LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 54Mbps Wireless-G

WIRELESS

VPN Broadband Router

User Guide

Model No. **WRV54G**

CISCO SYSTEMS

Copyright and Trademarks

How to Use this Guide

Your Guide to the Wireless-G VPN Broadband Router has been designed to make understanding networking with the Router easier than ever. Look for the following items when reading this User Guide:

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

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

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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

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

Table of Contents

Chapter 1: Introduction

Welcome

Wireless-G is the upcoming 54Mbps wireless networking standard that's almost five times faster than the widely deployed Wireless-B (802.11b) products found in homes, businesses, and public wireless hotspots around the country—but since they share the same 2.4GHz radio band, Wireless-G devices can also interoperate with existing 11Mbps Wireless-B equipment.

Since both standards are built in, you can protect your investment in existing 802.11b infrastructure, and migrate to the new screaming fast Wireless-G standard as your needs grow.

The Linksys Wireless-G Broadband VPN Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect Wireless-G or Wireless-B devices to the network. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices. Connect four PCs directly, or daisy-chain out to more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

To protect your data and privacy, the Wireless-G Broadband VPN Router can encrypt all wireless transmissions. The Router can serve as a DHCP Server, has NAT technology to protect against Internet intruders, supports VPN pass-through, and can be configured to filter internal users' access to the Internet. Configuration is a snap with the web browser-based configuration utility.

With the Linksys Wireless-G Broadband VPN Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games with the flexibility, speed, and security you need!

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G VPN Broadband Router.

- Chapter 1: Introduction
  This chapter describes the Wireless-G VPN Broadband Router applications and this User Guide.
- Chapter 2: Planning your Wireless Network
  This chapter describes the basics of wireless networking.
- Chapter 3: Getting to Know the Wireless-G VPN Broadband Router
  This chapter describes the physical features of the Router.
- Chapter 4: Connecting the Wireless-G VPN Broadband Router
  This chapter instructs you on how to connect the Router to your network.
- Chapter 5: Configuring the PCs
  This chapter explains how to configure the PCs for your network.
- Chapter 6: Configuring the Router
  This chapter explains how to use the Web-Based Utility to configure the settings on the Router.
- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G VPN Broadband Router.
- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- Appendix C: Configuring IPSec between a Windows 2000 Pc and the Router
  This appendix instructs you on how to establish a secure IPSec tunnel using preshared keys to join a private network inside the VPN Router and a Windows 2000 or XP PC.
- Appendix D: SNMP Functions
  This appendix explains SNMP.
- Appendix E: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on your Router if you should need to do so.
- Appendix F: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

- Appendix G: Finding the MAC Address and IP Address for your Ethernet Adapter.
  This appendix describes how to find the MAC address for your computer's Ethenet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router.

- Appendix H: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix I: Specifications
  This appendix provides the technical specifications for the Router.

- Appendix J: Warranty Information
  This appendix supplies the warranty information for the Router..

- Appendix K: Regulatory Information
  This appendix supplies the regulatory information regarding the Router.

- Appendix L: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning your Wireless Network

The Router's Functions

Simply put, a router is a network device that connects two networks together.

In this instance, the Router connects your Local Area Network (LAN), or the group of PCs in your home or office, to the Internet. The Router processes and regulates the data that travels between these two networks.

The Router's NAT feature protects your network of PCs so users on the public, Internet side cannot "see" your PCs. This is how your network remains private. The Router protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate PC on your network. The Router inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

Remember that the Router's ports connect to two sides. The LAN ports connect to the LAN, and the Internet port connects to the Internet. The LAN and Internet ports transmit data at 10/100Mbps.

Figure 2-1: Network

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including PCs, print servers, and routers, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices. You can assign static IP addresses or use the Router to assign IP addresses dynamically.

Static IP Addresses

A static IP address is a fixed IP address that you assign manually to a PC or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server PCs or print servers.

***LAN**: the computers and networking products that make up your local network*

NOTE: Since the Router is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Router uses NAT technology, the only IP address that can be seen from the Internet for your network is the Router's Internet IP address. However, even this Internet IP address can be blocked, so that the Router and network seem invisible to the Internet—see the Block WAN Requests description under Filters in "Chapter 7: The Router's Web-based Utility."

If you use the Router to share your cable or DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Router. You can get that information from your ISP.

Dynamic IP Addresses

A dynamic IP address is automatically assigned to a device on the network, such as PCs and print servers. These IP addresses are called "dynamic" because they are only temporarily assigned to the PC or device. After a certain time period, they expire and may change. If a PC logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address.

