LINKSYS®

A Division of Cisco Systems, Inc.

2.4 GHz 54Mbps Wireless-G

VPN Broadband Router

User Guide

WIRELESS

Model No. **WRV54G ver. 2**

CISCO SYSTEMS

Copyright and Trademarks

Specifications are subject to change without notice. Instant Etherfast, Linksys, and the Linksys logo are registered trademarks of Linksys Group, Inc. Other brands and product names are trademarks or registered trademarks of their respective holders. Copyright © 2003 Linksys. All rights reserved.

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 1
Welcome 1
What's in this Guide? 2
Chapter 2: Planning your Wireless Network 4
The Router's Functions 4
IP Addresses 4
Why do I need a VPN? 5
What is a VPN? 6
Chapter 3: Getting to Know the Wireless-G VPN Broadband Router 9
The Back Panel 9
The Front Panel 10
Chapter 4: Connecting the Wireless-G Broadband Router 11
Overview 11
Wired Connection to a PC 12
Wireless Connection to a PC 12
Chapter 5: Configuring the PCs 14
Overview 14
Configuring Windows 98 and Millennium PCs 14
Configuring Windows 2000 PCs 15
Configuring Windows XP PCs 16
Chapter 6: Configuring the Router 18
Overview 18
How to Access the Web-based Utility 20
The Setup Tab 20
The Wireless Tab 27
The Security Tab 31
The Access Restrictions Tab 36
The Applications and Gaming Tab 38
The Administration Tab 42
Status 46
Appendix A:Troubleshooting 49
Common Problems and Solutions 49

Frequently Asked Questions 57
Appendix B: Wireless Security 64
A Brief Overview 64
What Are The Risks? 64
Appendix C: Configuring IPSec between a Windows 2000 PC and the Router 71
Introduction 71
Environment 71
How to Establish a Secure IPSec Tunnel 72
Windows 98 or Me Instructions 82
Windows 2000 or XP Instructions 83
Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter 84
Appendix E: SNMP Functions 84
Appendix F: Upgrading Firmware 85
Appendix G: Windows Help 86
Appendix H: Glossary 87
Appendix I: Specifications 93
Appendix J: Warranty Information 95
Appendix K: Regulatory Information 96
Appendix L: Contact Information 98

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

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

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.

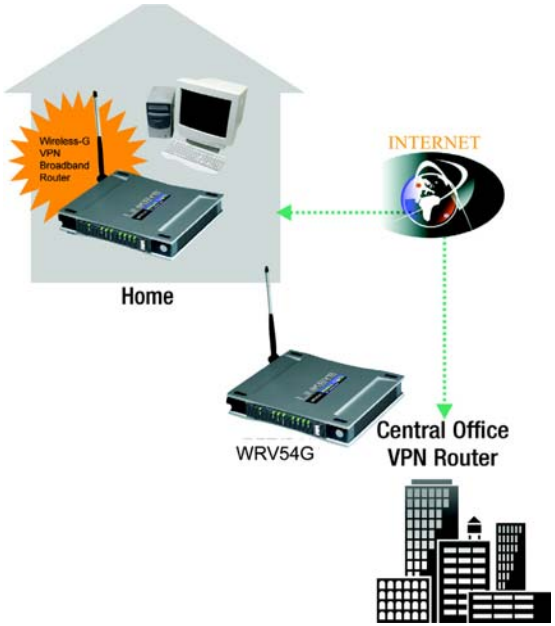


Figure 2-2:

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

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.

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.

The Front Panel

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

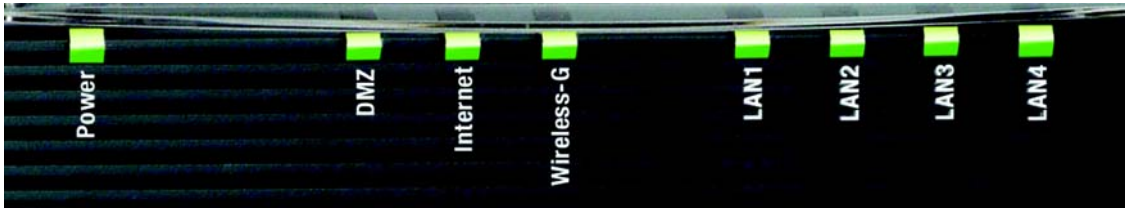


Figure 3-2: Front Panel

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.

