LINKSYS®

A Division of Cisco Systems, Inc.

EtherFast®

Cable/DSL VPN Router

with 4-Port 10/100 Switch

User Guide

WIRED

Model No. **BEFVP41 v2**

Cisco Systems

Copyright and Trademarks

How to Use this Guide

This User Guide has been designed to make understanding networking with the Router easier than ever. Look for the following items when reading this Guide:

This checkmark means there is a Note of interest and is something you should pay special attention to while using the Router.

This exclamation point means there is a Caution or Warning and is something that could damage your property or the Router.

This question mark provides you with a reminder about something you might need to do while using the Router.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the EtherFast Cable/DSL VPN Router with 4-Port 10/100 Switch. This Router provides your network with a high-security way to share a high-speed Internet connection as well as resources, including files and printers.

How is this done? Inside this Router you have the Internet-access sharing ability of a standard Linksys Router, along with the network expandibility of a 4-Port 10/100 Switch, and the network security functions of VPN.

But what does all of this mean?

At the core of this Router, is a standard, Linksys Router, providing you the ability to share your broadband, Internet access within your network. This also comes with the protection of a firewall and the easy setup and configuration you've come to expect from a Linksys Router. Add to that the network expandibility of a 4-port 10/100 Switch. The four ports in the back of the Router are all auto-detecting, meaning that the Router can tell if you're connecting a straight-through or cross-over cable, making this easier to use than ever. Finally, adding VPN network security to the Router allows you to secure data, not just behind the Router, but as it is transmitted over the Internet. VPNs, or Virtual Private Networks, create virtual tunnels that connect your PC to another across the Internet, keeping the data secure as it passes from one to another.

In this User Guide, you'll find all you need to setup, configure, and use the Router, including appendices describing VPNs. Welcome to secure, broadband networking.

network: *a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users*

switch: *a data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports*

broadband: *an always-on, fast Internet connection*

firewall: *a set of related programs located at a network gateway server that protects the resources of a network from users from other networks*

What's in this Guide?

This user guide covers everything you'll need to know about the Router. In addition to giving directions in the Chapters about how to set it up and use it, serveral Appendices are provided for further information.

- Chapter 1: Introduction
  This chapter describes the Router's applications and this User Guide.
- Chapter 2: Networking Basics
  This chapter briefly explains how a network functions.
- Chapter 3: Getting to Know the Router
  This chapter provides a quick guide to the Router's LED display on the front and ports on the back.
- Chapter 4: Connecting the Router
  This chapter instructs you on how to connect the DSL modem to the Router and connect the PC(s) to the Router.
- Chapter 5: Configuring the Router
  This chapter explains how to configure the Router using your web browser and the Router's Web-based Utility. You will configure the Router using the settings provided by your ISP.
- Chapter 6: Using the Router's Web-based Utility
  This chapter describes the Web-based Utility and the features available, so you can use and alter advanced configuration settings.
- Appendix A: Troubleshooting
  This appendix describes some possible problems and solutions, as well as frequently asked questions, regarding installation and use of the Router.
- Appendix B: Upgrading Firmware
  This appendix explains how you can upgrade the Router's firmware.
- Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter
  This appendix instructs you on how to find the MAC address or Ethernet address of your PC's Ethernet network adapter.
- Appendix D: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

dsl: *an always-on broadband connection over traditional phone lines*

isp(*I****nternet*** ***S****ervice*** ***P****rovider): a company that provides access to the Internet*

firmware: *theprogramming code that runs a networking device*

ethernet: *an IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium*

mac *(****M****edia*** ***A****ccess*** ***C****ontrol) address: the unique address that a manufacturer assigns to each networking device*

- Appendix E: Maximizing VPN Security
  This appendix tells you how to get the most out of the VPN Router, using VPN tunnels.
- Appendix F: Configuring IPSec between a Windows 2000 or XP PC and the VPN Router
  So, how do you set your PCs up for VPN tunnels? This appendix tells you how.
- Appendix G: SNMP Functions
  This appendix tells you about the Simple Network Management Protocol.
- Appendix H: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix I: Specifications
  This appendix provides the technical specifications for the Router.
- Appendix J: Warranty Information
  This appendix supplies the warranty information for the Router.
- Appendix K: Regulatory Information
  This appendix supplies the regulatory information regarding the Router.
- Appendix L: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

***IPSec** (**I**nternet **P**rotocol **S**ecurity): A VPN protocol used to implement secure exchange of packets at the IP layer*

***snmp** (**S**imple **N**etwork **M**anagement **P**rotocol): a widely used network monitoring and control protocol*

Chapter 2: Your Virtual Private Network (VPN)

Why do I need a VPN?

***vpn** (**V**irtual **P**rivate **N**etwork): a security measure to protect data as it leaves one network and goes to another over the Internet*

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

***packet**: a unit of data sent over a network*

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.)

***encryption**: encoding data transmitted in a network*

***IP (Internet Protocol)**: a protocol used to send data over a network*

***software**: instructions for the computer*

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 (Windows 2000 and XP) allows the VPN Router to create a VPN tunnel using IPSec (refer to “Appendix F: 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. 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.

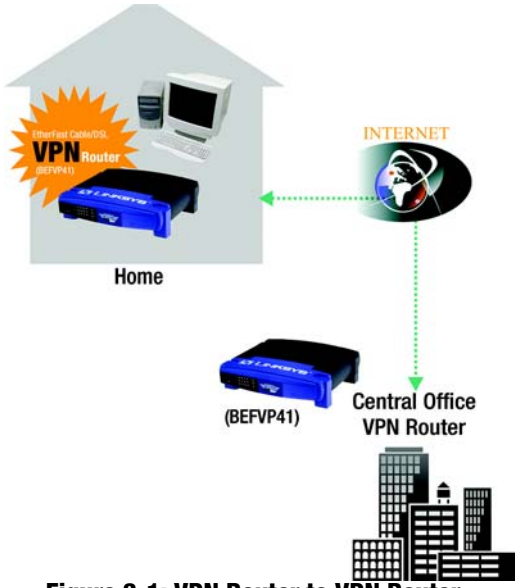

Figure 2-1: VPN Router to VPN Router

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. 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.

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

Figure 2-2: Computer to VPN Router

Chapter 3: Getting to Know the Router

The Back Panel

The Router's ports and the Reset button are located on the back panel of the Router.

Figure 3-1: Back Panel

Internet This **Internet** port connects to your cable or DSL modem.

1-4 These four **Ethernet** ports connect to network devices, such as PCs, print servers, or additional switches.

Reset Button The Reset button can be used in one of two ways:

If the Router is having problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the Reset button on your PC to reboot it.

If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for 30 seconds. This will restore the factory defaults and clear all of the Router's settings, such as port forwarding or a new password.

Power The **Power** port is where you will connect the power adapter.

port: *the connection point on a computer or networking device used for plugging in cables or adapters*

The Front Panel

The Router's LEDs, which inform you about network activities, are located on the front panel.

Figure 3-2: Front Panel

Power Green. The **Power** LED lights up when the Router is powered on. If the LED is flashing, the Router is running a diagnostic test.

Ethernet Green. The **Ethernet** LED serves two purposes. If the LED is continuously lit, the Router is connected to a device through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.

Internet Green. The **Internet** LED lights up when the Router is connected to your cable or DSL modem.

Proceed to "Chapter 4: Connecting the Router."

Chapter 4: Connecting the Router

Overview

To set up your network, do the following:

- Connect the Router to one of your PCs.
- If necessary, configure your PCs to obtain an IP address automatically from the Router. (By default, Windows 98, 2000, Millennium, and XP computers are set to obtain an IP address automatically, so unless you have changed the default setting, then you will not need to configure your PCs.)
- Configure the Router with the setting(s) provided by your Internet Service Provider (ISP).

IP Address: *the address used to identify a computer or device on a network*

The installation technician from your ISP should have left the setup information with you after installing your broadband connection. If not, you can call your ISP to request the information. Once you have the setup information for your specific type of Internet connection, then you can begin installation and setup of the Router.

adapter: *a device that adds network functionality to your PC*

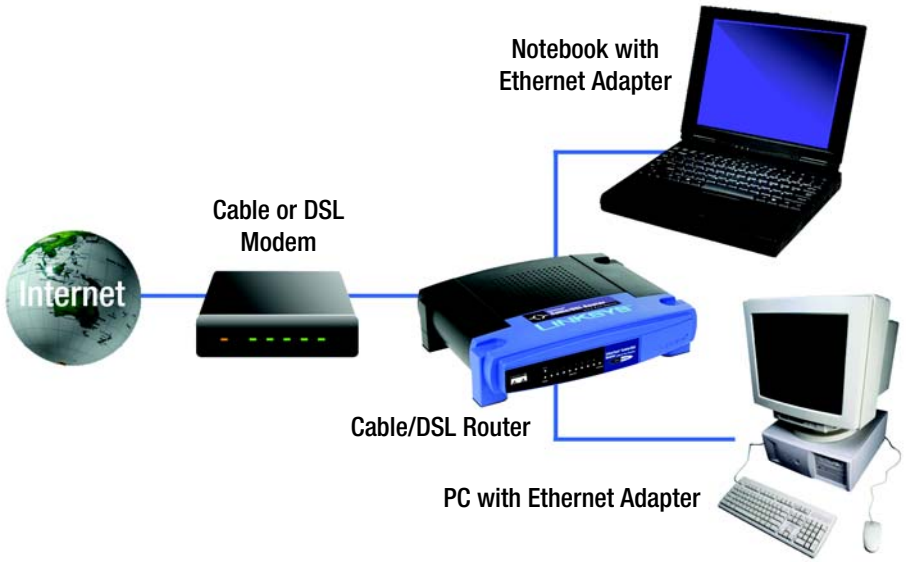

Figure 4-1: Example of a Typical Network

Connection Instructions

1. Before you begin, make sure that all of your hardware is powered off, including the Router, PCs, hubs, switches, and cable or DSL modem.
2. Connect one end of an Ethernet network cable to one of the numbered ports on the back of the Router. Connect the other end to an Ethernet port on a network device, e.g., a PC, print server, hub, or switch.

