

*Instant EtherFast® Series*

# USB VPN & Firewall Adapter



Use this guide to install:

USBVPN1

User Guide

 **LINKSYS®**

## COPYRIGHT & TRADEMARKS

Copyright © 2003 Linksys, All Rights Reserved. Linksys, EtherFast, and Instant Broadband are registered trademarks of Linksys. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. All other trademarks and brand names are the property of their respective proprietors.

## LIMITED WARRANTY

Linksys guarantees that every USB VPN & Firewall Adapter will be free from physical defects in material and workmanship for one year from the date of purchase, when used within the limits set forth in the Specifications section of this User Guide. If the product proves defective during this warranty period, call Linksys Technical Support in order to obtain a Return Authorization number. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. When returning a product, mark the Return Authorization number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. All customers located outside of the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS OFFERS NO REFUNDS FOR ITS PRODUCTS. Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

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

## FCC STATEMENT

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

UG-USBVPN1-022003NC-BW

# Table of Contents

Chapter 1: Introduction	1
The Linksys USB VPN & Firewall Adapter	1
Features	1
Chapter 2: Getting to Know the EtherFast Cable/DSL Firewall Router	2
The Adapter's Front Panel	2
The Adapter's Ports and Reset Button	3
The Adapter's LEDs	4
Chapter 3: Connect the USB VPN & Firewall Adapter	6
Overview	6
Connecting Your Hardware Together and Booting Up	7
Chapter 4: Install the Driver for the Adapter	8
Overview	8
Driver Installation for Windows XP	8
Driver Installation for Windows 2000	11
Driver Installation for Windows Me	15
Driver Installation for Windows 98SE	16
Chapter 5: Configure TCP/IP	20
Overview	20
Configuring Windows XP	21
Configuring Windows 2000 PCs	23
Configuring Windows 98 and Me PCs	25
Chapter 6: Configure the Adapter	27

# Chapter 1: Introduction

## The Linksys USB VPN & Firewall Adapter

Let the Linksys USB VPN and Firewall Adapter protect your PC and your communications wherever you go. This easy-to-pack, lightweight, network interface with advanced safety and security features connects you to the Internet through any broadband connection (cable, DSL, or your hotel's fast Internet service), and protects your PC from most known Internet attacks with a powerful Stateful Packet Inspection firewall. You can also optionally block Java, Active X, and Cookies -- known points of entry for hackers.

The Adapter connects to virtually any PC through the USB port, and requires no external power supply. Once you're connected, you can establish a Virtual Private Network tunnel from your PC to a corporate network using the popular IPSec VPN standard, and your transmitted data will be protected by government-spec DES or Triple-DES encryption.

It's also a perfect traveling companion to the Linksys Firewall Router (BEFSX41) or VPN Router (BEFVP41) on your home or small office network. You can securely connect to your home resources to retrieve files, or check your local email. Once you're connected over VPN, it's just like being attached to the local network.

With the Linksys USB VPN and Firewall Adapter protecting your PC and communications, you'll have one less thing to worry about when you're traveling.

## Features

- A USB-attached network interface with firewall safety and a secure communication link
- Establishes an IPSec Virtual Private Network tunnel to your corporate network
- Advanced firewall with Stateful Packet Inspection protects your PC from Internet attacks, wherever you connect
- USB interface -- works with virtually any PC

Chapter 7: The USB VPN & Firewall Adapter's Web-based Utility	32
Overview	32
Quick and Easy Router Administration	32
Setup	33
Firewall	38
VPN	41
Password	54
Status	55
DHCP	57
Log	59
Help	60
Appendix A: Troubleshooting	62
Common Problems and Solutions	62
Frequently Asked Questions	68
Appendix B: Installing the TCP/IP Protocol	70
Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter	72
Appendix D: Glossary	76
Appendix E: Specifications	88
Environmental	88
Appendix F: Warranty Information	89
Appendix G: Contact Information	90

## Chapter 2: Getting to Know the USB & VPN Firewall Adapter

### The Adapter's Front Panel

The Adapter's ports and LEDs are shown in Figure 2-1. For details on the Reset Button and Ethernet port, see Figure 2-2. For details on the USB port, see Figure 2-3. For details on the LEDs, see Figure 2-4 and Figure 2-5.



Figure 2-1

### The Adapter's Ports and Reset Button

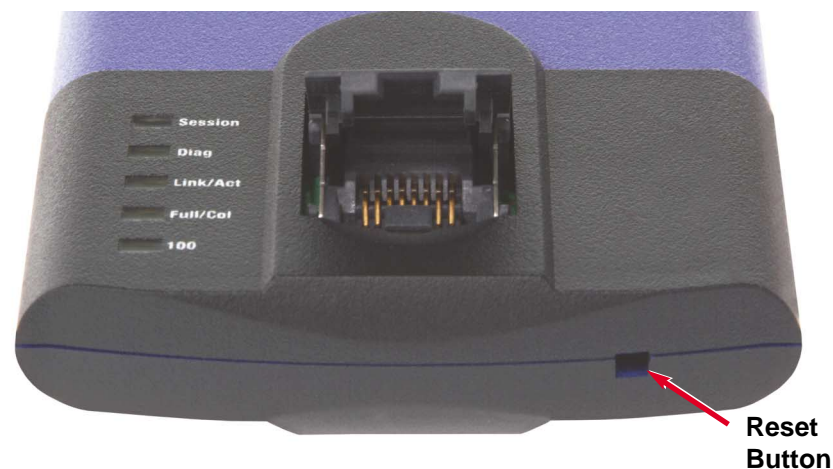


Figure 2-2

**Ethernet** The **Ethernet** port is where you connect the Ethernet cable to a Router or cable or DSL modem. (See Figure 2-2.)

#### The Reset Button

Briefly pressing the Reset Button (see Figure 2-2) will refresh the Adapter's connections, potentially clearing any jammed links.

Pressing the Reset Button and holding it in for a few seconds will clear all of the Adapter's data. This should be done only if you are experiencing heavy routing problems, and only after you have exhausted all of the other troubleshooting options. By resetting the Adapter, you run the risk of creating conflicts between your PC's actual IP Address and what the Adapter thinks its IP Address should be. You may be forced to reboot the entire system. Please restart your computer after resetting the Adapter.

If the Adapter locks up, simply power it down for three to five seconds by removing the USB cable from the Adapter's USB Port. Reconnect the USB cable to the Adapter's USB port and check your connection status again.



Figure 2-3

**USB** The **USB** port is where you connect the USB cable to the Adapter (See Figure 2-3.) from the USB cable that is connected to a USB port on your PC.

#### The Adapter's LEDs

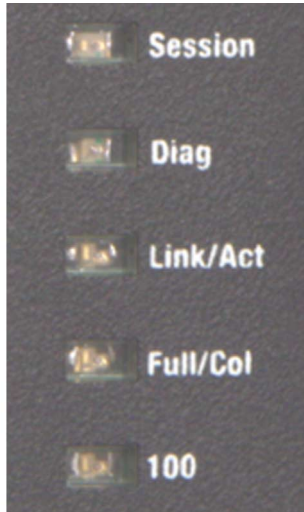


Figure 2-4

**Session** *Orange.* The **Session** LED indicates a successful VPN Tunnel has been established between two endpoints.

**Diag** *Red.* The **Diag** LED lights up when the Adapter goes through its self-diagnosis mode during every boot-up. It will turn off upon successful completion of the diagnosis.

**Link/Act** *Green.* The **Link/Act** LED serves two purposes. If the LED is continuously lit, the Adapter is successfully connected. If the LED is flickering, the Adapter is actively sending or receiving data.

**Full/Col** *Green.* The **Full/Col** LED also serves two purposes. If this LED is lit up continuously, the connection is running in Full Duplex mode. If the LED flickers, the connection is experiencing collisions.

If this LED flickers too often, there may be a problem with your connection. See “Appendix A: Troubleshooting” if you encounter this problem.

**100** *Orange.* The **100** LED lights up when a successful 100Mbps connection is made.

If this LED does not light up, then your connection speed is 10 Mbps.



Figure 2-5

**USB** *Green.* The **USB** LED lights up when the Adapter is connected to a PC and powered on. (See Figure 2-4.)

**Proceed to “Chapter 3: Connect the Adapter.”**

# Chapter 3: Connect the USB VPN & Firewall Adapter

## Overview

The Adapter's setup consists of more than simply plugging hardware together. You will have to configure your networked PC to accept the IP address that the Adapter assigns to your computer, and you will also have to configure the Adapter with setting(s) provided by your Internet Service Provider (ISP).

Contact your ISP for the correct settings if you do not have the information available.

Once you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Adapter.

The diagram in Figure 3-1 shows a typical configuration.

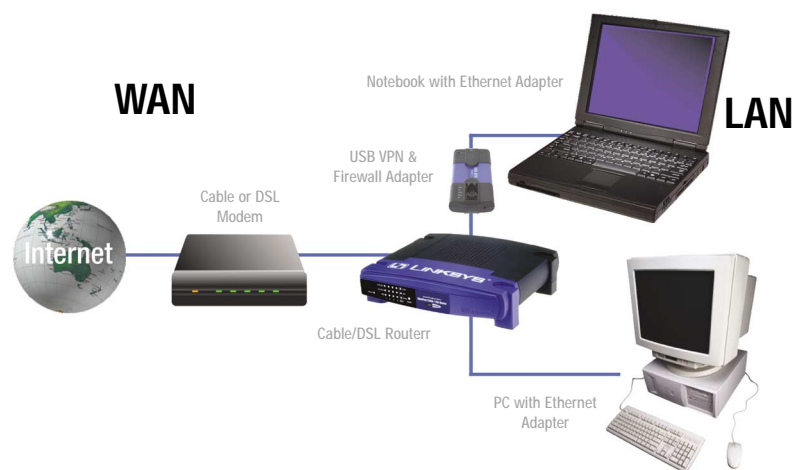


Figure 3-1

## Connecting Your Hardware Together and Booting Up

1. Before you begin, make sure that all of your hardware is powered off, including the Adapter, PCs, cable or DSL modem, and/or Router.
2. Connect one end of the USB cable to the USB port on the Adapter (see Figure 3-2) and the other end of the USB cable to a USB port on your PC (see Figure 3-3.)



Figure 3-2



Figure 3-3

3. Connect one end of an Ethernet cable to the Ethernet port on the Adapter, and the other end to an Ethernet port (LAN port) on a Router. If you are not using a Router, you can connect it directly to a cable or DSL modem.
- The **USB** LED will light up green as soon as the Adapter is connected correctly to the PC. (The LED is shown in Figure 2-5.)
  - The **Diag** LED will light up red for a few seconds when the Adapter goes through its self-diagnostic test. This LED will turn off when the self-test is complete. (The LEDs are shown in Figure 2-4.)
4. Turn on the PC, cable or DSL modem and/or Router.

**The Adapter's hardware installation is now complete.**

# Chapter 4: Install the Driver for the Adapter

## Overview

After connecting the USB VPN & Firewall Adapter to your computer, follow the instructions for your operating system to install the hardware device's driver. If at any time during the installation you encounter problems, consult the Troubleshooting section.



**Note:** Do not click **Cancel** at any time during the installation process or your driver will not install correctly on your PC.

## Driver Installation for Windows XP

1. If you haven't already, start your computer.
2. Windows XP will automatically detect the Adapter connected to your computer and display the *Welcome to the Found New Hardware Wizard* screen. Select **Install the software automatically (Recommended)**, and insert the Setup CD into the CD-ROM drive. Then click the **Next** button.

