destination of an inbound packet matches the source of a previous outbound request. It examines not just the headers of the packet, but also the contents, to determine more about the packet than just its source and destination information. It is called "stateful" because verifies that the stated destination computer has previously requested the current communication. In this way, it verifies that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being a more rig-

orous inspection, stateful packet inspection closes off ports until connection to the specific port is requested. This allows an added layer of protection from the threat of port scanning.

Static IP Address - A permanent IP address that is assigned to a node in an IP or a TCP/IP network.

Static Routing - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

Switch - 1. A data switch connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a "connection oriented" protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one place to another in a given time period.

UDP (**U**ser **D**atagram **P**rotocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling

the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connection-less" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network. In a communications session, upload means transmit, download means receive.

URL (**U**niform **R**esource **L**ocator) - The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

VPN (**V**irtual **P**rivate **N**etwork) - A technique that allows two or more LANs to be extended over public communication channels by creating private communication subchannels (tunnels). Effectively, these LANs can use a WAN as a single large "virtually private" LAN. This removes the need to use leased lines for WAN communications through secure use of a publicly available WAN (such as the Internet). Examples of VPN technology are: PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (Internet Protocol Security).

VPN endpoint - VPN end point capability within a router provides the ability to initiate a VPN tunnel to some other location that supports either a VPN client or has VPN end point capability.

WAN (**W**ide **A**rea **N**etwork)- A communications network that covers a relatively large geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the telephone (DSL) or cable systems, or through leased lines or satellites. In its most basic definition, the Internet could be considered a WAN.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

Workgroup - Two or more individuals that share files and databases.

Appendix I: Specifications

Model Number:	BEFVP41
Standards:	IEEE 802.3 (10BaseT),
	IEEE 802.3u (100BaseTX)
Protocol:	CSMA/CD
VPN Encryption:	DES (56-bit), 3DES (168-bit)
VPN Authentication:	MD5, SHA
Ports:	
WAN:	One 10Base-T RJ-45 Port
LAN:	Four 10/100 RJ-45 Ports
Cabling Type:	
10BaseT:	UTP Category 3 or better
100BaseTX:	UTP Category 5 or better
Speed (Mbps):	WAN: 10
	LAN: 10/100 (Half Duplex Mode)
	20/200 (Full Duplex Mode)
LEDs	Power
	WAN: Diag, Act, Link
	LAN: Link/Act, Full/Col, 100
Topology:	Star

Environmental

Dimensions:	7.31" x 6.06" x 1.88" (186 mm x 154 mm x 48 mm)
Unit Weight:	12.8 oz. (0.36 kg)
Power:	External, 5V DC, 2.1 A
Certifications:	FCC Class B, CE Mark
Operating Temp.:	0ºC to 45ºC (32ºF to 113ºF)
Storage Temp.:	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity:	0% to 90%, Non-Condensing
Storage Humidity:	5% to 90%, Non-Condensing

Appendix J: Warranty Information

BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.

IN NO EVENT SHALL LINKSYS' LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDEN-TAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCU-MENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PROD-UCT.

LINKSYS OFFERS CROSS SHIPMENTS, A FASTER PROCESS FOR PRO-CESSING AND RECEIVING YOUR REPLACEMENT. LINKSYS PAYS FOR UPS GROUND ONLY. ALL CUSTOMERS LOCATED OUTSIDE OF THE UNITED STATES OF AMERICA AND CANADA SHALL BE HELD RESPONSIBLE FOR SHIPPING AND HANDLING CHARGES. PLEASE CALL LINKSYS FOR MORE DETAILS.

Appendix K: Contact Information

For help with the installation or operation of this product, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

Sales Information	800-546-5797 (LINKSYS)
Technical Support	800-326-7114
RMA Issues	949-271-5461
Fax	949-265-6655
Email	support@linksys.com
Web	http://www.linksys.com
FTP Site	ftp.linksys.com

LINKSYS®

http://www.linksys.com