   Repeat this step to connect more PCs or other network devices to the Router.
3. Connect your cable or DSL modem's Ethernet cable to the Router's Internet port.
4. Power on the cable or DSL modem.
5. Connect the included power adapter to the Router's Power port, and then plug the power adapter into an electrical outlet.

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

Proceed to "Chapter 5: Configuring the Router."

Figure 4-2: Connect a PC

Figure 4-3: Connect the Internet

Figure 4-4: Connect the Power

Chapter 5: Configuring the Router

Note: The directions included in this Chapter are meant for quick configuration of the Router and do not include all you need to know to use all of the Router's functions. Complete directions on all of the Router's functions, configured through the Web-based Utility, can be found in Chapter 6: Using the Router's Web-based Utility.

Now that the Router is connected to your network, this chapter will walk you through a quick configuration.

Note: If the TCP/IP protocol is not configured on your PC, go to "Appendix D: Windows Help" for instructions on how Windows can help you configure this protocol on your PC.

browser: *an application program that provides a way to look at and interact with all the information on the World Wide Web*

1. Open your web browser and type **http://192.168.1.1** in the browser's Address box. This number is the Router's default IP address. Press the **Enter** key.

Figure 5-1: Router's IP Address for Basic Setup

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. 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 Router's LED is lit up for the port where you're connected.

Figure 5-2: Router Login screen

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.

   ***domain**: a specific name for a network of computers*

   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.

   ***static ip address**: a fixed address assigned to a computer or device that is connected to a network*

4. The Router supports six connection types: obtain an IP automatically (DHCP), Static IP, PPPoE, RAS, PPTP, and Heart Beat Signal. These types are listed in the drop-down menu for the **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.

   PPPoE (Point to Point Protocol over Ethernet): a type of broadband connection that provides authentication (username and password) in addition to data transport

   DHCP (Dynamic Host Configuration Protocol): a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

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.

Obtain an IP Automatically - DHCP

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

A. Select **Obtain an IP automatically** as the Connection Type.

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

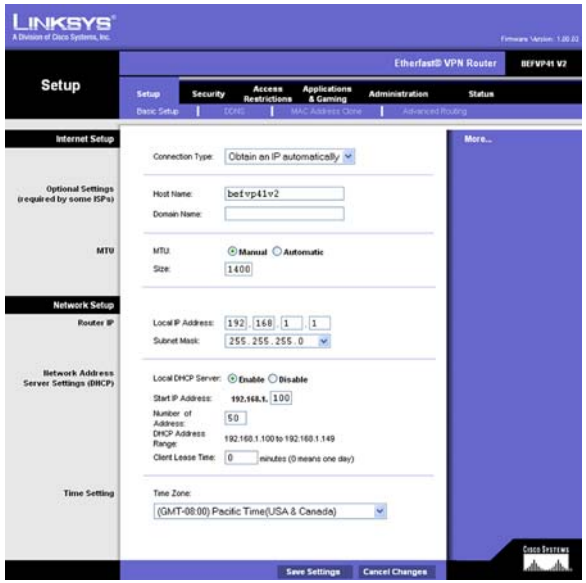

Figure 5-3: Basic DHCP Setup

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 Connection Type.

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 **Save Settings** button to save the settings, or click the **Cancel Changes** button to clear the settings and start over. When you are finished, then proceed to step 5.

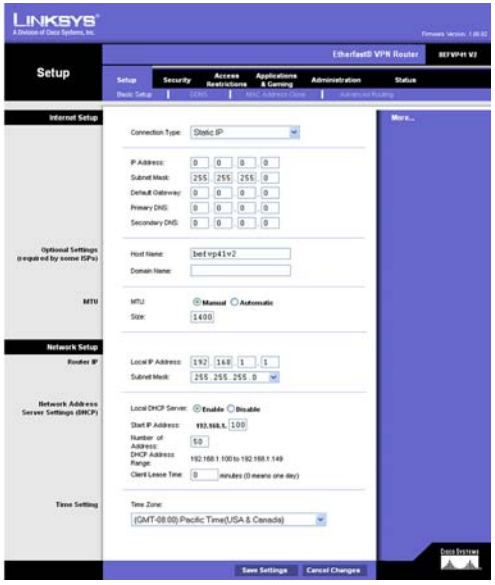

Figure 5-4: Basic Static IP Setup

PPPoE

If your DSL provider says that you are connecting through PPPoE or if you normally enter a user name and password to access the Internet, perform these steps:

A. Select **PPPoE** as the Connection Type.

B. Enter the **User Name**.

C. Enter the **Password**.

D. Enter the **Service Name**, if required.

E. Click the **Save Settings** button to save the settings, or click the **Cancel Changes** button to clear the settings and start over.

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

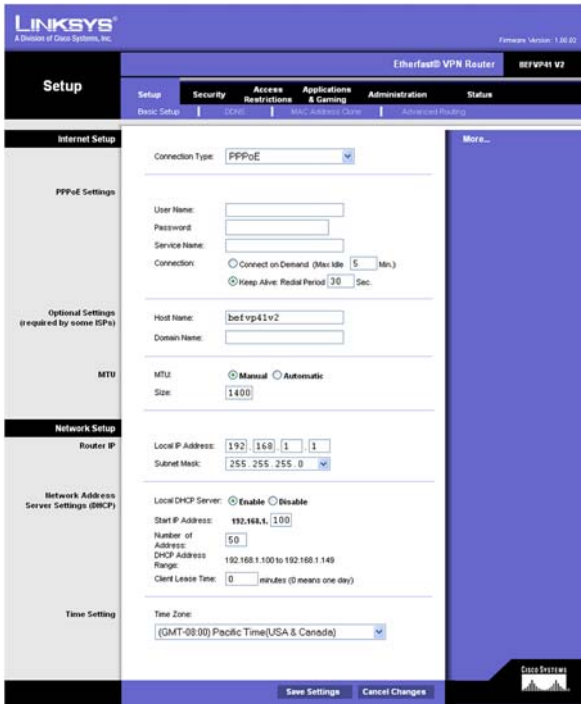

Figure 5-5: Basic PPPoE Setup

RAS

RAS is a service used in Singapore only. If you are using a RAS connection, check with your ISP for the necessary setup information.

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

PPTP

PPTP is a service used in Europe only. If you are using a PPTP connection, check with your ISP for the necessary setup information.

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

Heart Beat Signal

Heart Beat Signal is a service used in Australia only. If you are using a Heart Beat Signal connection, check with your ISP for the necessary setup information.

A. When finished making your changes on this tab, click the **Save Settings** button to save this change, or click the **Cancel Changes** button to undo your change. For further help on this tab, click the **Help** button.

B. Click the **Status** tab, and then click the **Connect** button. When you are finished, proceed to step 5.

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: Using the Router's Web-based Utility" or the Linksys support website at *support.linksys.com*.

Congratulations! You've successfully configured the Router. Test the setup by opening your web browser from any computer and entering *www.linksys.com/registration*.

Figure 5-6: The Registration URL

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: Using the Router's Web-based Utility"

for more details and advanced settings information.

Chapter 6: Using The Router's Web-based Utility

Overview

For your convenience, use the Router's Web-based Utility to administer it. This chapter will explain all of the functions in this Utility. The Utility can be accessed via Microsoft Internet Explorer or Netscape Navigator through use of a computer connected with an Ethernet cable to the Router.

For a basic network setup, most users only have to use the following screens of the Utility:

- Basic Setup
  On the *Basic Setup* screen, enter the settings provided by your ISP.
- Management
  Click the **Administration** tab and then select the **Management** screen. The Router's default password is **admin**. To secure the Router, change the Password from its default.

Navigating the Utility

There are six main tabs: Setup, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional screens will be available from the main tabs.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.
- DDNS. To enable the Router's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen.
- Advanced Routing. On this screen, you can alter Network Address Translation (NAT), Dynamic Routing, and Static Routing configurations.

***nat** (**N**etwork **A**ddress **T**ranslation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet.*

Security

- Firewall. This screen allows you to enable to disable the firewall, block Internet requests, and enable a variety of Internet filters.

- VPN. To enable and setup VPN Passthrough and configure up to 50 VPN tunnels, use this screen.

Access Restrictions

- Internet Access. From this screen, you will be able to manage Internet access, blocking websites, from your network.

Applications & Gaming

- Port Range Forwarding. You can set up public services or other specialized Internet applications on your network from this screen.
- Port Triggering. Set up triggered ranges and forwarded ranges for Internet applications from this screen.
- UPnP Forwarding. Use this screen to alter UPnP forwarding settings.
- DMZ. To allow one local user to be exposed to the Internet for use of special-purpose services, use this screen.

Administration

- Management. On this screen, alter the Router's password, access privileges, and UPnP settings.
- Log. You can view or save, even email, activity logs from this screen.
- Diagnostics. From this screen, you can test network performance and connections.
- Factory Defaults. If you want to restore the Router's factory defaults, then use this screen.
- Firmware Upgrade. From this screen, you can upgrade the Router's firmware.

upgrade*: to* replace existing software or firmware with a newer version

Status

- Gateway. This screen provides status information about the Router and your Internet connection.
- Local Network. This provides status information about the local network.