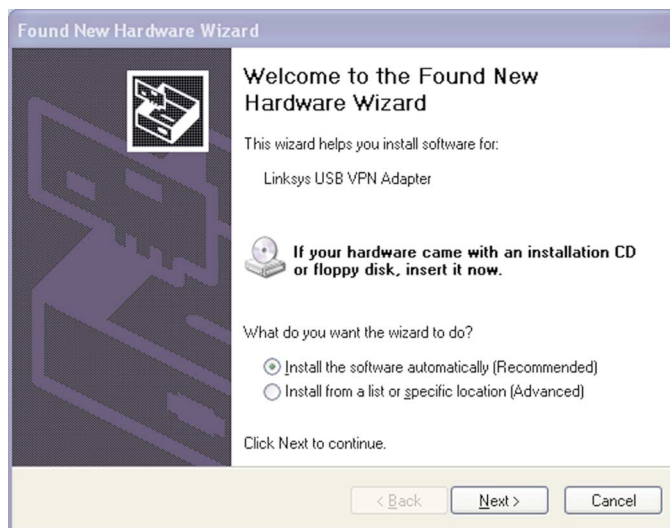


Figure 4-1

3. Windows may inform you that it is searching for the driver.

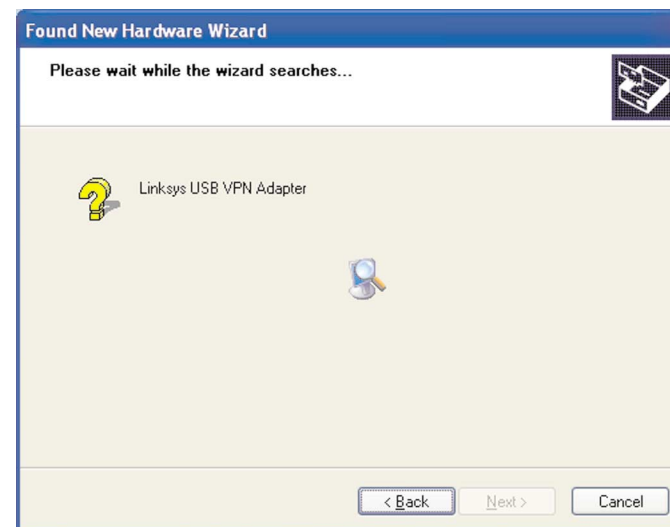


Figure 4-2

4. Then, it will notify you that the driver has not passed Windows Logo testing. This is normal, and it has been verified that the Adapter does work with Windows XP. Click the **Continue Anyway** button.

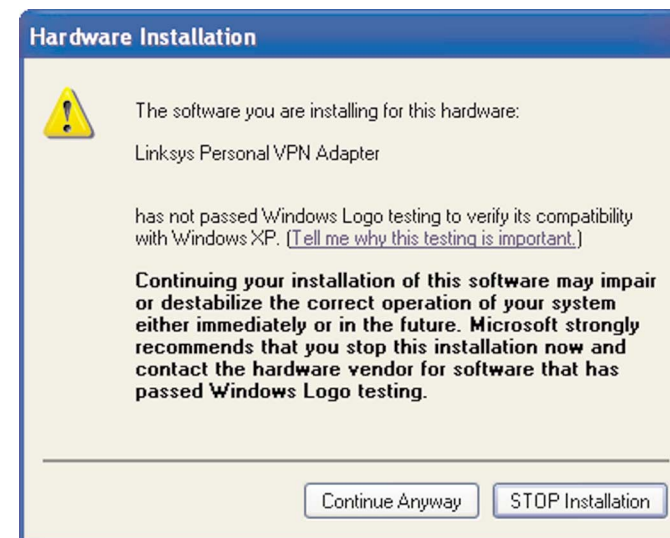


Figure 4-3



5. Windows may inform you that it is installing the software.

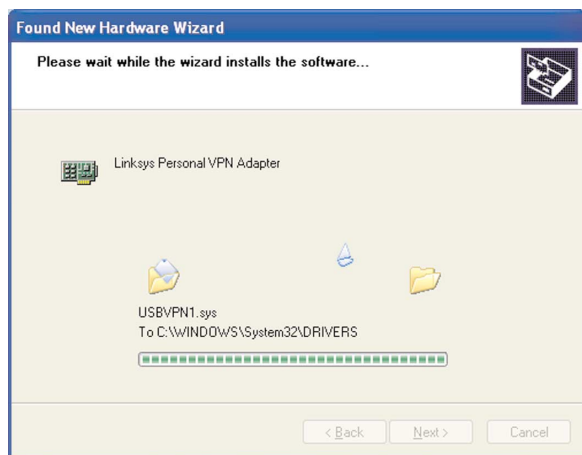


Figure 4-4

6. The *Completing the Found New Hardware Wizard* screen will appear. Click the **Finish** button. Then remove the Setup CD from the CD-ROM drive.

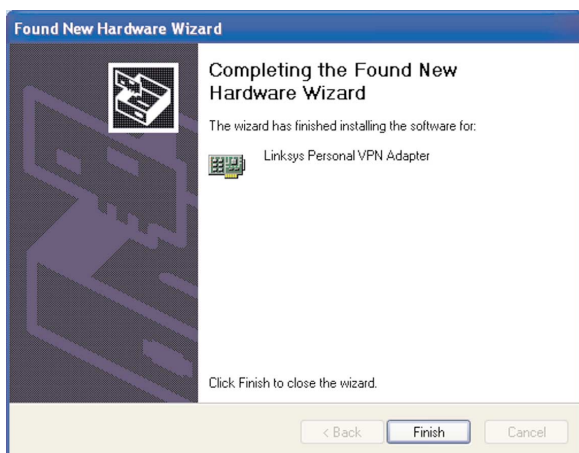


Figure 4-5

**Congratulations! The installation of the USB VPN and Firewall Adapter's driver is complete.**

**For more information about networking under Windows XP, refer to your Microsoft Windows XP documentation.**

## Driver Installation for Windows 2000

1. If you haven't already, start your computer.
2. Windows 2000 will automatically detect the Adapter connected to your PC. When the *Welcome to the Found New Hardware Wizard* screen appears, insert the Setup CD into your CD-ROM drive, and click the **Next** button.



Figure 4-6

3. Select **Search for a suitable driver for my device (recommended)**. Click the **Next** button.



Figure 4-7



4. When the *Locate Driver Files* screen appears, select **CD-ROM drives** and Windows will find the driver on the CD. Click the **Next** button to continue.



Figure 4-8

5. The *Driver Files Search Results* screen will appear when Windows has found the driver. Click the **Next** button to continue.



Figure 4-9

6. You may be informed that a digital signature has not been found (see Figure 4-10). This is normal, and it has been verified that the Adapter does work with Windows 2000. Click the **Yes** button to continue.

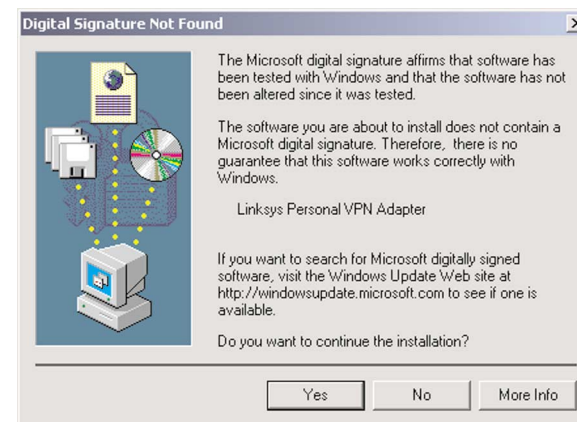


Figure 4-10

7. The *Completing the Found New Hardware Wizard* screen will appear. Click the **Finish** button, and remove the Setup CD from the CD-ROM drive.

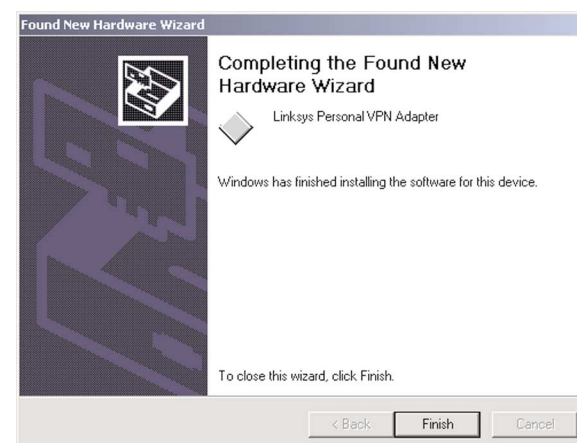


Figure 4-11

8. When you are asked if you want to restart your computer, click **Yes**, and allow your system to restart. If Windows does not ask you to restart your PC, restart your PC anyway.
9. After your computer restarts, you can make the necessary changes to your system's network settings by clicking on the **Start** button, then **Settings**, then **Control Panel**. Next, double-click **Network and Dial-up**, then double-click **Local Area Connections**. Click **Properties**.
  - *Client for Microsoft Networks*
  - *File and Printer Sharing for Microsoft Networks*
  - *Internet Protocol (TCP/IP)*
10. When the *Local Area Connection* screen is displayed, confirm that all the following network components are installed:

There might be additional components listed; however, if any of the above components are missing, refer to your Windows 2000 documentation. When you have verified that each component is listed, click **OK**.

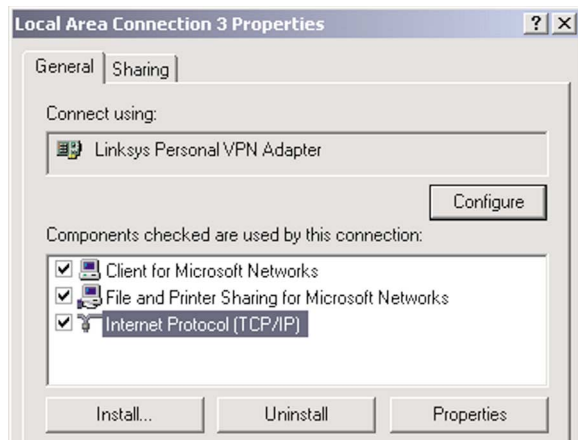


Figure 4-12

**Congratulations! The installation of the USB VPN and Firewall Adapter's driver is complete.**

**For more information about networking under Windows 2000, refer to your Microsoft Windows 2000 documentation.**

## Driver Installation for Windows Me

1. If you haven't already, start your computer.
2. Windows Me will automatically detect the Adapter connected to your PC and display the *New Hardware Found* screen.



Figure 4-13

3. When the *Add New Hardware Wizard* screen appears, insert the Setup CD into your CD-ROM drive, and select **Automatic search for a better driver (Recommended)**. Click the **Next** button.



Figure 4-14

4. When Windows is finished installing the driver, it will ask you to restart your computer. Click **Yes**, and allow your system to restart. If Windows does not ask you to restart your PC, restart your PC anyway.

**Congratulations! The installation of the USB VPN and Firewall Adapter's driver is complete.**

**For more information about networking under Windows Me, refer to your Microsoft Windows Me documentation.**

## Driver Installation for Windows 98SE

1. If you haven't already, start your computer.
2. Windows 98 will automatically detect the Adapter connected to your PC. When the first *Add New Hardware Wizard* screen appears, insert the Setup CD into your CD-ROM drive, and click the **Next** button.

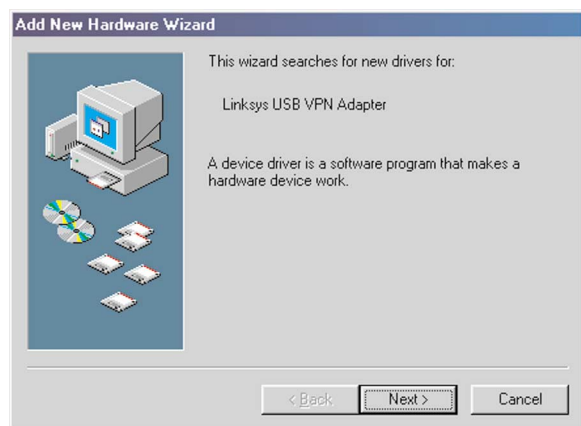


Figure 4-16

3. Select **Search for the best driver for your device (Recommended)**, and click the **Next** button.



Figure 4-17

4. When the *next* screen appears, select **CD-ROM drives** and Windows will find the driver on the CD. Click the **Next** button to continue.