Figure 4-1:

Figure 4-2:

Figure 4-3:

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.

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.

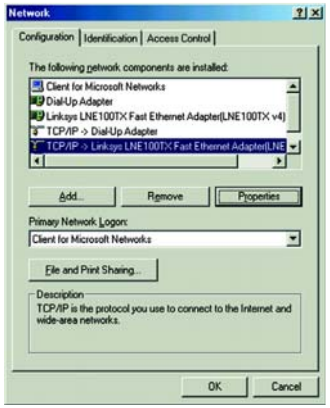


Figure 5-1: Configuration Tab

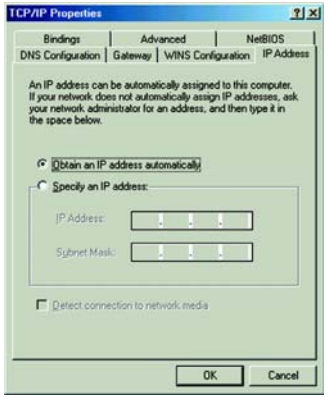


Figure 5-2: IP Address Tab

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

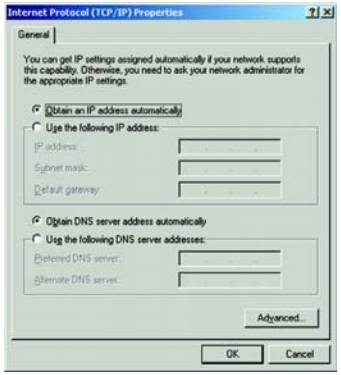


Figure 5-5: IP Address

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

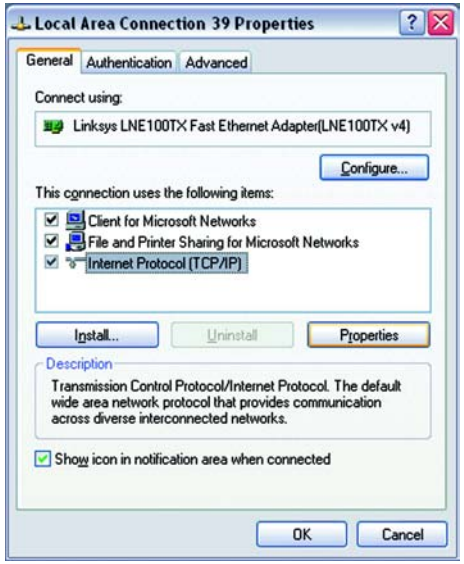


Figure 5-7: TCP/IP

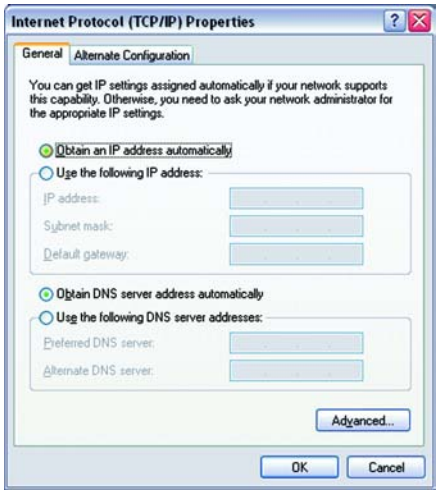


Figure 5-8: IP Address

Chapter 6: Configuring the Router

Overview

Linksys recommends using the Setup CD-ROM for first-time installation of the Router and setting up additional computers. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then follow the steps in this chapter and use the Router's web-based utility to configure the Router. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users only have to use the following screens of the Utility:

• Basic Setup. On the Basic Setup screen, enter the settings provided by your ISP.

• Management. Click the **Administration** tab and then the **Management** tab. The Router's default password is admin. To secure the Router, change the Password from its default.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Setup

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

Wireless

- Basic Wireless Settings. You can choose your Wireless Network Mode and Wireless Security on this screen.
- Wireless Network Access. This screen displays your network access list.

Note: The Router is designed to function properly after connecting the Router to your network. This chapter is provided solely for those who wish to perform more advanced

Have You: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to Appendix D: Windows Help for more information on TCP/IP.

Note: For added security, you should change the password through the Administration screen of the web-based utility.

NAT (Network Address Translation): *NAT technology translates IP addresses of a local area network to a different IP address for the Internet.*

- Advanced Wireless Settings. On this screen you can access the Advanced Wireless features of Authentication Type, Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, RTS Threshold, and Fragmentation Threshold.