Accessing the Utility

To access the Web-based Utility of the Router, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Press the **Enter** key.

Figure 6-1: The Router's IP Address

A screen will appear asking you for your User name and Password. Leave the *User name* field blank, and enter **admin** in the *Password* field. Then click the **OK** button.

When finished making your changes on a screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

Figure 6-2: Router Login

The Setup tab

The *Setup* tab is the first tab you see when you access the Web-based Utility. This tab is divided into four screens: Basic Setup, DDNS, MAC Address Clone, and Advanced Routing. Each of these screens are described in detail below.

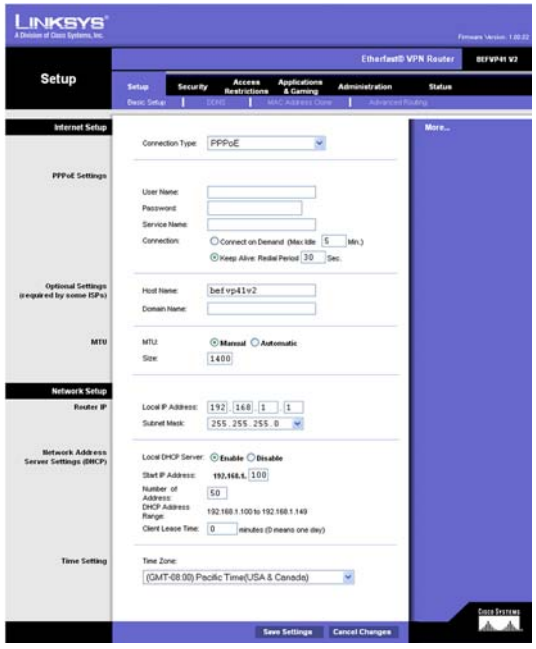

Figure 6-3: Setup tab - Basic Setup

Basic Setup

Internet Setup

This section allows you to select the type of Internet setup and connection your network employs. The Router supports six connection types: Obtain an IP automatically (DHCP), Static IP, PPPoE, RAS, PPTP, and Heart Beat Signal. Each *Basic Setup* screen and available features will differ depending on what kind of connection type you select.

Connection Type: Obtain an IP automatically - DHCP

By default, the Router's Internet Connection Type is set to **Obtain an IP automatically** and it should be used only if your ISP supports DHCP.

Host Name/Domain Name. Enter a Host Name and Domain Name if required by your ISP.

MTU. The MTU option specifies the largest packet size permitted for network transmission. Select **Manual** if you do not want the Router to regulate this packet size (otherwise, leave it set at **Automatic**) and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use the default of 1400.

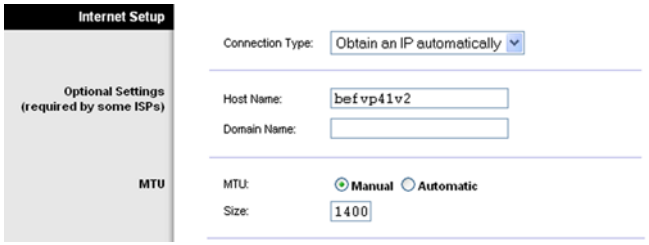

Figure 6-4: DHCP Connection type

Connection Type: Static IP

Note: For DSL users, if you need to enable PPPoE support, remember to remove any PPPoE applications that are installed on your PCs.

If you are required to use a permanent IP address, then select **Static IP**. This information can be obtained from your ISP.

IP Address. This is the IP address that the Router has, when 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. Your ISP will provide you with the Default Gateway Address.

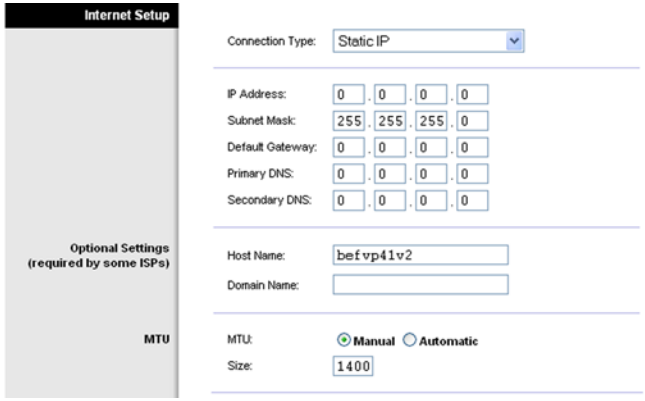

Figure 6-5: Static IP Connection type

***subnet mask**: an address code that determines the size of the network*

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

Host Name/Domain Name. Enter a Host Name and Domain Name if required by your ISP.

MTU. The MTU option specifies the largest packet size permitted for network transmission. Select **Manual** if you do not want the Router to regulate this packet size (otherwise, leave it set at **Automatic**) and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use the default of 1400.

Connection Type: PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable it.

User Name and Password. Enter the User Name and Password provided by your ISP.

Service Name. If provided by your ISP, enter the Service Name.

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.* The default Redial Period is 30 seconds.

Host Name/Domain Name. Enter a Host Name and Domain Name if required by your ISP.

MTU. The MTU option specifies the largest packet size permitted for network transmission. Select **Manual** if you do not want the Router to regulate this packet size (otherwise, leave it set at **Automatic**) and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use the default of 1400.

When you are finished, click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button to start the connection.

Figure 6-6: PPPoE Connection type

Connection Type: RAS (for SingTel)

Remote Access Service (RAS) is a service that applies to connections in Singapore only. For users in Singapore, check with Singtel for information on RAS.

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

Host Name/Domain Name. Enter a Host Name and Domain Name if required by your ISP.

MTU. The MTU option specifies the largest packet size permitted for network transmission. Select **Manual** if you do not want the Router to regulate this packet size (otherwise, leave it set at **Automatic**) and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use the default of 1400.

When you are finished, click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button to start the connection.

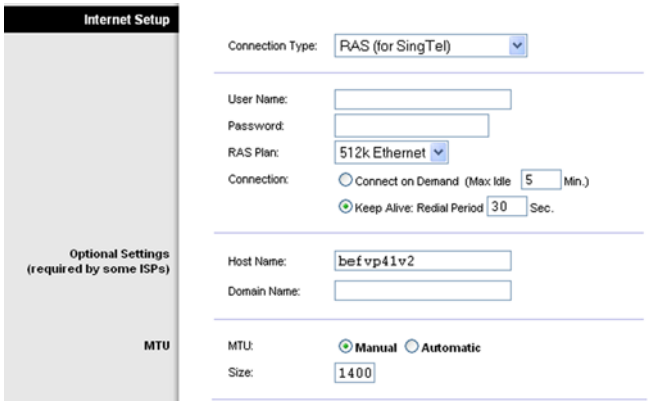

Figure 6-7: RAS Connection type

Connection Type: PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe and Israel only.

IP Address. This is the IP address that the Router has, when 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. Your ISP will provide you with the Default Gateway Address.

User Name and Password. Enter the User Name and Password provided by your ISP.

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

Host Name/Domain Name. Enter a Host Name and Domain Name if required by your ISP.

MTU. The MTU option specifies the largest packet size permitted for network transmission. Select **Manual** if you do not want the Router to regulate this packet size (otherwise, leave it set at **Automatic**) and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use the default of 1400.

When you are finished, click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button to start the connection.

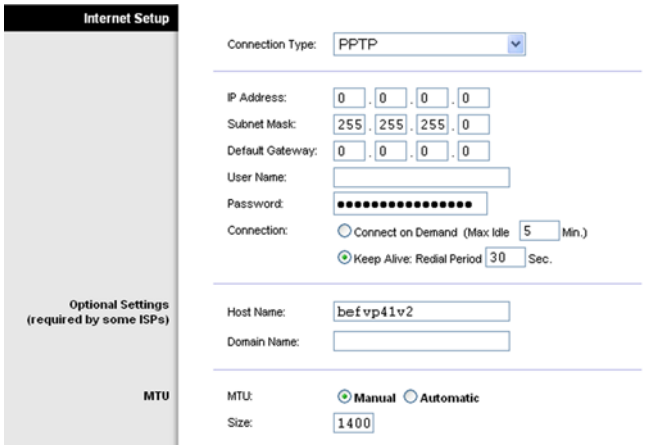

Figure 6-8: PPTP Connection type

Connection Type: Heart Beat Signal

Heart Beat Signal is a service used in Australia only. If you are using a Heart Beat Signal connection, check with your ISP for the necessary setup information.

User Name and Password. Enter the User Name and Password provided by your ISP.

Heart Beat Server. This is the IP address that the Router has, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

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.* The default Redial Period is 30 seconds.

Host Name/Domain Name. Enter a Host Name and Domain Name if required by your ISP.

MTU. The MTU option specifies the largest packet size permitted for network transmission. Select **Manual** if you do not want the Router to regulate this packet size (otherwise, leave it set at **Automatic**) and enter the value desired. You should leave this value in the 1200 to 1500 range. Most DSL users should use the default of 1400.

When you are finished, click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button to start the connection.

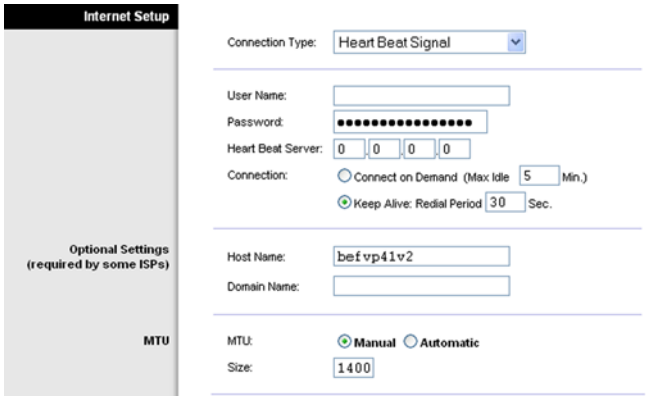

Figure 6-9: Heart Beat Signal Connection type

***server**: any computer whose function in a network is to provide user access to files, printing, communications, and other services*

Network Setup

Router IP

The values for the Router's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.