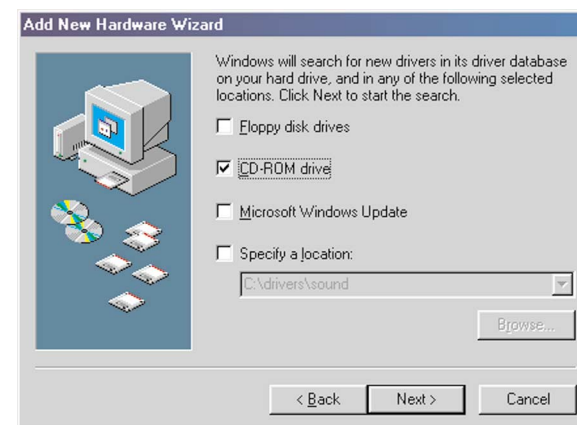


Figure 4-18

5. When Windows notifies you that it is ready to install the driver files, click the **Next** button to continue.



Figure 4-19

6. Windows will begin copying the driver files to your computer. If Windows asks you for the original Windows CD-ROM, insert the CD-ROM, and direct Windows to the proper location for the CD-ROM (e.g., **D:**). If you have the Windows 98 setup files already installed in a directory, enter **C:\windows\options\cabs** (if “C” is the letter of your hard drive) in the field and click **OK**.



Figure 4-20

7. When Windows has completed copying the files, click the **Finish** button.



Figure 4-21

8. When asked if you want to restart your computer, remove the Driver CD from the CD-ROM drive, and click the **Yes** button. If Windows does not ask you to restart your PC, restart your PC anyway.

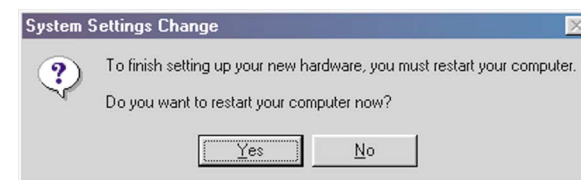


Figure 4-22

**Congratulations! The installation of the Compact USB VPN & Firewall Adapter is complete.**

**For more information about networking under Windows 98SE, refer to your Microsoft Windows 98SE documentation.**

# Chapter 5: Configure TCP/IP

## Overview



**Important:** These instructions apply only to Windows XP, 2000, Millennium, or 98 machines. By default, Windows XP, 2000, Millennium, and 98 has TCP/IP installed and set to obtain an IP address automatically.

The instructions in this chapter will help you configure your computer to be able to communicate with the Adapter using TCP/IP.

To do this, you need to configure your PC's network settings to obtain an IP (or TCP/IP) address automatically (called DHCP). Computers use IP addresses to communicate with each other across a network or the Internet.

Find out which operating system your computer is running, such as Windows XP, 2000, Millennium, or 98. You will need to know which operating system your computer is running. You can find out by clicking the **Start** button and then going to the **Settings** option. Then click **Control Panel**, and then double-click the **System** icon. If your Start menu doesn't have a Settings option, you're running Windows XP. Click the **Cancel** button when done.

You may need to do this for each computer that you are connecting to the Router.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an adapter has been successfully installed in each PC you will configure. Once you've configured your computers, continue to "Chapter 6: Configure the Adapter."

## Configuring Windows XP PCs

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 in the next section for Windows 2000.

1. Click to the Network screen by clicking the **Start** button and then **Control Panel**. From there, click the **Network and Internet Connections** icon and then the **Network Connections** icon.
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button. (See Figure 5-1.)

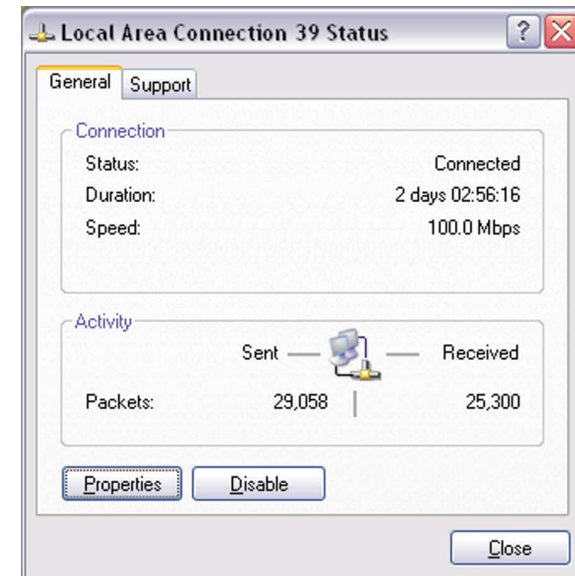


Figure 5-1

3. Select **Internet Protocol (TCP/IP)**, as shown in Figure 5-2, and click the **Properties** button.

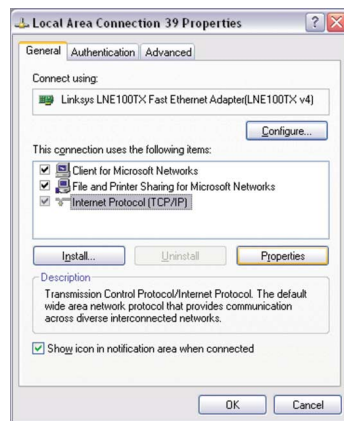


Figure 5-2

4. Select **Obtain an IP address automatically**. Once the new window **Select Obtain an IP address automatically** in both places, as shown in Figure 5-3, and click the **OK** button. Click the **OK** button again to complete the PC configuration.

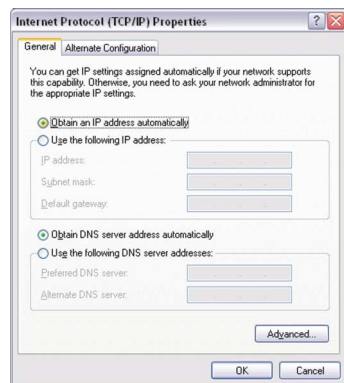


Figure 5-3

5. Restart your computer.

**Go to “Chapter 6: Configure the Adapter.”**

## Configuring Windows 2000 PCs

1. Go to the Network screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network and Dial-up Connections** icon.
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. (See Figure 5-4.) Click the **Properties** button.

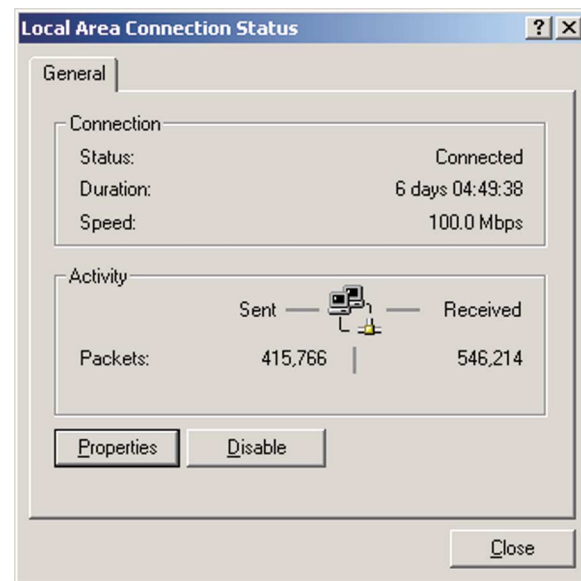


Figure 5-4



3. Select **Internet Protocol (TCP/IP)**, shown in Figure 5-5, and click the **Properties** button.



Figure 5-5

4. Select **Obtain an IP address automatically** in both places, as shown in Figure 5-6, and click the **OK** button. Click the **OK** button again to complete the PC configuration.

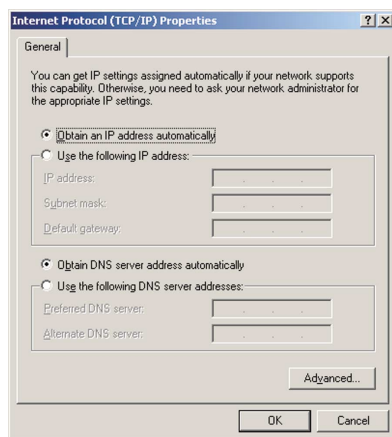


Figure 5-6

5. Restart your computer.

**Go to “Chapter 6: Configure the Adapter:”**

## Configuring Windows 98 and Millennium PCs

1. Go to the Network screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network** icon.
2. On the Configuration tab, shown in Figure 5-7, select the **TCP/IP** line for the USB VPN & Firewall Adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. (If there is no TCP/IP line listed, refer to “Appendix F: Installing the TCP/IP Protocol” or your Ethernet adapter’s user guide to install TCP/IP now.) Click the **Properties** button.

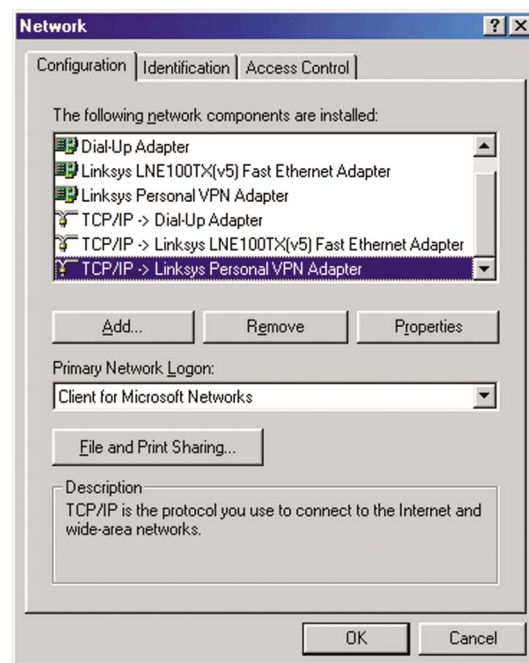


Figure 5-7

- Click the **IP Address** tab and select **Obtain an IP address automatically**, as shown in Figure 5-8.

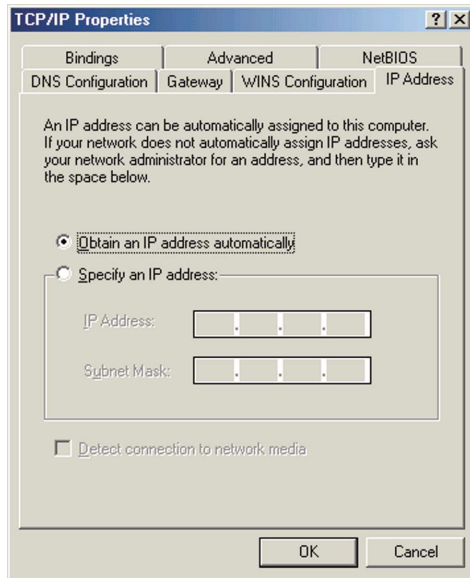


Figure 5-8

- Now click the **Gateway** tab to ensure that the Installed Gateway field is left blank. Click the **OK** button.
- Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Supply them by pointing to the correct file location, e.g., D:\win98, D:\win9x, c:\windows\options\cabs, etc. (if "D" is the letter of your CD-ROM drive).
- Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

**Go to "Chapter 6: Configure the Adapter."**

## Chapter 6: Configure the Adapter

This chapter will show you how to configure the Adapter to function in your network and gain access to the Internet through your Internet Service Provider (ISP). Detailed description of the Adapter's Web-based Utility can be found in "Chapter 7: The USB VPN & Firewall Adapter's Web-based Utility." Your ISP may require the use of a Host Name and Domain Name. Further, you will set the WAN Connection Type on the Adapter's Setup tab based on the information provided by your ISP. *You will need the setup information from your ISP.* If you do not have this information, please contact your ISP before proceeding.

The instructions from your ISP will tell you how to set up your PC for Internet access. Because you are now using the Adapter, you will use the setup information to configure the Adapter instead of your PC.

- Open your web browser. (It is all right if you get an error message at this point. Continue following these directions.) Enter **http://192.168.1.1** in the web browser's Address field, as shown in Figure 6-1. Press the **Enter** key.



Figure 6-1

- An Enter Network Password window, shown in Figure 6-2, will appear (Windows XP users will see a Connect to 192.168.1.1 window, shown in Figure 6-3). Windows XP, the screen may look different.) Leave the User Name field empty, and enter **admin** in lowercase letters in the Password field (**admin** is the default password). Then, click the **OK** button.