Security

- Filter. To block specific users from Internet access, you can set up IP address, port, and MAC address filtering on the Filter screen.
- VPN. To enable or disable IPSec, L2TP, and/or PPTP Pass-through, and set up VPN tunnels, use this screen.
- 802.1x. Use this screen to set up RADIUS authentication.

Access Restrictions

- Access Restriction. This screen allows you to prevent or permit only certain users from attaching to your network.

Applications & Gaming

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

Administration

- Management. On this screen, alter router access privileges and UPnP settings.
- Log. If you want to view or save activity logs, click this tab.
- Diagnostics. Use this screen to check the connection between your Router and PC.
- Factory Defaults. If you want to restore the Router's factory defaults, then use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Router's firmware.

Beacon Interval :*The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.*

DTIM (Delivery Traffic Indication Message): *A message included in data packets that can increase wireless efficiency.*

RTS (Request To Send): *A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.*

Fragmentation: *Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.*

Status

- Router. This screen provides status information about the Router.
- Local Network. This provides status information about the local network.

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, 192.168.1.1, in the Address field. Then press Enter.

A password request page, shown in Figure 6-1 will appear. (non-Windows XP users will see a similar screen.) Enter **admin** (the default user name) in the User Name field, and enter **admin** (the default password) in the Password field. Then click the **OK** button.

Figure 6-1: Password Screen

The Setup Tab

The Basic Setup Tab

The first screen that appears is the Basic Setup tab. (See Figure 6-2.) This tab allows you to change the Router's general settings. Change these settings as described here and click the **Save Settings** button to save your changes or **Cancel Changes** to cancel your changes.

Internet Setup

- Internet Connection Type. The Router supports four connection types: Automatic Configuration - DHCP (the default connection type), PPPoE, Static IP, and PPTP. Each Basic Setup screen and available features will differ depending on what kind of connection type you select.

  Automatic Configuration - DHCP

  By default, the Router's Configuration Type is set to Automatic Configuration - DHCP, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.

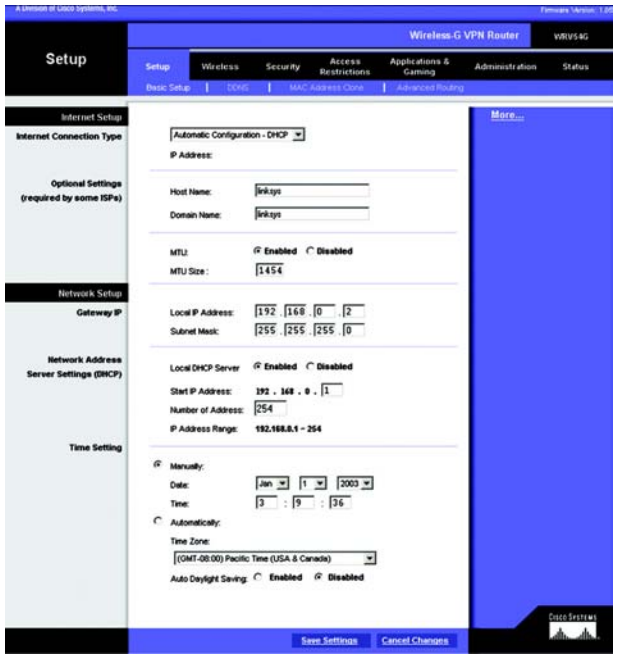


Figure 6-2: Setup Tab/DHCP Internet Connection Type

Static (See Figure 6-3.)

If you are required to use a permanent IP address to connect to the Internet, then select Static IP.

- IP Address. This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.
- Primary DNS. (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

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

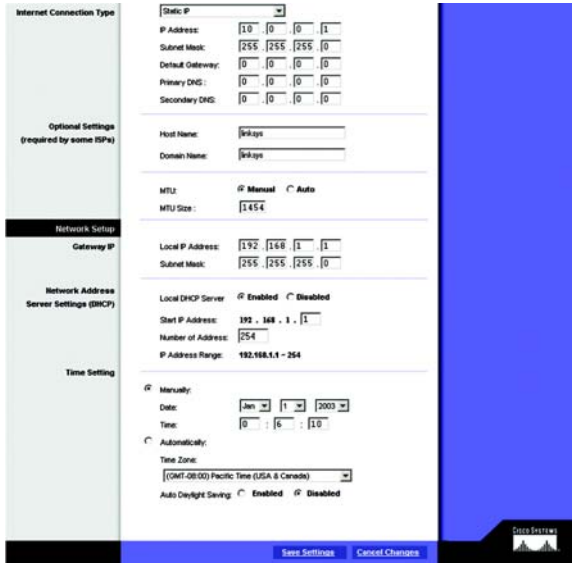


Figure 6-3: Static Internet Connection Type

PPPoE (See Figure 6-4.)