Local IP Address. The default value is **192.168.1.1**.

Subnet Mask. The default value is **255.255.255.0**.

Network Address Server Settings (DHCP)

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each PC on your network for you. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**. If you disable DHCP, remember to assign a static IP address to the Router.

Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Router is 192.168.1.1.

Number of Address (Optional). Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users. By default, add 100 to 50, and the range is 192.168.1.100 to 192.168.1.149.

DHCP Address Range. The range of DHCP addresses is displayed here.

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.

Time Setting

For an accurate keeping in the Router's logs and functions, select your local time zone from the drop-down menu.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

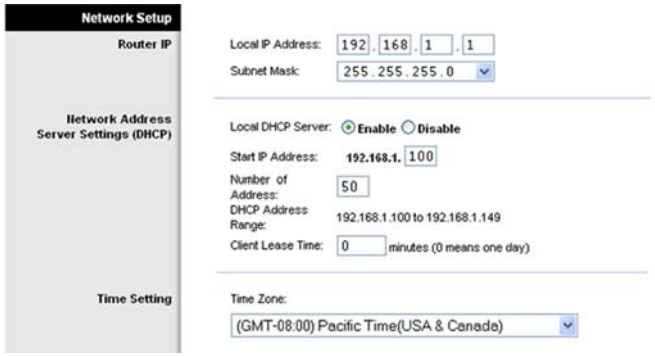

Figure 6-10: Network Setup

***Dynamic IP address**: a temporary IP address assigned by a DHCP server*

DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

Before you can use this feature, you need to sign up for DDNS service the DDNS service currently incorporated, DynDNS.org. If you do not want to use this feature, keep the default setting, **Disable**.

DDNS Service. To enable this function, select **DynDNS.org** from the drop-down menu. If you do not want to use this feature, keep the default setting, **Disable**.

User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.

Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, it will change.

Status. The status of the DDNS service connection is displayed here.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

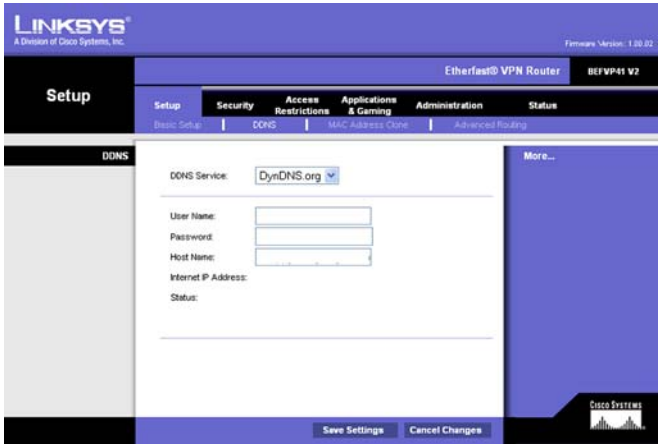

Figure 6-11: Setup tab - DDNS

ddns: *allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address*

MAC Address Clone

The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. If your ISP requires MAC address registration, find your adapter's MAC address by following the instructions in "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

MAC Clone Service. To use MAC address cloning, select **Enable**.

MAC Address. To manually clone a MAC address, enter the 12 digits of your adapter's MAC address in the on-screen fields. Then click the **Save Settings** button.

Clone. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click the **Clone** button. The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the *MAC Address Clone* screen.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

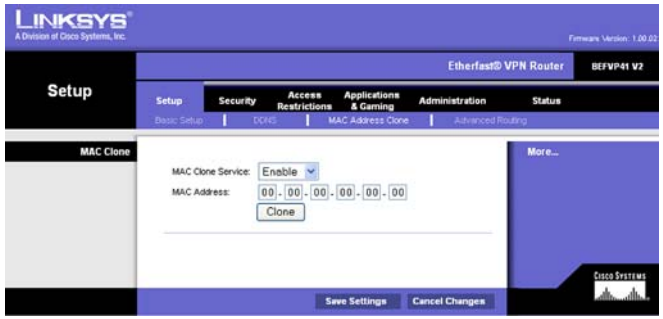

Figure 6-12: Setup tab - MAC Address Clone

Advanced Routing

The *Advanced Routing* screen allows you to configure the Network Address Translation (NAT), dynamic routing, and static routing settings.

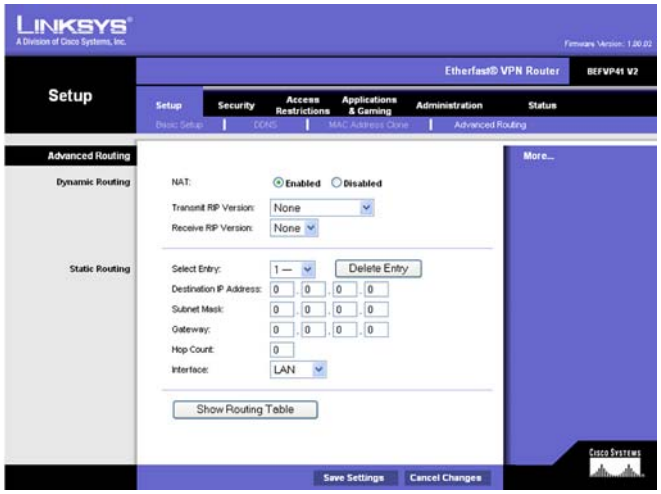

Figure 6-13: Setup tab - Advanced Routing

Dynamic Routing

NAT. NAT is a security feature that is enabled by default. It enables the Router to translate IP addresses of your local area network to a different IP address for the Internet. To disable NAT, click the **Disable** radio button. (When NAT is disabled, the DHCP server feature is also disabled.)

With Dynamic Routing you can enable the Router to 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.

Transmit RIP Version. To use dynamic routing for transmission of network data select the protocol you want: **RIP1**, **RIP1-Compatible**, or **RIP2**.

Receive RIP Version. To use dynamic routing for reception of network data, select the protocol you want: **RIP1** or **RIP2**.

Static Routing.

static routing: *Forwarding data in a network via a fixed path*

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, alter the following settings:

Select Entry. Select the number of the static route from the drop-down menu. The Router supports up to 20 static route entries.

Delete Entry. If you need to delete a route, select its number from the drop-down menu, and click the **Delete Entry** button.

Destination IP Address. The Destination IP Address 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. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit 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.

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

Gateway. 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.

Hop Count. This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as PCs, print servers, routers, etc.

Interface. Select **LAN** or **Internet**, depending on the location of the static route's final destination.

Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your network. For each route, the Destination LAN IP address, Subnet Mask, Default Gateway, Hop Count, and Interface are displayed. Click the **Refresh** button to update the information.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

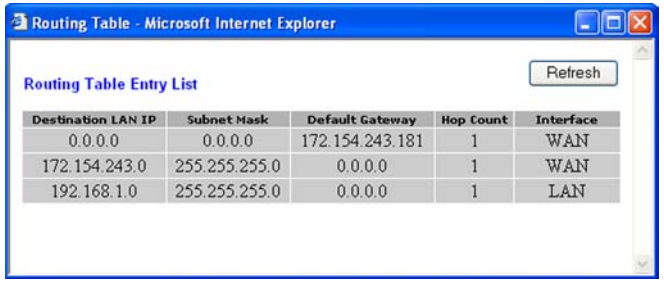

Figure 6-14: The Routing Table

gateway: *a device that interconnects networks with different, incompatible communications protocols*

The Security tab

The *Security* tab is the second tab listed atop the Web-based Utility. This tab is divided into two screens: Firewall and VPN. Each of these screens is described in detail below.

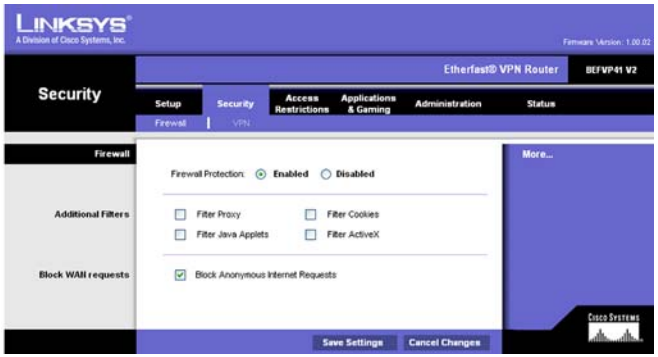

Figure 6-15: Security tab -Firewall

multicasting: *sending data to a group of destinations at once*

Firewall

When you click Security, you will see the *Firewall* screen. This allows you to **Enable** or **Disable** the firewall, which shields your network from outside users, and manage different filters, which provide additional protection. Filters block specific internal users from accessing the Internet and block anonymous Internet requests and/or multicasting.

Additional Filters

This area allows you to block, or filter, certain Internet applications from your network. Click the box next to those applications you wish to filter.

Block WAN Requests

Block Anonymous Internet Requests. This keeps your network from being "pinged" or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to work their way into your network. Click the box beside this option to enable it.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

VPN

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 tab allows you to configure your VPN settings to make your network more secure.

VPN Passthrough

IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enabled** button. To disable IPSec Passthrough, click the **Disabled** button.