Figure 6-2

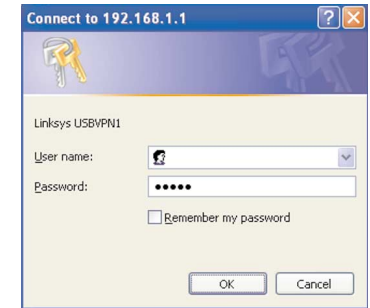


Figure 6-3

3. The Adapter 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 Adapter. These fields are usually left blank. If requested by your ISP (usually cable ISPs), complete these two fields.

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

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

## Obtain an IP Address Automatically

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 Address Automatically** as the WAN Connection Type. (Shown in Figure 6-4.)

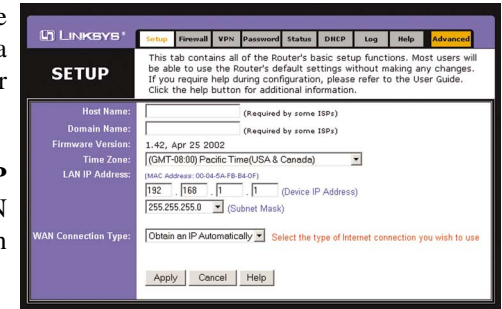


Figure 6-4

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

## Static IP Address

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

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

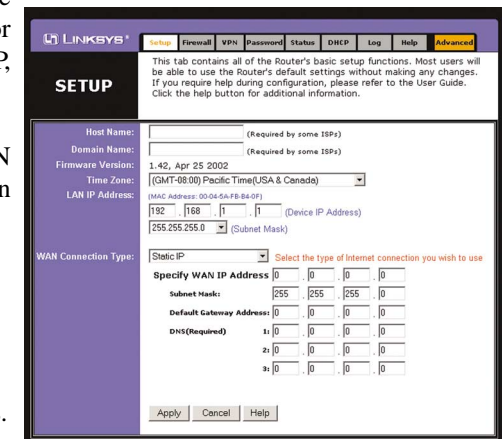


Figure 6-5

- B. Enter the **IP Address**.
- C. Enter the **Subnet Mask**.
- D. Enter the **Gateway Address**.
- E. Enter the **DNS** in the 1, 2, and/or 3 fields. You need to enter at least one DNS address.
- F. Click the **Apply** and **Continue** buttons to save the settings, or click the **Cancel** button to clear the settings and start over. When you are finished, proceed to step 5.

## 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:

- Select **PPPoE** as the WAN Connection Type. (Shown in Figure 6-6.)
- Enter the **User Name**.
- Enter the **Password**.
- Click the **Apply** and **Continue** buttons to save the settings, or click the **Cancel** button to clear the settings and start over.
- When you are finished, click the **Status** tab, and then click the **Connect** button to start the connection. Proceed to step 5.

## PPTP

PPTP is a service used in Europe only. (Shown in Figure 6-7.) 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.

The image shows the Linksys Setup web interface. The 'WAN Connection Type' is set to 'PPPoE'. The 'User Name' and 'Password' fields are visible. The 'Apply' button is at the bottom.

Figure 6-6

The image shows the Linksys Setup web interface. The 'WAN Connection Type' is set to 'PPTP'. The 'Specify WAN IP Address' field is visible. The 'Apply' button is at the bottom.

Figure 6-7

## USB VPN & Firewall Adapter

- 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.
- Reset the power on your cable or DSL modem.
- Restart your computer so that they can obtain the Adapter's new settings.

If you need advanced setting information, please refer to "Chapter 7: The USB VPN & Firewall Adapter's Web-based Utility".

Congratulations! You've successfully configured the Adapter. Test the setup by opening your web browser and entering [www.linksys.com/registration](http://www.linksys.com/registration), as shown in Figure 6-8.

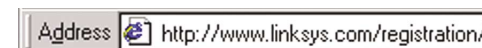


Figure 6-8

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 7: The USB VPN & Firewall Adapter's Web-based Utility" for more details and advanced settings information.**

# Chapter 7: The USB VPN & Firewall Adapter's Web-based Utility

## Overview

For your convenience, use the Adapter'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 the computer connected with a USB cable to the Adapter.

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

- **Setup** Enter the settings provided by your ISP.
- **Password** The Adapter's default password is **admin**. To make the Adapter more secure, change the Password from its default.

The Status, Firewall, VPN, Password, Status, DHCP, Log, and Help tabs are also available for basic setup of the Adapter.

## Quick and Easy Adapter Administration

To access the web-based utility of the Adapter, launch Internet Explorer or Netscape Navigator, and enter the Adapter's default IP address, **192.168.1.1**, in the Address field, as shown in Figure 7-1. Then, press **Enter**.



Figure 7-1

## USB VPN & Firewall Adapter

An Enter Network Password window, shown in Figure 7-2, will appear (Windows XP users will see a Connect to 192.168.1.1 window, shown in Figure 7-3). Leave the User Name field blank, and enter **admin** in the Password field. Then click the **OK** button.



Figure 7-2



Figure 7-3

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

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

## Setup

The Setup screen is the first screen you see when you access the web-based utility. If you have already installed and set up the Adapter, you have already seen this screen and properly configured all of the screen's values.

- **Host Name & Domain Name** These fields allow you to supply a host and domain name for the Adapter. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.
- **Firmware Version** This entry shows the version and date of the firmware you are using. Future versions of the Adapter's firmware will be posted and available for download on the Linksys website at [www.linksys.com](http://www.linksys.com).



- **LAN IP Address and Subnet Mask** The values for the Adapter's IP Address and Subnet Mask are shown here. The default values are 192.168.1.1 for the Device IP Address and 255.255.255.0 for the Subnet Mask.
- **WAN Connection Type** The Adapter supports four connection types: DHCP, PPPoE, Static IP, and PPTP. Each Setup screen and available features will differ depending on what kind of connection type you select.



**Note:** You can test and see if the settings are correct by successfully connecting to the Internet.

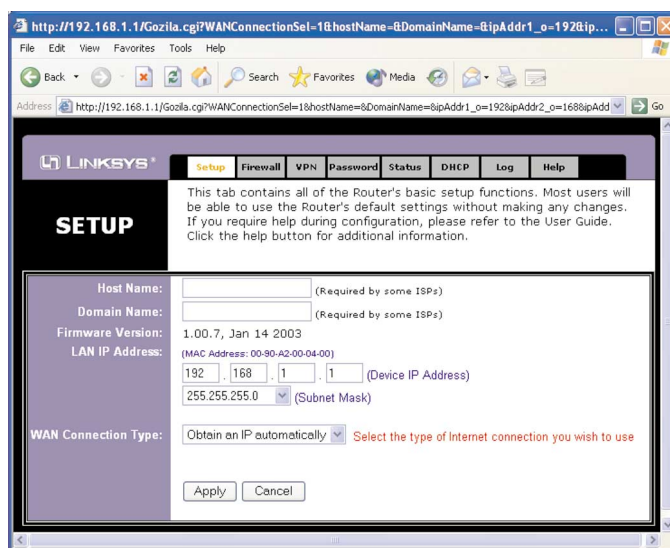


Figure 7-4

## Obtain an IP Address Automatically

By default, the Adapter's WAN Connection Type is set to obtain an IP address automatically, shown in Figure 7-4, and it should be used only if your ISP supports DHCP.

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

## Static IP

If you are required to use a permanent IP address, then select **Static IP**, as shown in Figure 7-5.

### Specify WAN IP Address

This is the IP address that the Adapter has, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

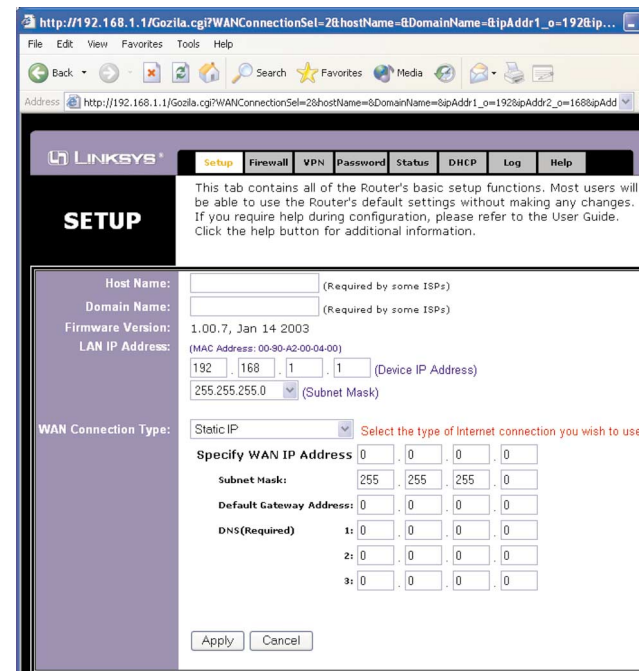


Figure 7-5

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

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

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

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



## PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections for end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, select the PPPoE connection type, as shown in Figure 7-6.

The screenshot shows the Linksys Setup page in a web browser. The 'WAN Connection Type' is set to 'PPPoE'. The 'User Name' is 'linksys' and the 'Password' is masked with asterisks. The 'Connect on Demand' option is selected, with a 'Max Idle Time' of 5 minutes. The 'Keep Alive' option is not selected, with a 'Redial Period' of 30 seconds. The 'Apply' button is visible at the bottom.

Figure 7-6

**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 Adapter 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 Adapter 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. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet access disconnects.

**Keep Alive Option and Redial Period** If you select this option, the Adapter will periodically check your Internet connection. If you are disconnected, then the Adapter will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. The default Redial Period is 30 seconds.

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



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

## PPTP

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

**Specify WAN IP Address** This is the IP address that the Adapter has, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

The screenshot shows the Linksys Setup page in a web browser. The 'WAN Connection Type' is set to 'PPTP'. The 'Specify WAN IP Address' field is set to 192.168.1.1, and the 'Subnet Mask' is set to 255.255.255.0. The 'Default Gateway Address' is set to 0.0.0.0. The 'User Name' is 'linksys' and the 'Password' is masked with asterisks. The 'Connect on Demand' option is selected, with a 'Max Idle Time' of 5 minutes. The 'Keep Alive' option is not selected, with a 'Redial Period' of 30 seconds. The 'Apply' button is visible at the bottom.

Figure 7-7

**Subnet Mask** This is the Adapter's Subnet

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

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

**Connect on Demand and Max Idle Time** You can configure the Adapter 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 Adapter 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. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet access disconnects.

**Keep Alive Option and Redial Period** If you select this option, the Adapter will periodically check your Internet connection. If you are disconnected, then the Adapter will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. The default Redial Period is 30 seconds.

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

## Firewall

Figure 7-8

The Firewall Tab, shown in Figure 7-8, allows you to set the Cable/DSL Firewall Adapter's level of security. Some environments require greater security while some Internet applications work better with fewer restrictions. This tab allows you to customize these settings.

**Advanced Firewall Protection** Enable this option to use SPI (Stateful Packet Inspection) and DoS (Denial of Service). These functions allow for more detailed review of data packets entering your network environment and prevention of Denial of Service attacks.

**Web Filter** You can either enable or disable these four filtering methods by selecting **Allow** or **Deny**.

- **Proxy** Use of WAN proxy servers may compromise the Adapter's security. Denying Proxy will disable access to any WAN proxy servers.
- **Java** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language.
- **ActiveX** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language.
- **Cookie** A cookie is data stored on your PC and used by Internet sites when you interact with them, so you may not want to deny cookies.

**Blocked URL Contents** These ten fields are for denying access to specific websites. Type the URL (or Internet address) of the site you wish to block or any text you wish the browser to discriminate against in one of the empty fields. You can also block specific files like JPEG or GIF files (e.g., files with the extension ".jpg" or ".gif").

**Time Filter** This option allows you to block access to your LAN or WAN, or both within a prescribed time period. Enabling Time Filter will display further options, as shown in Figure 7-9. Clicking **Block Incoming Traffic** will block access to your local area network. Clicking **Block Outgoing Traffic** will block access to your wide area network. To block access to both, click **Block Bi-Direction Traffic**. In choosing these options, you will be allowed to change the time when access is being filtered. This option is turned off by default with the **Disable** radio button selected. Next, click the drop-down windows to set the time and days when access will be filtered.