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

- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Aliv**e. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

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

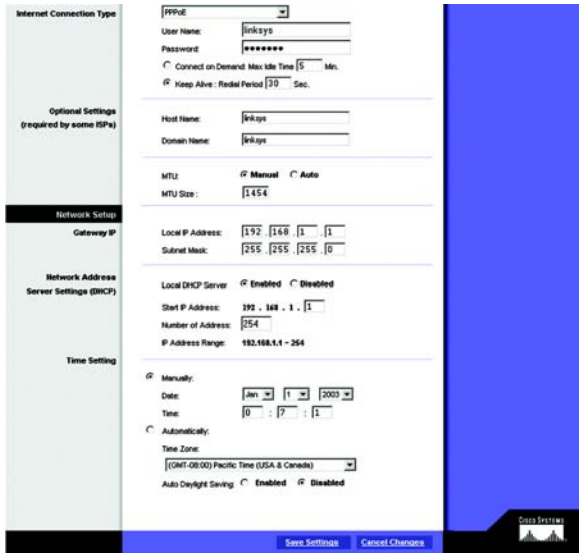


Figure 6-4: PPPoE Internet Connection Type

PPTP (See Figure 6-5.)

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only (see Figure 6-8).

- Internet IP Address. This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the Default Gateway Address.
- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

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

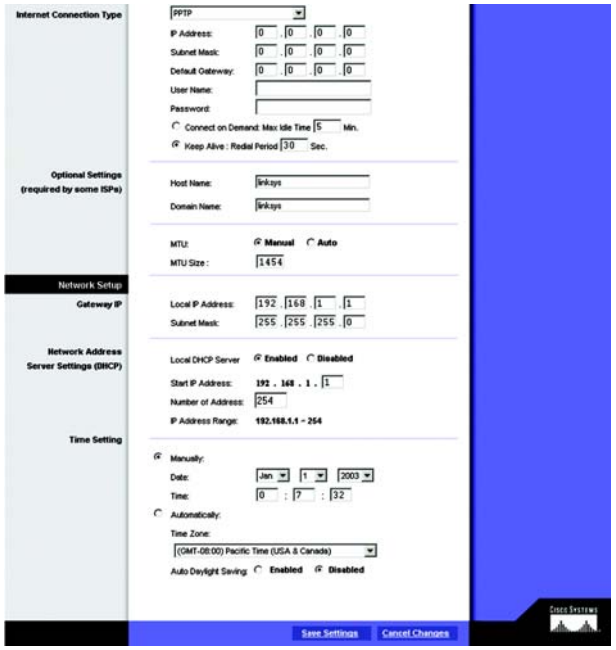


Figure 6-5: PPTP Internet Connection Type

Optional Settings (Required by some ISPs)

- Host Name and Domain Name. These fields allow you to supply a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.
- MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Enabled** and enter the value desired. It is recommended that you leave this value in the

1200 to 1500 range. For most DSL users, it is recommended to use the value 1492. By default, MTU is set at 1500 when disabled.

Network Setup

- Gateway IP. The values for the Router's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.
  - Local IP Address. The default value is 192.168.1.1.
  - Subnet Mask. The default value is 255.255.255.0.
  - Network Address Server Settings (DHCP). A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each PC on your network for you. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.
  - Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to Disable. If you disable DHCP, remember to assign a static IP address to the Router.
  - Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Router is 192.168.1.1.
  - Number of Address. 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 6-9, add 100 to 50, and the range is 192.168.1.100 to 192.168.1.149.
  - DHCP Address Range. The range of DHCP addresses is displayed here.
- Time Setting. This is where you set the time for your Router. You can set the time and date manually or automatically, by setting the time zone.

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

The DDNS Tab

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

Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com.