PPTP Pass Through. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows 2000 server. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

VPN Tunnel

Establishing a Tunnel

The 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 50 simultaneous tunnels. To delete a tunnel, click the **Delete** button. To view a summary of that tunnel, click the **Summary** button.

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

A Local Secure Group is a computer(s) on your network that can access the tunnel. A Remote Secure Group is a 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.

Subnet. If you select Subnet (which is also the default), this will allow all computers on the local subnet to access the tunnel. When using the Subnet setting, the default values of 0 should remain in the last fields of the IP and Mask settings.

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.

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.

The next to options are for Remote Secure Groups only.

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.

Figure 6-16: Security tab - VPN

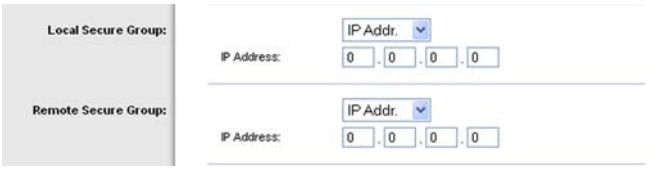

Figure 6-17: Local and Remote Secure Group

Any. If you select Any for the Remote Security Group, the local VPN Router will accept a request from any IP address. This setting should be chosen when the other endpoint is using DHCP or PPPoE on the Internet side.

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. In this section, you can also set the levels and types of encryption and authentication.

Figure 6-18: Remote Security Gateway

IP Address. If you select IP Address, 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.

FQDN (Fully Qualified Domain Name). If you select FQDN, 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.

Any. If you select Any for the Remote Security Gateway, 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 6-19: Key Management

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.

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.

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 the word **chappy** 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.

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. 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. That is, the Inbound SPI and Outbound SPI values would be opposite on the other end of the tunnel. Only numbers can be used in these fields. After you click the **Save Settings** button, hexadecimal characters (series of letters and numbers) are displayed in the Inbound SPI and Outbound SPI fields.

The *Status* field at the bottom of the screen will show when a tunnel is active.

To connect a VPN tunnel, click the **Connect** button. The **View Logs** button, when logging is enabled on the Log screen of the Administration tab, will show you VPN activity on a separate screen. The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used. For more advanced VPN options, click the **Advanced Setting** button to open the Advanced Setting screen.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Advanced VPN Tunnel Setup

From the Advanced Settings screen you can adjust the settings for specific VPN tunnels.

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. If a user on one side of the tunnel is using a Unique Firewall Identifier, this should be entered under the **Username** field.

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.

Figure 6-20: Advanced VPN Tunnel Setup

bit: *a binary digit*

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).

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The Access Restrictions tab

The Access Restrictions tab allows you to block or allow network access as well as manage specific kinds of Internet usage.

Internet Access

Internet Access Policy. Access is managed by a policy. An access policy is established with the settings on this screen (after **Save Settings** is clicked). Selecting a policy from the drop-down menu will display that policy's settings on this screen. To delete a policy, select that policy's number and click the **Delete** button. To view the policies established, click the **View Summary** button. (Policies can be deleted from the summary screen by selecting the policy or policies and clicking the **Delete** button.)

Enter Policy Name. Each policy can be named, using no more than 30 characters, so you can remember what it's for.

PCs. Click the Edit List of PCs button to select which PCs will be affected by the policy. You can enter the PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you wish this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Days/Times. When will this policy be in effect? On every day? At certain times? Select if you wish to Allow or Deny access during the times in this section. Select the individual days or select **Everyday**. Select **24 Hours** or enter a range of hours in which the policy will be in effect.

Blocked Services. To block specific port services, such as POP3, SNMP, etc., select the service you wish to block from the pull-down menu and enter a range of ports in the fields beside it. If the service is not listed, you can add or even edit a service by clicking the Add/Edit Service button.

Website Blocking by URL Address. Enter the URL of any website you wish to block in these fields.

Website Blocking by Keyword. If you don't know the address of the website you wish to block, you can enter keywords specific to the site in these fields. The Router will block access to sites that use those keywords.

When finished making your changes on this screen, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

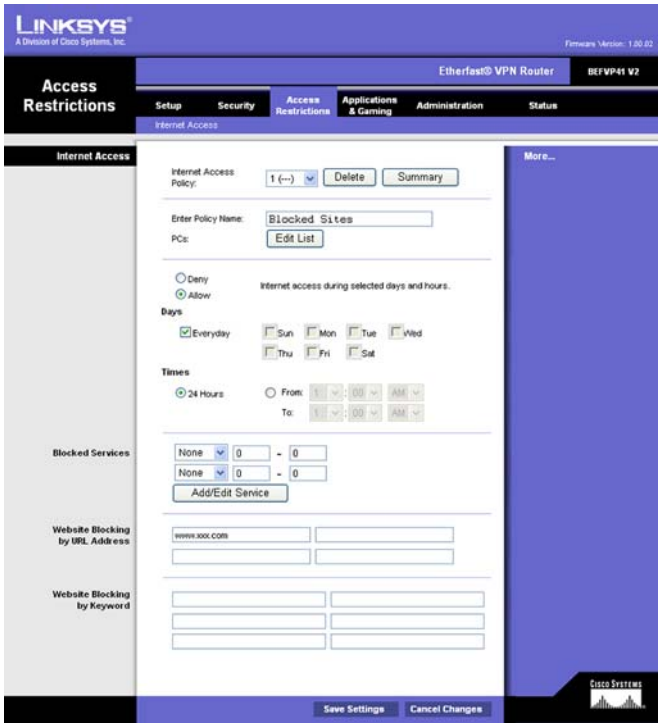

Figure 6-21: Access Restrictions tab

***pop3(Post Office Protocol 3)**: a standard mail server commonly used on the Internet*

***url (Uniform Resource Locator)**: the address of a file located on the Internet*

The Applications & Gaming tab

The Applications & Gaming tab allows you to manage ports that are used for various applications and gaming over the Internet.

Port Range Forwarding

When you click the Applications & Gaming tab, you will see the *Port Range Forwarding* screen. Port Range Forwarding sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) 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 should assign a static IP address to the designated PC.

If you need to forward all ports to one PC, click the **DMZ** tab.

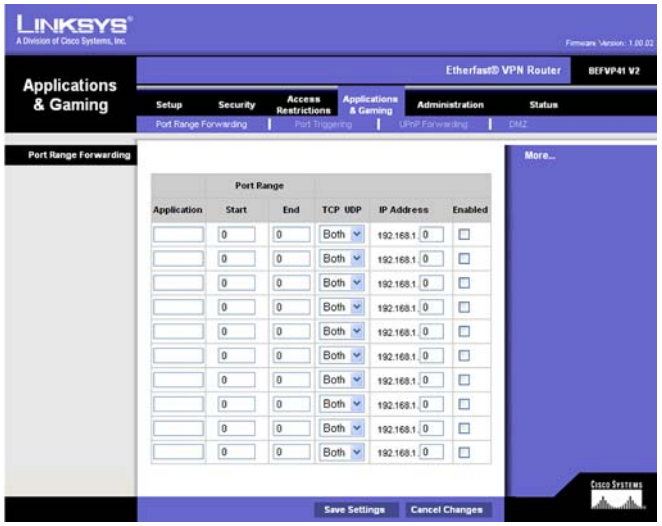

Figure 6-22: Applications & Gaming tab - Port Range Forwarding

To add a server using Port Range Forwarding, complete the following fields:

Application. Enter the name of the application.

Start and End. Enter the number or range of external port(s) used by the server or Internet application. Check with the Internet application software documentation for more information.

Protocol. Select the protocol **TCP** or **UDP**, or select **Both**.

IP Address. Enter the IP address of the server that you want the Internet users to be able to access. To find the IP address, go to "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

Enabled. Check the **Enabled** box to enable the services you have defined. Port Range Forwarding will not function if the Enabled button is left unchecked. This is disabled (unchecked) by default.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

***tcp** (**T**ransmission **C**ontrol **P**rotocol): a network protocol for transmitting data that requires acknowledgement from the recipient of data sent*

***udp** (**U**ser **D**atagram **P**rotocol): a nnetwork protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent*

Port Triggering

The *Port Triggering* screen 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 Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

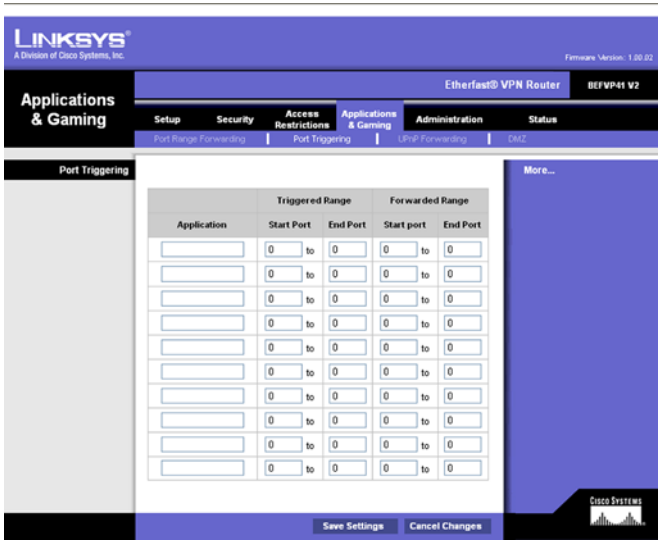

Figure 6-23: Applications & Gaming tab - Port Triggering

Port Triggering

Application. Enter the application name of the trigger.

Triggered Range

For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port. Enter the starting port number of the Triggered Range.

End Port. Enter the ending port number of the Triggered Range.

Forwarded Range

For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port. Enter the starting port number of the Forwarded Range.