The Time Filter selection uses a 24-hour clock. In this method, every hour until noon is displayed as 1:00 through 12:00. Every hour after that is an hour added to 12. For example, 3:00 pm would be displayed as 15:00 and 9:45 pm would be displayed as 21:45.

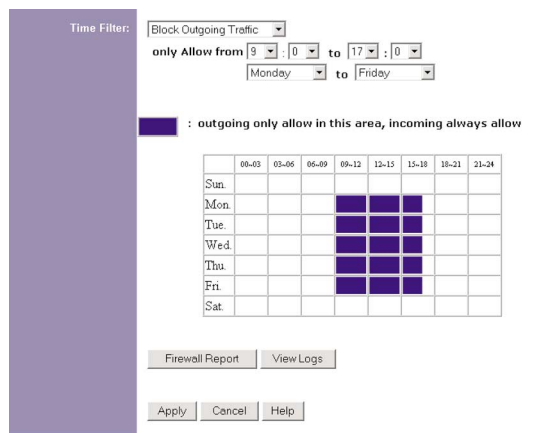


Figure 7-9

Click the **Firewall Report** button to view a status report on the firewall. (This is the same as the Firewall Log.)

Click the **View Logs** button to open a new window (which is the same as the Log tab). From the drop-down menu, select the log you wish to view: All (to view all logs), System Log, Access Log, Firewall Log, or VPN Log.

Note: To be able to view any of the Logs, you must first select the **Enable** option next to Log on the Log tab.

- **System Log** The System Log screen displays a list of cold and warm starts, web login successes and failures, and packet filtering policies.
- **Access Log** The Access Log screen shows all incoming and outgoing traffic.
- **Firewall Log** The Firewall Log screen lists activities performed by the firewall to prevent DoS attacks, including URL filtering and time filtering.
- **VPN Log** The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used.

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

## VPN

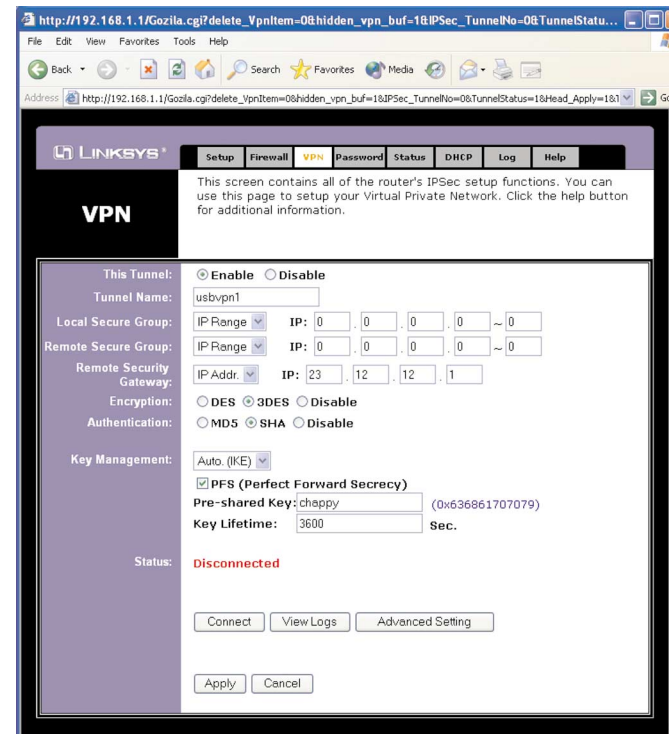


Figure 7-10

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. This connection is very specific as far as its settings are concerned; this is what creates the security. The VPN screen, shown in Figure 7-10, allows you to configure your VPN settings to make your network more secure.



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

## Establishing a Tunnel

The Firewall Adapter creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

**This Tunnel** is where you enable or disable the tunnel. Click the radio button next to **Enable** to enable the tunnel. Click the radio button next to **Disable** to disable a tunnel entry.

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

## Local Secure Group and Remote Secure Group

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



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

- **Subnet** - If you select **Subnet** (which is the default), this will allow all computers on the local subnet to access the tunnel. In the example shown in Figure 7-11, all Local Secure Group computers with IP Addresses 192.168.1.xxx will be able to access the tunnel. All Remote Secure Group computers with IP Addresses 192.168.2.xxx will be able to access the tunnel (in your settings, use the IP Addresses appropriate for your VPN). When using the Subnet setting, the default values of **0** should remain in the last fields of the **IP** and **Mask** settings.

The screenshot shows the configuration window for the Firewall Adapter. It has a purple sidebar on the left with the following options: 'This Tunnel:', 'Tunnel Name:', 'Local Secure Group:', 'Remote Secure Group:', 'Remote Security Gateway:', 'Encryption:', and 'Authentication:'. The main area on the right contains the following settings:

- This Tunnel:** ☒ Enable ☐ Disable
- Tunnel Name:** Branch Office 1
- Local Secure Group:** Subnet (dropdown), IP: 192 . 168 . 1 . 0, Mask: 255.255.255.0
- Remote Secure Group:** Subnet (dropdown), IP: 192 . 168 . 2 . 0, Mask: 255 . 255 . 255 . 0
- Remote Security Gateway:** IP Addr. (dropdown), IP: 0 . 0 . 0 . 0
- Encryption:** ☒ DES ☐ 3DES ☐ Disable
- Authentication:** ☒ MD5 ☐ SHA ☐ Disable

Figure 7-11



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

- **IP Address** - If you select **IP Address**, only the computer with the specific IP Address that you enter will be able to access the tunnel. In the example shown in Figure 7-12, only the computer with IP Address 192.168.1.10 can access the tunnel from this end. Only the computer with IP Address 192.168.2.12 can access the tunnel from the remote end (in your settings, use the IP Addresses appropriate for your VPN).

<b>This Tunnel:</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>
<b>Tunnel Name:</b>	Branch Office 1
<b>Local Secure Group:</b>	IP Addr. IP: 192 . 168 . 1 . 10
<b>Remote Secure Group:</b>	IP Addr. IP: 192 . 168 . 2 . 12
<b>Remote Security Gateway:</b>	IP Addr. IP: 0 . 0 . 0 . 0
<b>Encryption:</b>	<input checked="" type="radio"/> <b>DES</b> <input type="radio"/> <b>3DES</b> <input type="radio"/> <b>Disable</b>
<b>Authentication:</b>	<input checked="" type="radio"/> <b>MD5</b> <input type="radio"/> <b>SHA</b> <input type="radio"/> <b>Disable</b>

Figure 7-12

- **IP Range** - If you select **IP Range**, it will be a combination of Subnet and IP Address. You can specify a range of IP Addresses within the Subnet which will have access to the tunnel. In the example shown in Figure 7-13, all computers on this end of the tunnel with IP Addresses between 192.168.1.1 and 192.168.1.20 can access the tunnel from the local end. Only computers assigned an IP Address between 192.168.2.1 and 192.168.2.100 can access the tunnel from the remote end (in your settings, use the IP Ranges appropriate for your VPN).

<b>This Tunnel:</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>
<b>Tunnel Name:</b>	Branch Office 1
<b>Local Secure Group:</b>	IP Range IP: 192 . 168 . 1 . 1 ~ 20
<b>Remote Secure Group:</b>	IP Range IP: 192 . 168 . 2 . 1 ~ 100
<b>Remote Security Gateway:</b>	IP Addr. IP: 0 . 0 . 0 . 0
<b>Encryption:</b>	<input checked="" type="radio"/> <b>DES</b> <input type="radio"/> <b>3DES</b> <input type="radio"/> <b>Disable</b>
<b>Authentication:</b>	<input checked="" type="radio"/> <b>MD5</b> <input type="radio"/> <b>SHA</b> <input type="radio"/> <b>Disable</b>

Figure 7-13

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

- **Host** - If you select **Host** for the Remote Secure Group, then the Remote Secure Group will be the same as the Remote Security Gateway setting: IP Address, FQDN (Fully Qualified Domain Name), or Any. (Remote Security Gateway settings are explained on the following page.) In the example shown in Figure 7-14, the Remote Secure Group is the same as the Remote Security Gateway, set to a specific IP Address.

<b>This Tunnel:</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>
<b>Tunnel Name:</b>	Branch Office 1
<b>Local Secure Group:</b>	IP Addr. IP: 192 . 168 . 1 . 1
<b>Remote Secure Group:</b>	Host (the same as Remote Security Gateway setting!)
<b>Remote Security Gateway:</b>	IP Addr. IP: 0 . 0 . 0 . 0
<b>Encryption:</b>	<input checked="" type="radio"/> <b>DES</b> <input type="radio"/> <b>3DES</b> <input type="radio"/> <b>Disable</b>
<b>Authentication:</b>	<input checked="" type="radio"/> <b>MD5</b> <input type="radio"/> <b>SHA</b> <input type="radio"/> <b>Disable</b>

Figure 7-14

- **Any** - If you select **Any** for the Remote Security Group, as shown in Figure 7-15, the local Firewall Adapter will accept a request from any IP address. This setting should be chosen when the other endpoint is using DHCP or PPPoE on the WAN side.

<b>This Tunnel:</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>
<b>Tunnel Name:</b>	Branch Office 1
<b>Local Secure Group:</b>	IP Addr. IP: 192 . 168 . 1 . 1
<b>Remote Secure Group:</b>	Any (This Gateway accepts request from any IP address!)
<b>Remote Security Gateway:</b>	IP Addr. IP: 0 . 0 . 0 . 0
<b>Encryption:</b>	<input checked="" type="radio"/> <b>DES</b> <input type="radio"/> <b>3DES</b> <input type="radio"/> <b>Disable</b>
<b>Authentication:</b>	<input checked="" type="radio"/> <b>MD5</b> <input type="radio"/> <b>SHA</b> <input type="radio"/> <b>Disable</b>

Figure 7-15



## Remote Security Gateway

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

- **IP Address** - If you select IP Address, as shown in Figure 7-16, enter the IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another Firewall Adapter, 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 Firewall Adapter, but the IP Address of the remote Firewall Adapter or device with which you wish to communicate.

This Tunnel: ☒ Enable ☐ Disable  
 Tunnel Name: Branch Office 1  
 Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1  
 Remote Secure Group: Host (the same as Remote Security Gateway setting!)  
 Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0  
 Encryption: ☒ DES ☐ 3DES ☐ Disable  
 Authentication: ☒ MD5 ☐ SHA ☐ Disable

Figure 7-16

- **FQDN (Fully Qualified Domain Name)** - If you select FQDN, as shown in Figure 7-17, enter the FQDN of the VPN device at the other end of the tunnel. The remote VPN device can be another Firewall Adapter, 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*.

This Tunnel: ☒ Enable ☐ Disable  
 Tunnel Name: Branch Office 1  
 Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1  
 Remote Secure Group: IP Addr. IP: 192 . 168 . 2 . 1  
 Remote Security Gateway: FQDN Fully-Qualified Domain Name:  
 Encryption: ☒ DES ☐ 3DES ☐ Disable  
 Authentication: ☒ MD5 ☐ SHA ☐ Disable

Figure 7-17

- **Any** - If you select Any for the Remote Security Gateway, as shown in Figure 7-18, 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 Firewall Adapter, 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.

This Tunnel: ☒ Enable ☐ Disable  
 Tunnel Name: Branch Office 1  
 Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1  
 Remote Secure Group: IP Addr. IP: 192 . 168 . 2 . 1  
 Remote Security Gateway: Any (This Gateway accepts request from any IP address!)  
 Encryption: ☒ DES ☐ 3DES ☐ Disable  
 Authentication: ☒ MD5 ☐ SHA ☐ Disable

Figure 7-18

## 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 in Figure 7-19, the word **MyTest** is used. Based on this word, which **MUST** be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you’d like the key to be useful, or leave it blank for the key to last indefinitely.