DHCP (Dynamic Host Configuration Protocol) Servers

PCs and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The PC or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated PC on the network or another network device, such as the Router. By default, the Router's DHCP Server function is enabled.

If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Router, see the DHCP section in "Chapter 6: The Router's Web-based Utility."

Why do I need a VPN?

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

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

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

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

1) MAC Address Spoofing

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

2) Data Sniffing

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

3) Man in the middle attacks

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

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

What is a VPN?

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

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

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates

a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Router using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:

•VPN Router to VPN Router

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

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

VPN Router to VPN Router

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

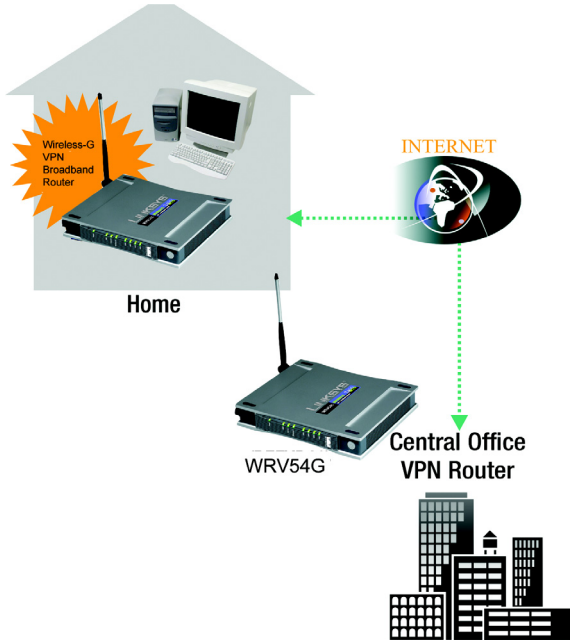

Figure 2-2:

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

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

The following is an example of a computer-to-VPN Router VPN. (See Figure 2-3.) In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software that supports IPSec and connects to the VPN Router at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.

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

Figure 2-3:

Chapter 3: Getting to Know the Wireless-G VPN Broadband Router

The Back Panel

The Router's ports, where a network cable is connected, are located on the back panel.

Figure 3-1: Back Panel

Internet The **Internet** port connects to your modem.

LAN (1-4) The **LAN** (Local Area Network) ports connect to your PC and other network devices.

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

Reset Button There are two ways to Reset the Router's factory defaults. Either press the **Reset Button**, for approximately ten seconds, or restore the defaults from the Password tab in the Router's Web-Based Utility.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com for more information about products that work with the Router.

Important: Resetting the Router will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Router if you want to retain these settings.

The Front Panel

The Router's LEDs, where information about network activity is displayed, are located on the front panel.

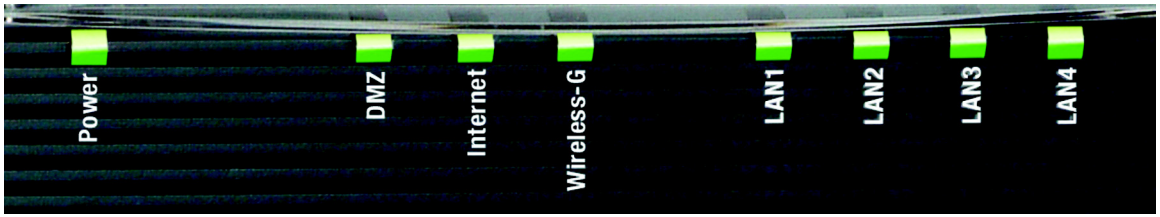

Figure 3-2: Front Panel

Power Green. The **Power** LED lights up when the Access Point is powered on.

DMZ Red. The **DMZ** LED indicates the Access Point's self- diagnosis mode during boot-up and restart. It will turn off upon completing the diagnosis. If this LED stays on for an abnormally long period of time, refer to Appendix A: Troubleshooting.

Internet Green. The **Internet** LED lights whenever there is a successful wireless connection. If the LED is flickering, the Router is actively sending or receiving data to or from one of the devices on the network.

Wireless-G Green. The **Wireless-G** LED lights whenever there is a successful wireless connection.

LAN (1-4) Green. The **LAN** LED serves two purposes. If the LED is continuously lit, the Router is successfully connected to a device through the LAN port. If the LED is flickering, it is an indication of any network activity.