End Port. Enter the ending port number of the Forwarded Range.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

UPnP Forwarding

The *UPnP Forwarding* screen displays preset application settings as well as options to customize port services for other applications.

UPnP Forwarding

Application. This provides ten preset applications. You can specify up to five additional applications in the available fields.

The preset applications are among the most widely used Internet applications. They include the following:

FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

SMTP (Simple Mail Transfer Protocol). 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.

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

TFTP (Trivial File Transfer Protocol). A version of the TCP/IP FTP protocol that has no directory or password capability.

Finger. A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being "fingered" must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

HTTP (HyperText Transport Protocol). 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 web browser.

POP3 (Post Office Protocol 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.

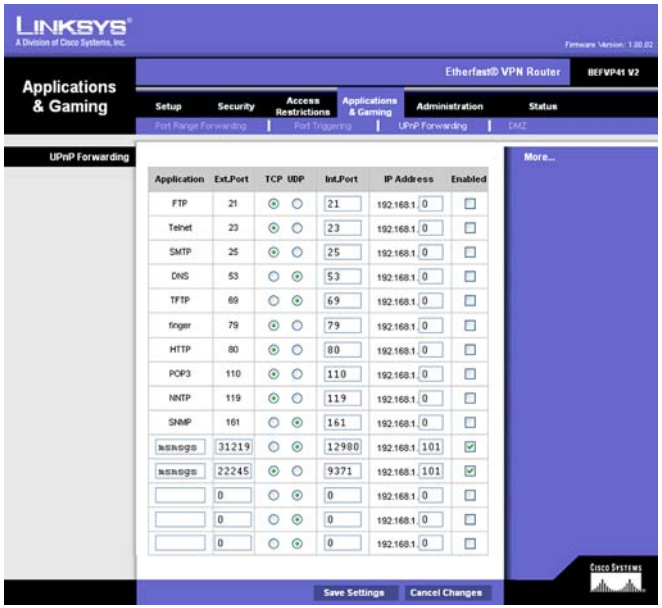

Figure 6-24: Applications & Gaming tab - UPnP Forwarding

***smtp** (**S**imple **M**ail **T**ransfer **P**rotocol): the standard e-mail*

***tftp** (**T**rivial **F**ile **T**ransfer **P**rotocol): a version of the TCP/IP FTP protocol that has no directory or password capability*

***finger:** aprogram that tells you the name associated with an e-mail address*

***http** (**H**yper**T**ext **T**ransport **P**rotocol): the communications protocol used to connect to servers on the World Wide Web*

***download:** to receive a file transmitted over a network*

NNTP (Network News Transfer Protocol). The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

nntp (Network News Transfer Protocol): The protocol used to connect to Usenet groups on the Internet

SNMP (Simple Network Management Protocol). 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.).

Ext. Port. Enter the number of the external port used by the server in the *Ext. Port* column. Check with the Internet application documentation for more information.

TCP or UDP. Select the protocol **UDP** or **TCP** for each application. You cannot select both protocols.

Int. Port. Enter the number of the internal port used by the server in the *Int. Port* column. Check with the Internet application software documentation for more information.

IP Address. Enter the IP address of the server that you want the Internet users to be able to access. To find the IP address, go to "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

Enabled. Check the **Enabled** box to enable the service you have defined. UPnP Forwarding will not function if the Enabled button is left unchecked. This is disabled (unchecked) by default.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

DMZ

The *DMZ* screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.

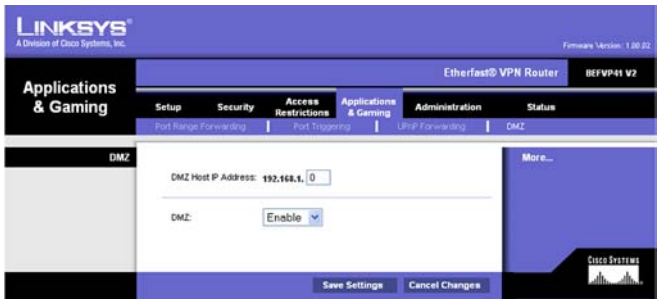

Figure 6-25: Applications & Gaming tab - DMZ

DMZ

DMZ. To use this feature, select **Enable**. To disable DMZ hosting, select **Disable**.

DMZ Host IP Address. To expose one PC, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter." Deactivate DMZ by entering a **0** in the field.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

dmz (Demilitarized Zone): *removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet*

The Administration tab

Management

When you click the Administration tab, you will see the *Management* screen. This screen allows you to change the Router's access settings as well as configure the UPnP (Universal Plug and Play) features.

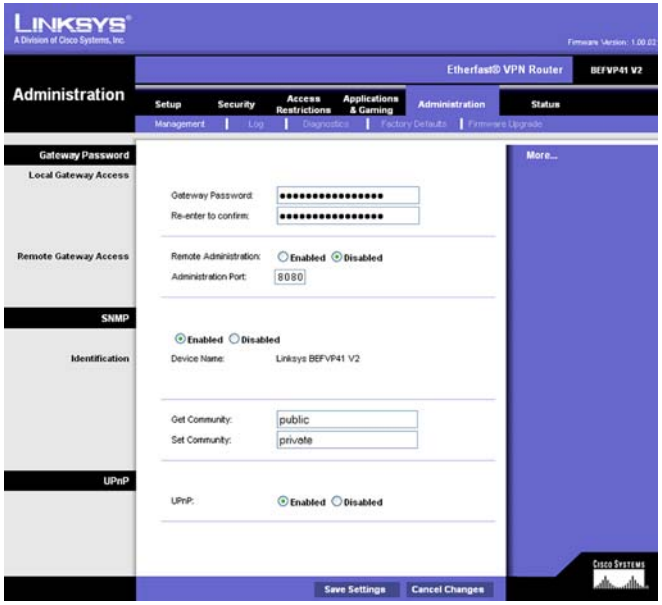

Figure 6-26: Administration tab - Management

Gateway Password

Local Gateway Access

To ensure the Router's security, you will be asked for your password when you access the Router's Web-based Utility. The default password is **admin**.

Gateway Password. It is recommended that you change the default password to one of your choice.

Re-enter to confirm. Re-enter the Router's new Password to confirm it.

Remote Gateway Access

This feature allows you to access the Router from a remote location, via the Internet.

Remote Administration. This feature allows you to manage the Router from a remote location, via the Internet. To enable Remote Administration, click the **Enabled** radio button.

Administration Port. Enter the port number you will use to remotely access the Router.

SNMP

The Router supports Simple Network Management Protocol (SNMP), which is a widely used network monitoring and control protocol. This allows network supervisors to monitor the Router using network management systems such as HP OpenView.

Enabled/Disabled. To use SNMP, select **Enabled**. If you do not want to use SNMP, keep the default, **Disabled**.

Get Community. Enter the password that allows read-only access to the Router's SNMP information.

Set Community. Enter the password that allows read/write access to the Router's SNMP information.

UPnP

UPnP allows Windows XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. Select the radio button beside **Enable** or **Disable**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Log

The *Log* screen provides you with options for email alerts and a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Email alerts. To enable the Router to send email alerts in the event of Denial of Service attacks and the like, click the radio button beside **Enable**. If you do not wish to have email alerts, click the radio button beside **Disable**.

Denial of Service Thresholds. This limit, from 20 to 100, is the amount of Denial of Service (DOS) attacks the Router detects before sending an email alert.

SMTP Mail Server. This is the IP Address or full mail server name (e.g. mail.domain.com) of your mail server.

Email address for alert logs. This is the email address where you would like the email alerts sent.

Return email address. Your mail server may require a return email address. Enter that here. If you're unsure as to what address to enter, enter the same email address for *Email address for alert logs*.

Log. To access activity logs, select the **Yes** radio button. With logging enabled, you can choose to view temporary logs (by clicking the **View Logs** button on the *VPN* screen under the *Security* tab) or keep a permanent record using the Logviewer software. Click the **No** button to disable this function.

Logviewer IP Address. For a permanent record of these logs, Logviewer software must be used. This software is downloadable from the Linksys website, *www.linksys.com*. The Logviewer saves all incoming and outgoing activity in a permanent file on your PC's hard drive. In the *Logviewer IP Address* field, enter the fixed IP address of the PC running the Logviewer software. The Router will now send updated logs to that PC.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

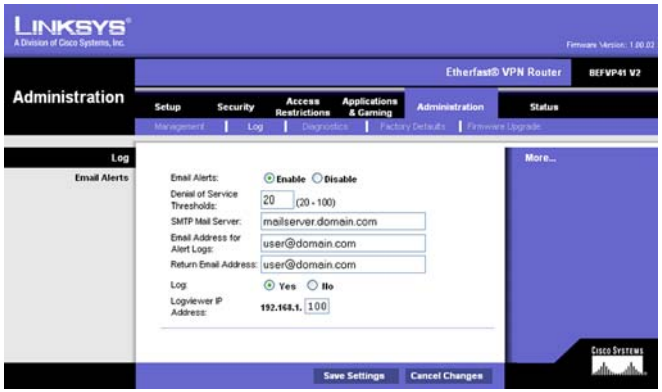

Figure 6-27: Administration tab - Log

Diagnostics

Diagnostics allow you to check the connections of your network components as well as locations outside your network via the Internet.

Ping Target IP. This is the IP Address of the PC or network component, or location outside of your network, that you wish to test.

Ping Size. Enter the amount of data, measured in bytes, sent in the ping test here. This number can be between **60** and **1514** bytes, more data being sent with a higher number.

No. of Pings. How many times in this test do you want the Router to ping the location? This number can be between **1** and **4** and should be entered here.