Key Management: Auto. (IKE)

☐ PFS (Perfect Forward Secrecy)

Pre-shared Key: MyTest (0x)

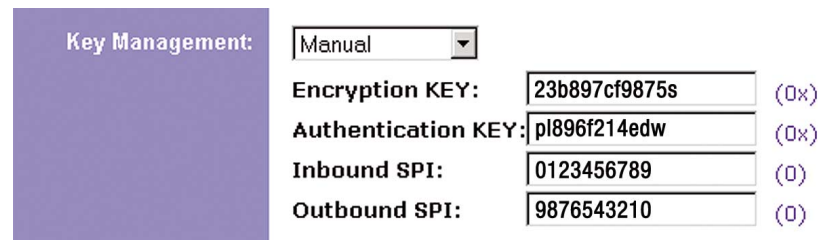
Key Lifetime: 3600 Sec.

Figure 7-19

### Manual Key Management

Similarly, you may choose **Manual** keying, which allows you to generate the key yourself. Enter your **key** into the Encryption KEY field. Then enter an **Authentication KEY** into that field. These fields must both match the information that is being entered in the fields at the other end of the tunnel. The example in Figure 7-20 shows some sample entries for both the Encryption and Authentication Key fields. Up to 24 alphanumeric characters are allowed to create the Encryption Key. Up to 20 alphanumeric characters are allowed to create the Authentication Key.

The **Inbound SPI** and **Outbound SPI** fields are different, however. The Inbound SPI value set here must match the *Outbound SPI* value at the other end of the tunnel. The Outbound SPI here must match the *Inbound SPI* value at the other end of the tunnel. In the example (see Figure 7-20), the Inbound SPI and Outbound SPI values shown would be opposite on the other end of the tunnel. Only numbers can be used in these fields. After you click the Apply button, hexadecimal characters (series of letters and numbers) are displayed in the Inbound SPI and Outbound SPI fields.



Key Management: Manual

Encryption KEY: 23b897cf9875s (0x)

Authentication KEY: pl896f214edw (0x)

Inbound SPI: 0123456789 (0)

Outbound SPI: 9876543210 (0)

Figure 7-20

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

After the VPN device is set up at the other end of the tunnel, you may click the **Connect** button to use the tunnel. This assumes that both ends of the tunnel have a physical connection to each other (e.g., over the Internet, physical wiring, etc.). After clicking the Connect button, click the **Summary** button.

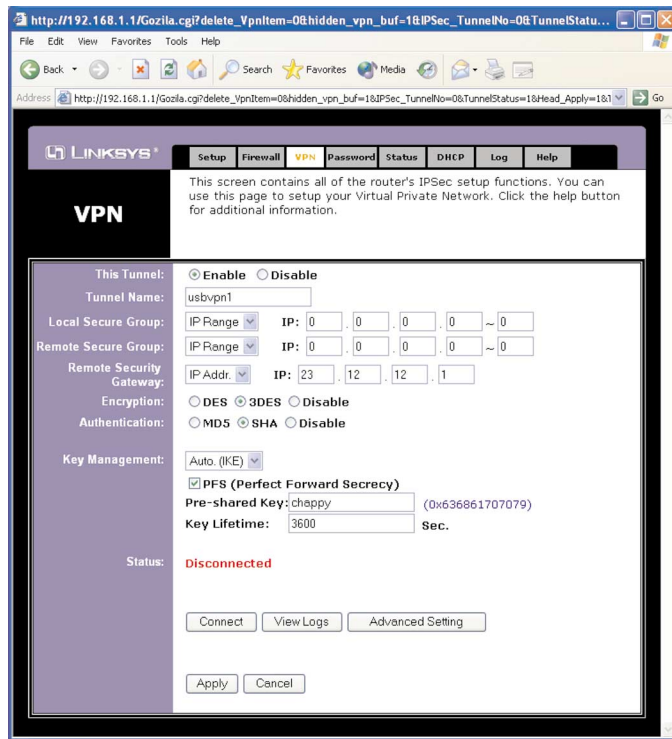


Figure 7-21

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

If **Disconnected** appears under Status, as shown in Figure 7-21, some problem exists that prevents the creation of the tunnel. Make sure that all of your wiring is securely connected. Double-check all the values you entered on the VPN screen to make sure they are correct. If the other end of the tunnel is some distance from you (e.g., in another city, etc.), call to make sure that the settings on that end of the tunnel are correct as well.

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

To get more details concerning your tunnel connection, click the **View Logs** button. The screen in Figure 7-22 will appear:

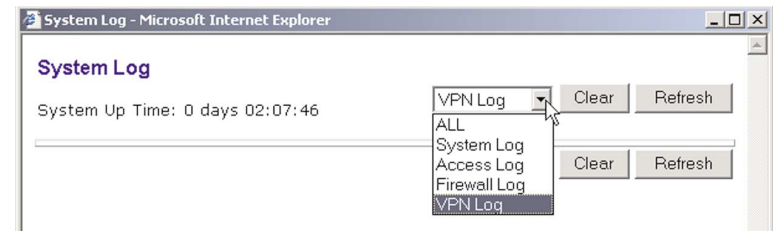


Figure 7-22

Select the log you wish to view: All (to view all logs), System Log, Access Log, Firewall Log, or VPN Log. The System Log screen displays a list of cold and warm starts, web login successes and failures, and packet filtering policies. The Access Log shows all incoming and outgoing traffic. The Firewall Log lists activities performed by the firewall to prevent DoS attacks, including URL filtering and time filtering. The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used.

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

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

## Advanced Settings for Selected IPSec Tunnel

From the Advanced Settings screen, shown in Figure 7-23, 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 Adapter will accept both Main and Aggressive requests from the remote VPN device.

## Encryption

### Advanced Settings for Selected IPSec Tunnel

**Tunnel 1**

Phase 1:

Operation mode : ☒ Main mode ☐ Aggressive mode

Proposal 1:

Encryption : 3DES

Authentication : MD5

Group : 1024-bit

Key Lifetime : 3600 seconds

(Note: Following three additional proposals are also proposed in Main mode:  
DES/MD5/768, 3DES/SHA/1024 and 3DES/MD5/1024)

Phase 2:

Proposal :

Encryption : DES

Authentication : MD5

PFS : OFF

Group : 768-bit

Key Lifetime : 3600 seconds

Other Settings:

☐ NetBIOS broadcast

☐ Anti-replay

☐ Keep-Alive

☐ If IKE failed more than 5 times, block this unauthorized IP for 60 seconds

Apply Cancel

**Figure 7-23**

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

## Authentication

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

## Group

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

## Key Lifetime

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

## Phase 2

### Group

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

### Key Lifetime

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

## Other Settings

### NetBIOS broadcast

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

### Anti-replay

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

### Keep-Alive

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

### Unauthorized IP Blocking

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

## Password

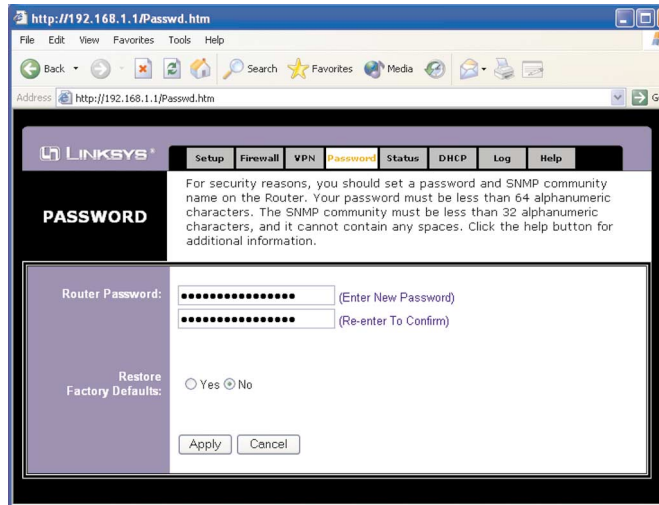


Figure 7-24

The Password screen, shown in Figure 7-24, allows you to change the password and restore default settings on the Adapter.

**Adapter Password** It is *strongly* recommended that you set a password for the Adapter. The default password is **admin**. If you don't change the password, all users on your network will be able to access the Adapter using the default password **admin**.

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

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

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

## Status

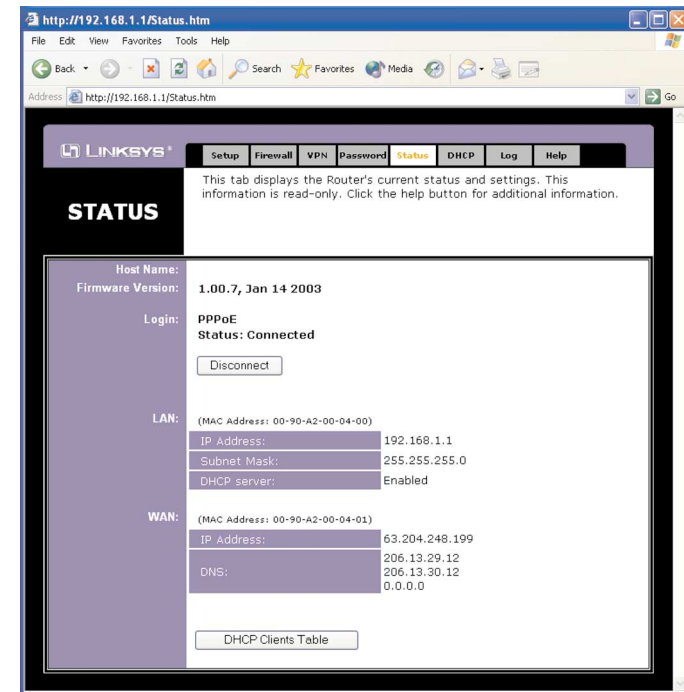


Figure 7-25

The Status screen, shown in Figure 7-25, displays the Adapter's current status and reflects the data and selections you've entered using the Setup screen. All of the information provided on this screen is read-only. To make changes, select the Setup tab.



**Note:** The information provided and buttons available may vary depending on the Adapter's settings.

**Host Name** This field shows the name of the Adapter. This entry is necessary for some ISPs.

**Firmware Version** This field shows the installed version and date of the firmware.

**Login** This indicates if you are using a dial-up style connection like PPPoE or PPTP. For PPPoE or PPTP, there is a **Connect** button to click if you are disconnected and want to re-establish a connection.

**LAN** These fields display the current IP Address and Subnet Mask of the Adapter, as seen by users on your local area network. The DHCP Server field shows the status of the Adapter's DHCP server function, which is either enabled or disabled.

**WAN** These fields display the WAN IP Address, WAN Subnet Mask, and WAN Default Gateway IP Address of the Adapter, as seen by external users on the Internet. The DNS (Domain Name System) IP Address fields show the IP address(es) of the DNS currently used by the Adapter. Multiple DNS IP settings are common. In most cases, the first available DNS entry is used.

**DHCP Release** Click the **DHCP Release** button to release the current IP address of the device connected to the Adapter's WAN port.

**DHCP Renew** Click the **DHCP Renew** button to replace the current IP address—of the device connected to the Adapter's WAN port—with a new IP address.

**DHCP Clients Table** Click the **DHCP Clients Table** button to view the PC that was given an IP address by the Adapter.

## DHCP

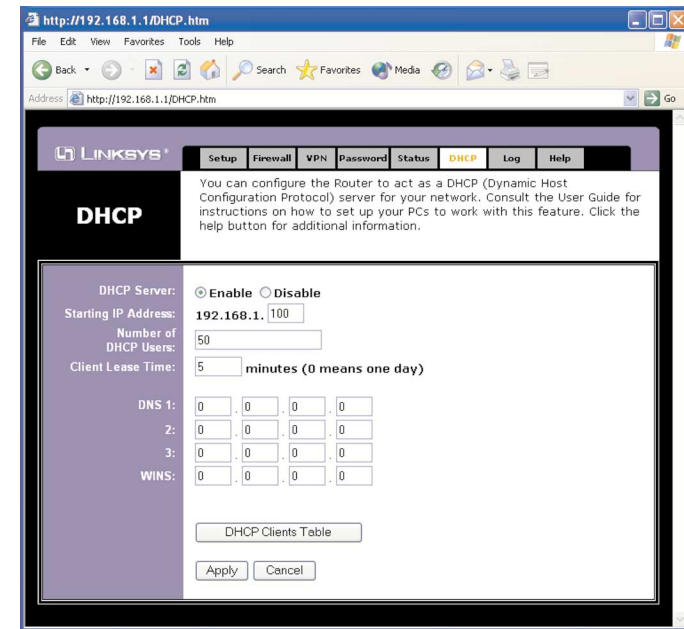


Figure 7-26

From the DHCP screen, shown in Figure 7-26, you can configure the Adapter as a DHCP Server.