Chapter 4: Connecting the Wireless-G Broadband Router

Overview

The Router's setup consists of more than simply plugging hardware together. You will have to configure your networked PCs to accept the IP addresses that the Router assigns them (if applicable), and you will also have to configure the Router with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information for your modem with you after installing your broadband connection. If not, you can call your ISP to request that data.

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

If you want to use a PC with an Ethernet adapter to configure the Router, continue to "Wired Connection to a PC." If you want to use a PC with a wireless adapter to configure the Router, continue to "Wireless Connection to a PC."

Wired Connection to a PC

1. Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
2. Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router (see Figure 4-1), and the other end to an Ethernet port on a PC.
3. Repeat this step to connect more PCs, a switch, or other network devices to the Router.
4. Connect a different Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel (see Figure 4-2). This is the only port that will work for your modem connection.
5. Power on the cable or DSL modem.
6. Connect the power adapter to the Router's Power port (see Figure 4-3), and then plug the power adapter into a power outlet.
   - The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, then it will light up steady when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."
7. Power on one of your PCs that is connected to the Router.

Wireless Connection to a PC

If you want to use a wireless connection to access the Router, follow these instructions:

1. Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
2. Connect an Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel (see Figure 4-2). This is the only port that will work for your modem connection.
3. Power on the cable or DSL modem.
4. Connect the power adapter to the Power port (see Figure 4-3), and then plug the power adapter into a power outlet.

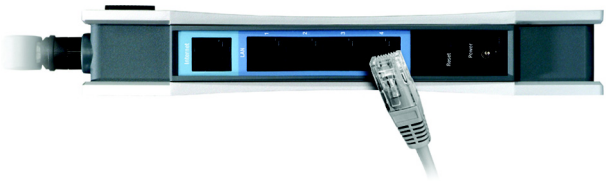

Figure 4-1:

Figure 4-2:

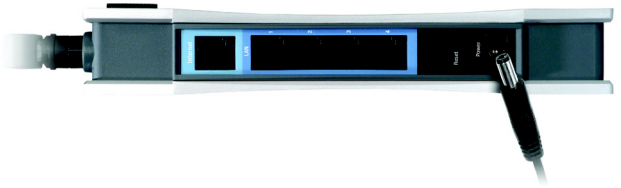

Figure 4-3:

NOTE: IYou should always plug the Router's power adapter into a power strip with surge protection.

NOTE: IYou should always change the SSID from its default, linksys, and enable WEP encryption.

- The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, then light up steady when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."

5. Power on one of the PCs on your wireless network(s).

6. For initial access to the Router through a wireless connection, make sure the PC's wireless adapter has its SSID set to linksys-g (the Router's default setting), and its WEP encryption is disabled. After you have accessed the Router, you can change the Router and this PC's adapter settings to match the your usual network settings.

The Router's hardware installation is now complete.

Go to "Chapter 5: Configuring the PCs."

Chapter 5: Configuring the PCs

Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the Router.

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

First, find out which Windows operating system your computer is running. You can find out by clicking the **Start** button. Read the side panel of the Start menu to find out which operating system your PC is running.

You may need to do this for each computer 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 Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you've configured your computers, continue to "Chapter 6: Using the Router's Web-Based Utility."

Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network** icon.
2. On the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter, as shown in Figure 5-1. 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. Click the **Properties** button.
3. Click the **IP Address** tab. Select **Obtain an IP address automatically**. (See Figure 5-2.)

IMPORTANT: Important: By default Windows 98, 2000, Me, and XP has TCP/IP installed and set to obtain an IP address automatically. If your PC does not have TCP/IP installed, click Start and then Help. Search for the keyword TCP/IP. Then follow the instructions to install TCP/IP.

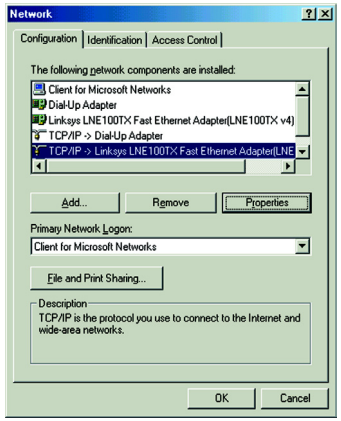

Figure 5-1: Configuration Tab

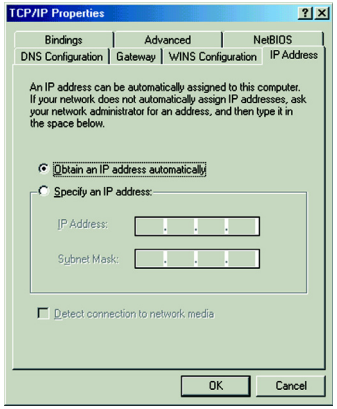

Figure 5-2: IP Address Tab

4. Now click the **Gateway** tab, and verify that the Installed Gateway field is blank. Click the **OK** button.

5. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (if "D" is the letter of your CD-ROM drive).