Ping Interval. How long, in milliseconds, would you like the Router to wait between pings? This number can be between **0** and **9999** milliseconds.

Ping Timeout. How long should the Router wait before it times out after an unsuccessful test? An unsuccessful test is determined when a location does not respond to a ping. This number can be between **0** and **9999** milliseconds.

Start Test. Click the **Start Test** button to begin the diagnostic tests.

The results of the test will be listed below the Start Test button.

When you are finished running your tests, click the **Save Settings** button to save these settings for future tests, or click the **Cancel Changes** button to return the settings to their previous state.

Figure 6-28: Administration tab - Diagnostics

***ping** (**P**acket **IN**ternet **G**roper): an Internet utility used to determine whether a particular IP address is online*

Factory Defaults

The *Factory Defaults* screen allows you to restore the Router's configuration to its factory default settings.

Restore Factory Defaults. To clear all of the Router's settings and reset them to its factory defaults, click the **Yes** radio button.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Note: 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 settings.

Figure 6-29: Administration tab - Factory Defaults

Firmware Upgrade

The *Firmware Upgrade* screen allows you to upgrade the Router's firmware.

Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, *www.linksys.com*. Then extract the file.

File Path. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Upgrade. After you have selected the appropriate file, click the **Upgrade** button (located at the bottom of the screen), and follow the on-screen instructions.

Note: If you upgrade the Router's firmware, you may lose its configuration settings.

Figure 6-30: Administration tab - Firmware Upgrade

The Status tab

When you click the Status tab, you will see the *Gateway* screen. It displays information about the Router and its settings.

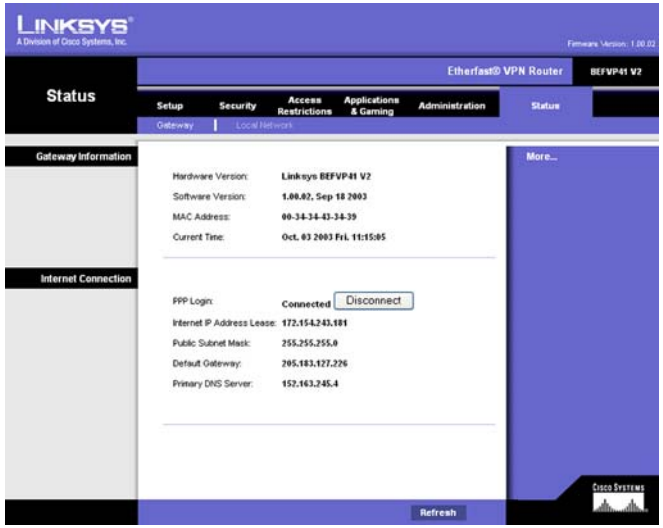

Figure 6-31: Status tab - Gateway

Gateway

Gateway Information

Hardware Version. This displays the Router's model number.

Software Version. This shows the installed version and date of the Router's firmware.

MAC Address. The MAC Address of the Router's Internet interface is displayed here.

Current Time. As selected from the Setup tab, this will show the proper time in your time zone.

Internet Connection

PPP Login. The status of your Internet connection is displayed here.

Internet IP Address Lease. Your current IP address is shown here.

Subnet Mask and Default Gateway. The Router's Subnet Mask and Default Gateway addresses are displayed here for DHCP and static IP connections.

Primary DNS Server. Shown here is the Primary DNS (Domain Name System) IP address currently used by the Router.

Click the **Refresh** button to update the on-screen information.

Local Network

The *Local Network* screen displays information about the local network.

Local MAC Address. The MAC Address of the Router's LAN (local area network) interface is displayed here.

IP Address. The Router's local IP Address is shown here.

Subnet Mask. The Router's Subnet Mask is shown here.

DHCP Server. If the Router is being utilized as a DHCP server will be displayed here.

DHCP Client Table. Click the **DHCP Clients Table** button to view a list of PCs that have been assigned IP addresses by the Router. The *DHCP Active IP Table* screen lists the DHCP Server IP Address, Client Hostnames, IP Addresses, and MAC Addresses. To delete a DHCP Client, select the box beside their information and click the **Delete** button. Click the **Refresh** button to update the information.

Click the **Refresh** button to update the on-screen information.

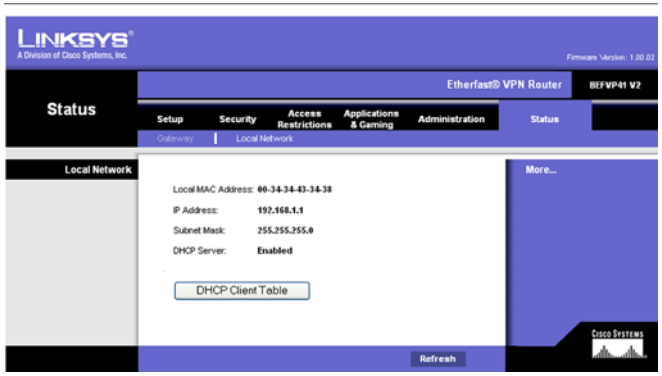

Figure 6-32: Status tab - Local Network

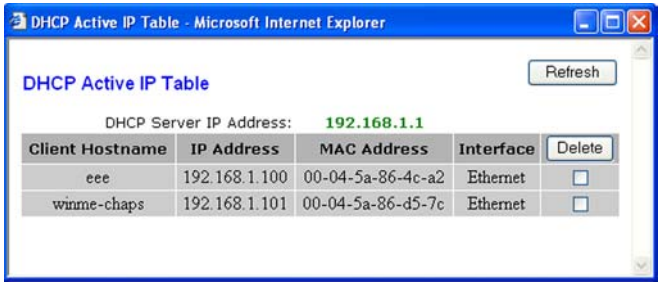

Figure 6-33: DHCP Active IP Table

Appendix A: Troubleshooting

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.

Common Problems and Solutions

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 98 and Me:

   A. Click **Start**, **Settings**, and open the **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 open the **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 for this 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.

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 select the **Control Panel**.
B. Click the **Network and Internet Connections** icon and then select 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).
J. 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 for this information.
H. 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. If you do not know how to do this, refer to Appendix D: Windows Help.

B. Open a command prompt.
- For Windows 98 and Me, click **Start** and select **Run**. In the *Open* field, type **command**. Press the **Enter** key or click the **OK** button.
- For Windows 2000 and XP, click **Start** and select **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 Internet IP address and press the **Enter** key. The Internet IP Address can be found in the Router's Web-based Utility. For example, if your Internet 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 cannot get an Internet connection through the Router.

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 C: 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: Using the Router's Web-based Utility" for details.

C. Make sure you are using the right Internet settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: Using the Router's Web-based Utility" for details on Internet settings.

D. Make sure you have the right cable. Check to see if the Router's Internet LED is solid.

E. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet 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 C: 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: Using the Router's Web-based Utility" and go to the VPN screen on the Security 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 network PC's 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 Web-based Utility's Setup tab. 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. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Applications & Gaming** => **Port Range Forwarding** tab.
B. Enter any name you want to use for the Application.
C. Enter the 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. Select the protocol you will be using, **TCP** or **UDP**, or select **Both**.
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 C: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Check the **Enabled** option for the port services you want to use. Consider the example below:

Application	Start and End	Protocol	IP Address	Enabled
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	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. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Applications & Gaming** => **Port Range Forwarding** tab.
B. Enter any name you want to use for the Application.
C. Enter the 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. Select the protocol you will be using, **TCP** or **UDP**, or select **Both**.

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 C: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enabled** option for the port services you want to use. Consider the example below:

Application	Start and End	Protocol	IP Address	Enabled
UT	7777 to 27900	Both	192.168.1.100	X
Halflife	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** 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. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Applications & Gaming** => **Port Range Forwarding** 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** tab.
D. Enter the Ethernet adapter's IP address of the computer you want exposed to the Internet. This will bypass the NAT security for that computer. Please refer to "Appendix C: 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 **Save Settings** 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. Access the Router's web interface by going to **http://192.168.1.1** or the IP address of the Router. Enter the default password admin, and click the **Administration** => **Management** tab.
B. Enter a different password in the *Router Password* field, and enter the same password in the second field to confirm the password.

Click the **Save Settings** button.

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 network.

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.

Close all the windows to finish.

11. To start over, I need to 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.

To upgrade the firmware, follow the steps in the Upgrade section found in "Chapter 6: Using the Router's Web-based Utility" or "Appendix B: Upgrading Firmware."

13. The firmware upgrade failed.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware:

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 Firmware Upgrade screen of the Administration 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 browser, and enter **http://192.168.1.1** or the IP address of the Router.
B. Enter the password, if asked. (The default password is admin.)
C. On the *Basic Setup* tab, select the option **Keep Alive**, and set the *Redial Period* option at **20** (seconds).
D. Click the **Save Settings** button.
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.

If the connection is lost again, follow steps E and F 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 browser, and enter **http://192.168.1.1** or the IP address of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. On the *Basic Setup* tab, look for the MTU option, and select **Enable**. In the *Size* field, enter 1492.
D. Click the **Save Settings** button 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 browser, and enter **http://192.168.1.1** or the IP address of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Applications & Gaming** => **Port Triggering** tab.
D. Enter any name you want to use for the Application Name.
E. Enter the *Start* and *End* Ports of the Triggered Port Range. Check with your Internet application provider for more information on which outgoing port services it is using.

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

- 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.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the network and power connections.)
- 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.
- Manually configure the TCP/IP with a DNS address provided by your ISP.

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**.

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 (Simple Network Management Protocol) is a widely-used network monitoring and control protocol. For more information on SNMP, see "Appendix G: 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 network. 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 network to network connections, but those protocols cannot connect from the Internet to your local network.