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

**DHCP Server** DHCP is already enabled by factory default. Click the **Apply** button and then the **Continue** button. If you disable DHCP, remember to assign a static IP address to the Adapter.

**Starting 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 Adapter is **192.168.1.1**.

**Number of DHCP Users** (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, as shown in Figure 7-28, add 100 to 50, and the range is 192.168.1.100 to 192.168.1.149.

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

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

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

**DHCP Clients Table** Click the **DHCP Clients Table** button to show the current DHCP Client data. (This data is stored in temporary memory and changes periodically.)

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

## Log

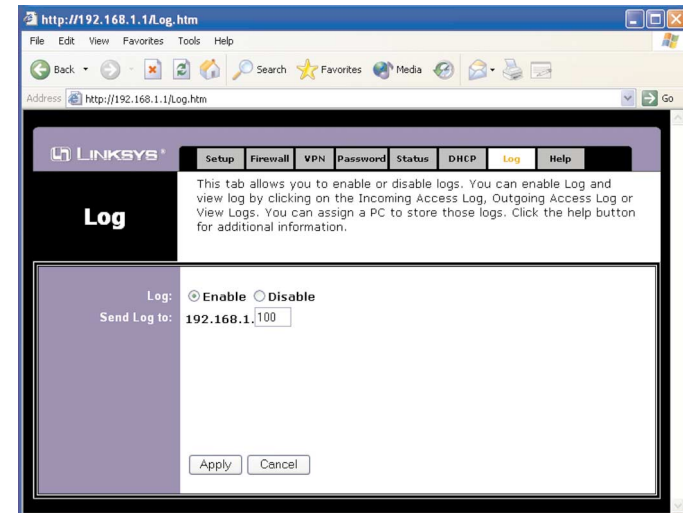


Figure 7-27

The Log tab, shown in Figure 7-27, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

To access activity logs, select the **Enable** option next to Log. This function can be disabled by clicking the **Disable** radio button.

With logging enabled, you can choose to view temporary logs by clicking **View Logs** on the VPN tab.

For a permanent record of these logs, Logviewer software must be used. This software is downloadable from the Linksys website, [www.linksys.com](http://www.linksys.com). The Logviewer saves all incoming and outgoing activity as a permanent file on your PC’s hard drive. In the *Send Log to* field, enter the fixed IP address of the PC running the Logviewer software. The Adapter will now send updated logs to that PC.

To clear any values you’ve entered on any page, click **Cancel** and re-enter information. To apply any settings you’ve altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**.



## Help

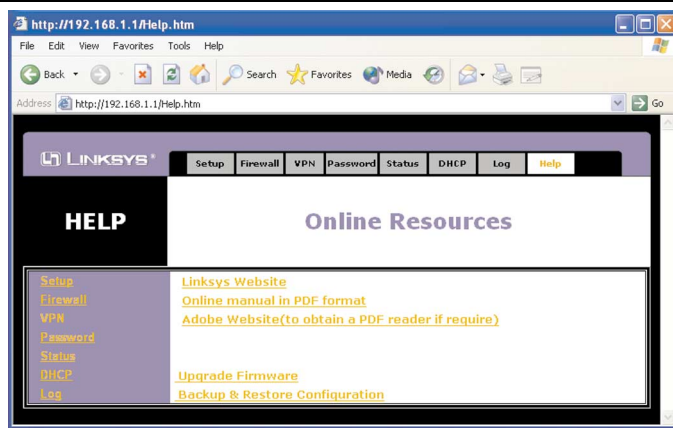


Figure 7-28

Under the Help tab, shown in Figure 7-28, you'll find links to all of the Utility's internal support documentation, including the application that upgrades the Adapter's firmware.

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

Clicking the Linksys Website link will take you to Linksys's website, [www.linksys.com](http://www.linksys.com), provided you are connected to the Internet.

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

New firmware versions are posted at [www.linksys.com](http://www.linksys.com) and can be downloaded for free. If the Adapter can access the Internet already, there's no need to download a newer firmware version, unless that version has a new feature that you want to use. Loading new firmware onto the Adapter does not always enhance the speed or the quality of your connection.

## USB VPN &amp; Firewall Adapter

To upgrade the Adapter's firmware:



**Note:** By upgrading the Adapter's firmware, you may lose the Adapter's configuration settings.

1. Click **Upgrade Firmware** to display the window shown in Figure 7-29.
2. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.
3. Double-click the **firmware file** you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.

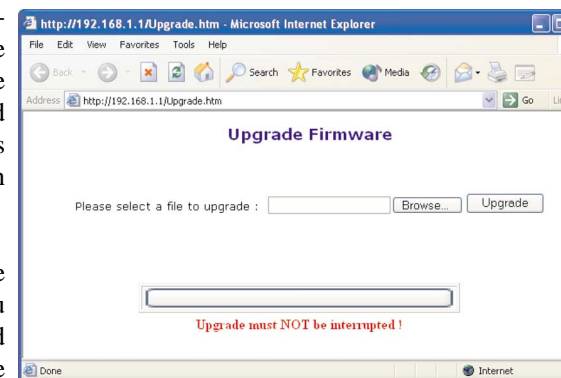


Figure 7-29

To use Backup & Restore Configuration



**Note:** You need Microsoft Internet Explorer 5.0 or above to use this feature.

1. Select **Backup & Restore Configuration** to display the window shown in Figure 7-30.
2. Click **Backup** to back up a configuration.
3. Select **Browse** to find a file, then click **Restore** to restore it.

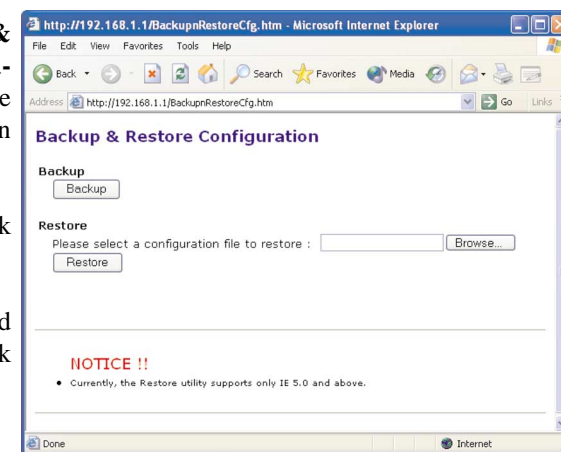


Figure 7-30

# Appendix A: Troubleshooting

## Common Problems and Solutions

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” Provided are possible solutions to problems regarding the installation and operation of the Adapter. 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](http://www.linksys.com).

1. I want to test my Internet connection.

A. Check your TCP/IP settings.

### For Windows 98 and Me:

- Refer to “Appendix B: Installing the TCP/IP Protocol” and “Chapter 5: Configure the TCP/IP” for details. Make sure **Obtain IP address automatically** is selected in the settings.

### For Windows 2000:

- Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
- Right-click the **Local Area Connection** that is associated with the Adapter you are using, and select the **Properties** option.
- In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
- Restart the computer if asked.

### For Windows XP:

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

- Click **Start** and **Control Panel**.
- Click the **Network and Internet Connections** icon and then the **Network Connections** icon.

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

B. Open a command prompt.

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

C. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.

- If you get a reply, the computer is communicating with the Adapter.
- 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 Adapter.

D. In the command prompt, type **ping** followed by your WAN IP address and press the **Enter** key. The WAN IP Address can be found in the web interface of the Adapter. For example, if your WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.

- If you get a reply, the computer is connected to the Adapter.
- If you do NOT get a reply, try checking the device manager under network adapters to make sure your Adapter is installed correctly.

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 do NOT get a reply, there may be a problem with the connection.

2. I am not getting an IP address on the WAN with my Internet connection.
  - A. Refer to “Problem #1, I want to test my Internet connection” to verify that you have connectivity.
  - C. Make sure you are using the right WAN settings. Contact your ISP to see if your WAN connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of “Chapter 7: The Cable/DSL Firewall Adapter’s Web-based Utility” for details on WAN settings.
  - D. Make sure you have the right cable. Check to see if the WAN column has a solidly lit Link LED.
  - E. Make sure the cable connecting from your cable or DSL modem is connected to the Adapter’s Ethernet port. Verify that the Status page of the Adapter’s web interface shows a valid IP address from your ISP.
  - F. Turn off the computer, Adapter, and cable/DSL modem. Wait 30 seconds, and then turn on the Adapter, cable/DSL modem, and computer. Check the Status tab of the Adapter’s web-based utility to see if you get an IP address.
3. I am not able to access the Adapter’s web interface Setup page.
  - A. Refer to “Problem #1, I want to test my Internet connection” to verify that your computer is properly connected to the Adapter.
  - B. Refer to “Appendix C: Finding the MAC Address and IP address for Your Adapter” to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
  - C. Refer to “Problem #5: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users).”
4. I forgot my password, or the password prompt always appears when saving settings to the Adapter.
 

Reset the Adapter 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 Adapter’s web interface by going to **http://192.168.1.1** or the **IP address** of the Adapter. Enter the default password **admin**, and click the **Password** tab.
  - B. Enter a **different password** in the Adapter Password field, and enter the same password in the second field to confirm the password.
  - C. Click the **Apply** and **Continue** buttons.

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

#### For Microsoft Internet Explorer 5.0 or higher:

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

#### For Netscape 4.7 or higher:

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

6. To start over, I need to set the Adapter to factory default.

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

7. 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](http://www.linksys.com). Follow these steps:

- A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware.
- B. To upgrade the firmware, follow the steps in the Help section found in “Chapter 7: The USB VPN & Firewall Adapter’s Web-based Utility.”

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

- A. If the firmware upgrade failed, use the **TFTP** program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- B. Set a **static IP address** on the PC. 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 Adapter's web-based utility through its Help tab.

9. 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 Adapter, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Adapter.
- B. Enter the **password**, if asked. (The default password is **admin**.)
- C. In the Setup tab, select the option **Keep Alive**, and set the **Redial Period** option at **20** (seconds).
- D. Click the **Apply** and **Continue** buttons.
- E. Click the **Status** tab, and click the **Connect** button.
- F. You may see the login status display as **Connecting**. Press the **F5** key to refresh the screen, until you see the login status display as **Connected**.
- G. Click the **Apply** and **Continue** buttons to continue.

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

10. The Diag LED stays lit continuously.

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

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

- Make sure 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 PC is configured correctly, but still not working, check the Adapter. Ensure that it is connected and ON and that the driver is installed correctly. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Adapter is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Adapter 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**.

12. The Full/Col LED keeps flickering continuously.

- Check the Category 5 Ethernet cable and its RJ-45 connectors.
- There may be interference with other network devices. Try removing other PCs or network devices to see if the problem persists. Eliminate each network device one at a time to determine the cause.

## Frequently Asked Questions

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

Is IPsec Pass-Through supported by the Adapter? Yes, it is a built-in feature that the Adapter automatically enables.

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

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

Does the WAN connection of the Adapter support 100 Mbps Ethernet? Yes, and it does, of course, support 100 Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Adapter.

Does the Adapter 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 Adapter 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 Adapter.

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

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do? Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your 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](http://www.linksys.com) for more information.

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

How will I be notified of new Adapter firmware upgrades? All Linksys firmware upgrades are posted on the Linksys website at [www.linksys.com](http://www.linksys.com), where they can be downloaded for free. The Adapter's firmware can be upgraded with TFTP programs. If the Adapter'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 Adapter firmware will not always enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

I am not able to get the web configuration screen for the Adapter. 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**.