6. 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: Using the Router's Web-Based Utility."

Configuring Windows 2000 PCs

1. Click the **Start** button. Select Settings and click the **Control Panel** icon. 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**. Click the **Properties** button. (See Figure 5-3.)

3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight Internet Protocol (TCP/IP), and click the **Properties** button. (See Figure 5-4.)

4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration. (See Figure 5-53.)

5. Restart your computer.

Go to "Chapter 6: Using the Router's Web-Based Utility."

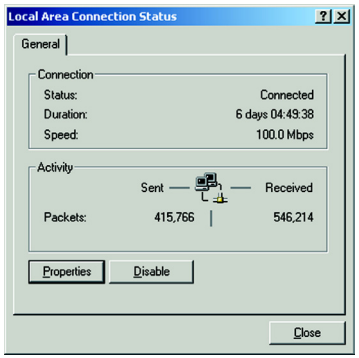

Figure 5-3: Properties

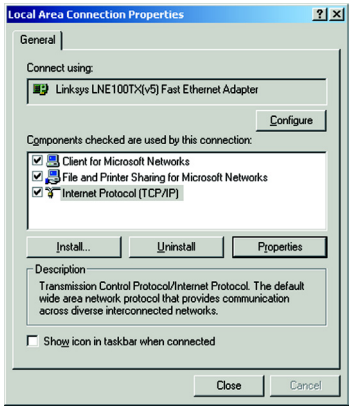

Figure 5-4: TCP/IP

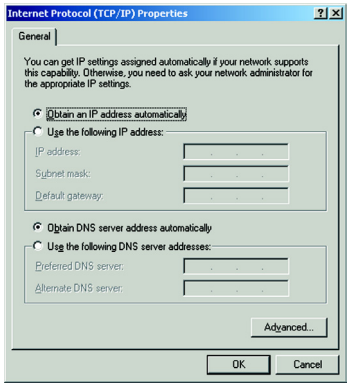

Figure 5-5: IP Address

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 for Windows 2000.

1. Click the **Start** button and then the **Control Panel** icon. Click the **Network and Internet Connections** icon. Then click 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 5-6.)

3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. (See Figure 5-7.)

4. Select **Obtain an IP address automatically**. (See Figure 5-8.) Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.

Go to "Chapter 6: Using the Router's Web-Based Utility."

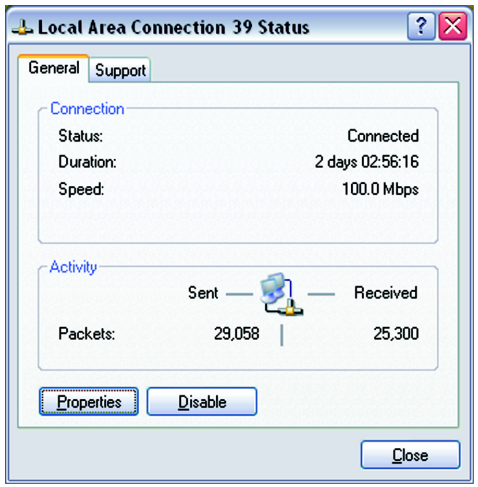

Figure 5-6: Properties

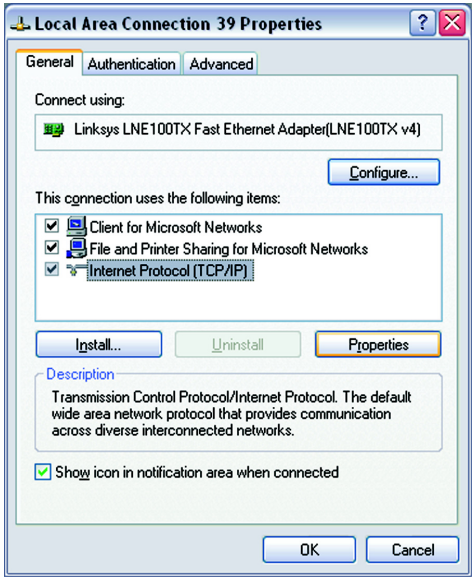

Figure 5-7: TCP/IP