***node**: a network junction or connection point, typically a computer or work station.*

Does the Router's Internet connection support 100 Mbps Ethernet?
Because of the speed limitations of broadband Internet connections, the Router's Internet 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 your local network 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 network 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 98, Windows 2000,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 network 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 network's 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 network 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.

mbps *(**M**ega**B**its **P**er **S**econd): one million bits per second; a unit of measurement for data transmission*

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 network 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 network (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, 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. 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 network adapter's IP address, see "Appendix C: 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.

buffer: *a shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other*

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.

mIRC: *an Internet Relay Chat program that runs under Windows*

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

Appendix B: Upgrading Firmware

You can use the Router's Web-based Utility to upgrade the firmware; however, if you do so, you may lose the settings you have configured on the Router.

To upgrade the Router's firmware, follow these instructions:

1. Download the Router's firmware upgrade file from the Linksys website, *www.linksys.com*.
2. Extract the file on your computer.
3. Click the **Administration** tab and then the **Firmware Upgrade** tab of the Router's Web-based Utility.
4. On the *Upgrade Firmware* screen, enter the location of the extracted firmware upgrade file, or click the **Browse** button to find this file.
5. Click the **Upgrade** button, and follow the on-screen instructions.

Figure B-1: Upgrade Firmware

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

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Router's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. Click **Start** and select **Run**. In the *Open* field, enter **winipcfg**. Then, press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Router via a CAT 5 Ethernet network cable.
3. Write down the Adapter Address as shown on your computer screen. This is the MAC address for your Ethernet adapter and is 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.

   The example shows the Ethernet adapter's IP address as **192.168.1.100**. Your computer may show something different.

4.

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

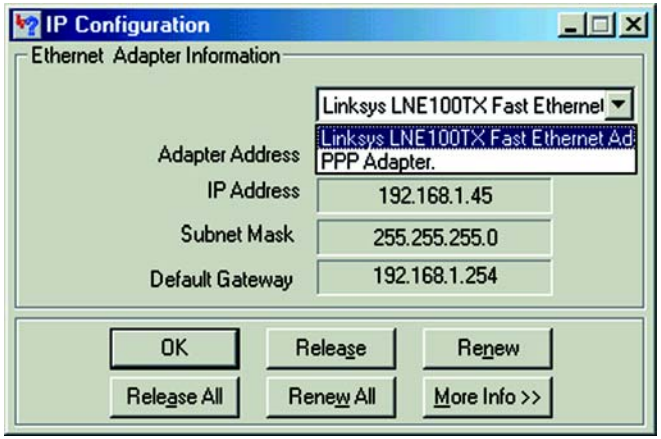

Figure C-1: IP Configuration Screen

Windows 2000 or XP Instructions

1. Click **Start** and select **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.
2. At the command prompt, enter **ipconfig /all**. Then, press the **Enter** key.

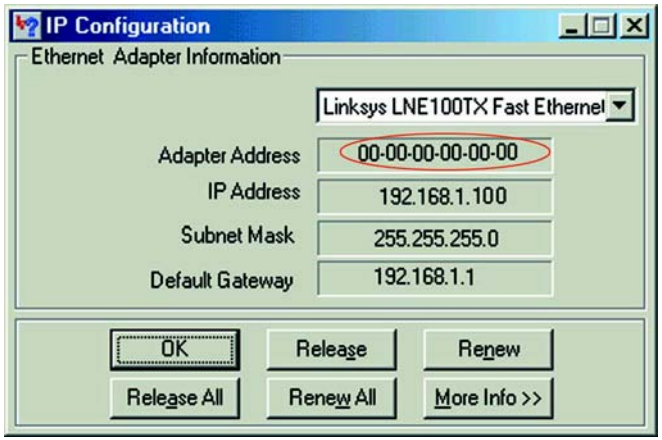

Figure C-2: MAC Address/Adapter Address

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

   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 shows the Ethernet adapter's IP address as **192.168.1.100**. Your computer may show something different.

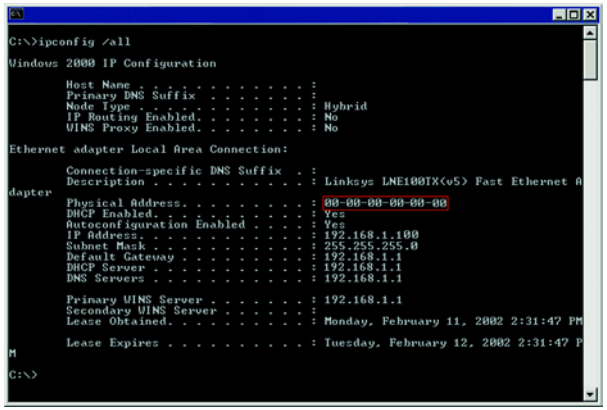

Figure C-3: MAC Address/Physical Address

For the Router's Web-based Utility

For MAC filtering, enter the 12-digit MAC address in this format, XXXXXXXXXXXX, WITHOUT the hyphens.

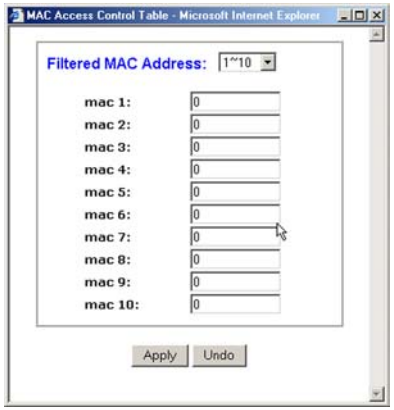

Figure C-4: MAC Address Filter

For MAC address cloning, enter the 12-digit MAC address in the *MAC Address* fields provided, two digits per field.

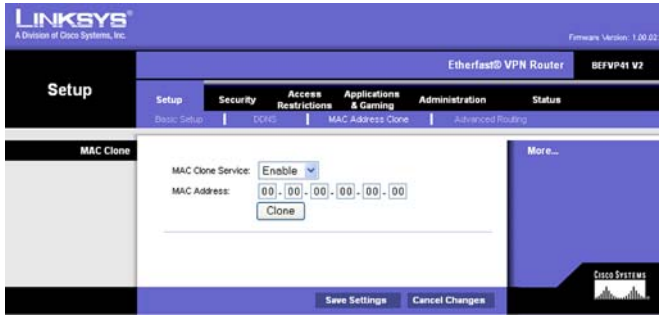

Figure C-5: MAC Address Clone

Appendix D: Windows Help

All networking products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with the Router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a wired or wireless network. Your PCs will not be able to utilize networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

tcp/ip *(**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol): a set of instructions PCs use to communicate over a network*

Shared Resources

If you wish to share printers, folders, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix E: 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.

throughput: *the amount of data moved successfully from one node to another in a given time period*

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 F: Creating a VPN Tunnel between two VPN Routers

NOTE: Further details on this step can be found in the VPN Tab section in "Chapter 6: Using the 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. Select the *Security* tab.
4. From the *Security* tab, select the **VPN** screen.
5. From the *VPN* screen, select **Enable** beside VPN Tunnel.
6. Enter a **Tunnel Name**. This name should be unique for this particular tunnel.
7. Select **Subnet** from the pull-down menu beside *Local Secure Group*. Then, enter the **IP Address** and **Subnet Mask** for this group. This would be your local network's IP Address scheme.
8. Select **IP Addr.** from the pull-down menu beside *Remote Secure Group*. Then, enter the **IP Address** and **Subnet Mask** for this group. This would be the IP Address scheme for the remote network, the network on the other side of the tunnel.
9. Select **IP Addr.** from the pull-down menu beside *Remote Security Gateway*. This would be the remote endpoint's IP Address as seen from the Internet. Enter this **IP Address** here.
10. Select a type of **Encryption** and **Authentication** for the tunnel your are establishing, making sure that both sides are identical.
11. Check **PFS** (Perfect Forward Secrecy) and enter the **Pre-Shared Key** and **Key Lifetime**.
12. Click the **Save Settings** button.

Figure F-1: The Web-based Utility's VPN screen

To test your connection, click the **Connect** button.

Your tunnel should now be established.

Appendix G: SNMP Functions

SNMP (Simple Network Management Protocol) 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 H: Glossary

Adapter - A device that adds network functionality to your PC.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that interconnects different networks together.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**D**emilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

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

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops networking standards.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

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

Packet - A unit of data sent over a network.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Router - A networking device that connects multiple networks together.

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.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that 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 network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

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 node to another in a given time period.

UDP (**U**ser **D**atagram **P**rotocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

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

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

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:	
Internet:	One 10Base-T RJ-45 Port
Local Network:	Four 10/100 RJ-45 Ports
Cabling Type:	
10BaseT:	UTP Category 3 or better
100BaseTX:	UTP Category 5 or better
Speed (Mbps):	Internet:10
	Local Network:10/100 (Half Duplex Mode)
	20/200 (Full Duplex Mode)
LEDs	Power, Ethernet (1-4), Internet
Topology:	Star

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

LIMITED WARRANTY

Linksys warrants to You that, for a period of one year (the “Warranty Period”), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the 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. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix K: Regulatory Information

FCC STATEMENT

This product 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

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that the Wireless-G ADSL Gateway conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.

EN 609 50 Safety

EN 300-328-1, EN 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys Group déclare la Passerelle ADSL sans fil-G est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

France:

2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le département. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

FCC PART 68 STATEMENT

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning. The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved. This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subject to state tariffs.

SAFETY NOTICES

Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.

Do not use this product near water, for example, in a wet basement or near a swimming pool.

Appendix L: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-261-8868
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-261-1288