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

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

What is the maximum number of VPN tunnels allowed by the Adapter? The Adapter supports one simultaneous IPsec VPN tunnel.

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

**If your questions are not addressed here, refer to the Linksys website, [www.linksys.com](http://www.linksys.com).**

## Appendix B: Installing the TCP/IP Protocol

Follow these instructions to install the TCP/IP protocol on your PC *only* after a the USB VPN & Firewall Adapter has been successfully installed on the PC. These instructions are for Windows 98 and Windows Me. For TCP/IP setup under 2000 and XP, see your Windows documentation or the Help feature.

1. Click the **Start** button. Choose **Settings** and then **Control Panel**.
2. Double-click on the **Network** icon to bring up your Network window. Select the **Configuration** tab.

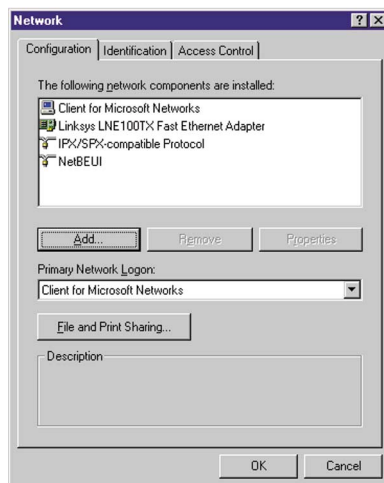


Figure B-1

3. Click the **Add** button.
4. Double-click on **Protocol**.
5. Highlight **Microsoft** under the list of manufacturers.

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

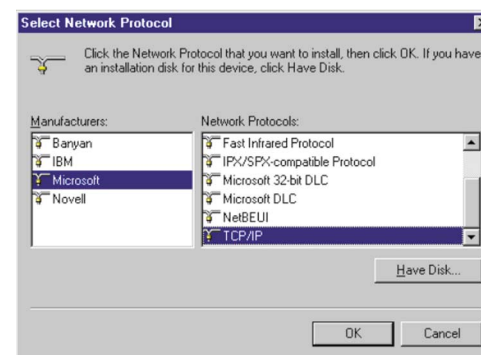


Figure B-2

7. After a few seconds, the main Network window will appear. The TCP/IP Protocol should now be listed.

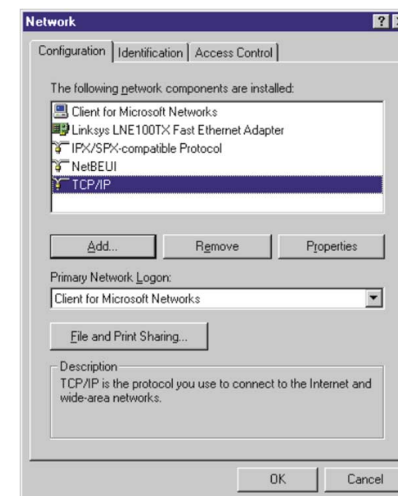


Figure B-3

8. Click the **OK** button. Windows may ask for original Windows installation files. Supply them as needed, e.g., c:\windows\options\cabs, D:\win98, D:\win95, D:\win9x.
9. Windows will ask you to restart the PC. Click the **Yes** button.

**The TCP/IP installation is now complete.**



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

This section describes how to find the MAC address for your Adapter to do MAC Address Cloning for the Adapter and ISP. You can also find the IP address of your Adapter. Follow the steps in this appendix to find the MAC address or IP address for your Adapter in Windows 98, Me, 2000, and XP.

## For Windows 98 and Me:

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

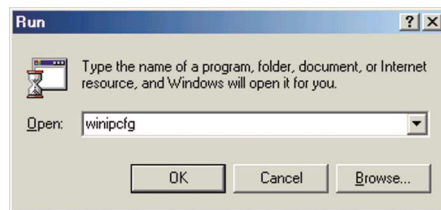


Figure C-1

2. When the IP Configuration window appears, select the Adapter you are using to connect to the Router and/or Modem via a CAT 5 Ethernet cable.

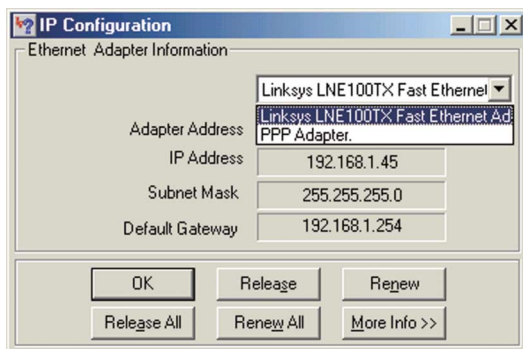


Figure C-2

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

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

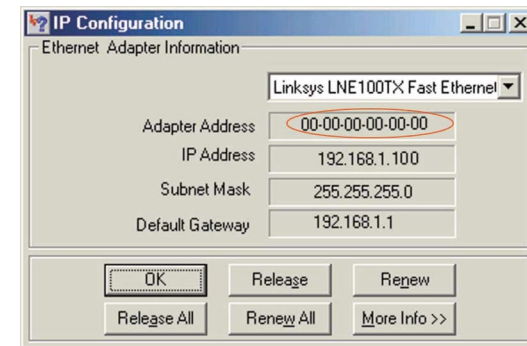


Figure C-3

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



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

## For Windows NT, 2000, and XP:

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

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

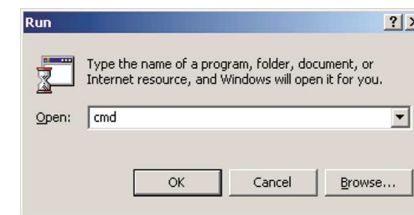


Figure C-4

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

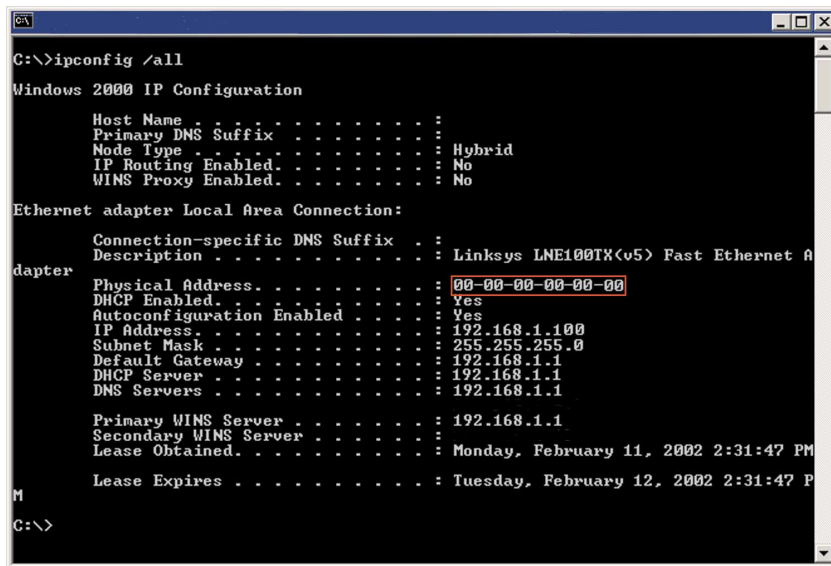


Figure C-5

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

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



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

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

When entering information for MAC Address Cloning, type the **12-digit MAC address** (see Figure C-6).

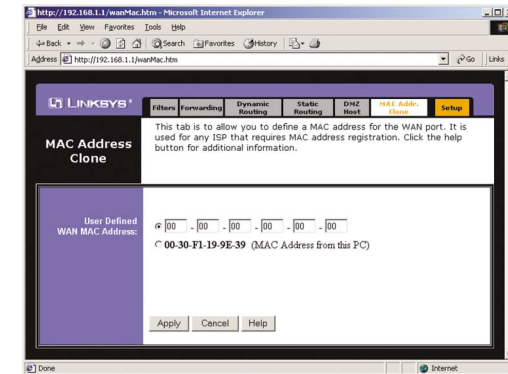


Figure C-6

## Appendix D: Glossary

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

**Adapter** - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC.

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

**Backbone** - The part of a network that connects most of the systems and networks together and handles the most data.

**Bit** - A binary digit. The value - 0 or 1-used in the binary numbering system. Also, the smallest form of data.

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

**Bridge** - A device that interconnects different networks together.

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

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

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

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

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

**Cookie** - Data created by a Web server that is stored on a user's computer. It provides a way for the Web site to keep track of a user's patterns and preferences and, with the cooperation of the Web browser, to store them on the user's own hard disk.

**Data Packet** - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

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

**Denial of Service** - A protocol that directs the network to no longer respond to requests that might arise as the result of a Denial of Service attack.

**Denial of Service Attack** - An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted.

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

**DHCP (Dynamic Host Configuration Protocol)** - A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a

unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

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

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

**DMZ (Demilitarized Zone)** - Allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

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

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

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

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

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

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

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

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

**Fast Ethernet** - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

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

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

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

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

**FTP (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 Web site on a local machine, they are typically uploaded to the Web server using FTP.

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

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

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

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

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

**Hardware** - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the "box" and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

**Hop** - The link between two network nodes.

**HTTP (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 browser.

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

**ICMP (Internet Control Message Protocol)** - Part of the TCP/IP protocol. Network devices such as routers or servers use ICMP to transmit error messages and control messages. For example, the PING program uses ICMP.

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

**IEEE (The Institute of Electrical and Electronics Engineers)** - The IEEE describes itself as "the world's largest technical professional society, promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society.

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

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

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

**IPSec (Internet Protocol Security)** - A suite of protocols used to implement secure exchange of packets at the IP layer. IPSec supports two basic modes: Transport and Tunnel. Transport encrypts the payload of each packet, leaving the header untouched, while Tunnel mode encrypts both the header and the payload and is therefore more secure. IPSec must be supported on both transmit-

ter and receiver and must share a public key. Tunnel mode is widely deployed in VPNs (Virtual Private Networks).

**IPX (Internetwork Packet EXchange)** - A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another.

**ISP (Internet Service Provider)** - A company that provides individuals and companies access to the Internet and other related services such as Web site building and virtual hosting.

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

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

**Mbps (Megabits per second)** - One million bits per second; unit of measurement for data transmission.

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

**MIB (Management Information Base)** - A set of database objects. This set contains information about a specific device for utilizing SNMP.

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

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

**NAT (Network Address Translation)** - The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

**NetBIOS** - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI),

NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols.

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

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

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

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

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

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

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

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

**Packet Filtering** - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).



**Ping (Packet INternet Groper)** - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

**Plug-and-Play** - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

**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.

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

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

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

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

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

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

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

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

**SMTP (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.

**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.).

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

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

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

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

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

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

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

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

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

**Telnet** - A terminal emulation protocol commonly used on the 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.

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

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

**UDP (User Datagram Protocol)** - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connection-less" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

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

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

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

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

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

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

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

## Appendix E: Specifications

Model Number	USBVPN1
Ports	One 10/100 RJ-45 One USB 1.1
Cabling Type	UTP Category 5 or Better
LED Indicators	Session, Diag, Link/Act, Full/Col, 10/100, USB

### Environmental

Dimensions	4.72" x 0.59" x 2.52" (120 mm x 15 mm x 64 mm)
Unit Weight	2.47 oz. (0.07 kg)
Power Input	500 mA Maximum
Certifications	FCC Class B, CE Mark
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85%, Non-condensing
Storage Humidity	5% to 90%, Non-condensing

## Appendix F: Warranty Information

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

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT.

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

## Appendix G: Contact Information

For help with the installation or operation of the USB VPN & Firewall Adapter, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

<b>Sales Information</b>	800-546-5797 (LINKSYS)
<b>Technical Support</b>	800-326-7114
<b>RMA (Return Merchandise Authorization) Issues</b>	www.linksys.com (or call 949-271-5461)
<b>Fax</b>	949-265-6655
<b>E-mail</b>	support@linksys.com
<b>Web</b>	http://www.linksys.com
<b>FTP Site</b>	ftp.linksys.com



[www.linksys.com](http://www.linksys.com)

© Copyright 2003 Linksys, All Rights Reserved.