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** in the drop-down menu. (See Figure 6-6.) If your DDNS service is provided by TZO, then select **TZO.com**. (See Figure 6-7.) The features available on the DDNS screen will vary, depending on which DDNS service provider you use.

DynDNS.org

- User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
- Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, it will change.
- Status. The status of the DDNS service connection is displayed here.

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

Figure 6-6: DynDNS.org

TZO.com Tab

- Email Address, TZO Password Key, and Domain Name. Enter the Email Address, TZO Password Key, and Domain Name of the service you set up with TZO.
- Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.
- Status. The status of the DDNS service connection is displayed here.

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

Figure 6-7: TZO.com

MAC Address Clone Tab (See Figure 6-8.)

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

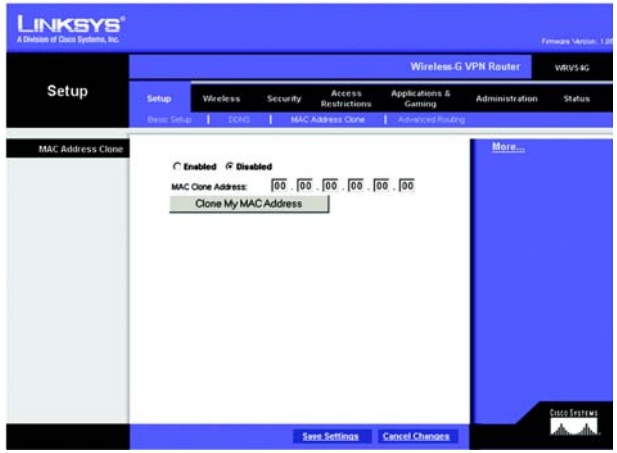


Figure 6-8: MAC Address Clone

MAC Clone

- MAC Clone Service. To use MAC address cloning, select **Enable**.
- MAC Address. To manually clone a MAC address, enter the 12 digits of your adapter's MAC address in the on-screen fields (see Figure 6-25). Then click the **Save Settings** button.
- Clone My MAC Address. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click the **Clone My MAC Address** button. The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone tab.

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

Advanced Routing Tab

The Advanced Routing screen allows you to configure the dynamic routing and static routing settings. (See Figure 6-9.)

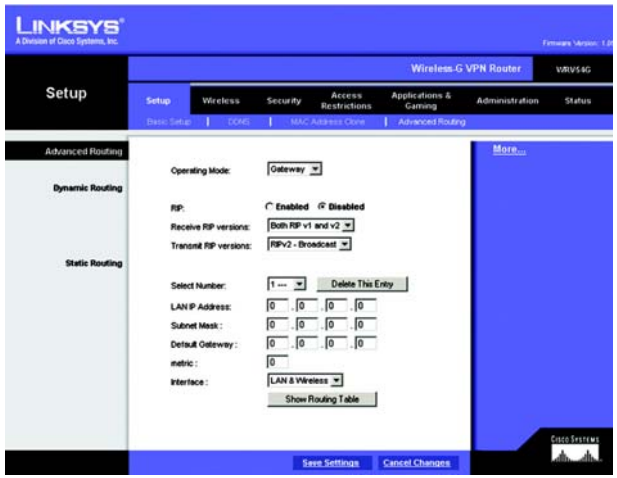


Figure 6-9: Advanced Routing

Advanced Routing

- Operating Mode. Select **Gateway** or **Router** for the Operating Mode from the drop-down menu.
- Dynamic Routing. With Dynamic Routing you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.
- Receive RIP Version To use dynamic routing for reception of network data, select the protocol you want: **RIP1** or **RIP2**.
- Transmit RIP Version. To use dynamic routing for transmission of network data, select the protocol you want: **RIP1, RIP1-Compatible, or RIP2**.

Static Routing

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

- Select Number. Select the **number** of the static route from the drop-down menu. The Router supports up to 20 static route entries.
- Delete This Entry. If you need to delete a route, select its **number** from the drop-down menu, and click the **Delete Entry** button.
- LAN IP Address. The LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router.
- Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the Subnet Mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.
- Default Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Router and the remote network or host.
- metric. This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as PCs, print servers, routers, etc.
- Interface. Select **LAN & Wireless** or **Internet**, depending on the location of the static route's final destination.
- Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your LAN. For each route, the Destination LAN IP address, Subnet Mask, Default Gateway, and Interface are displayed. Click the **Refresh** button to update the information. See Figure 6-10.

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

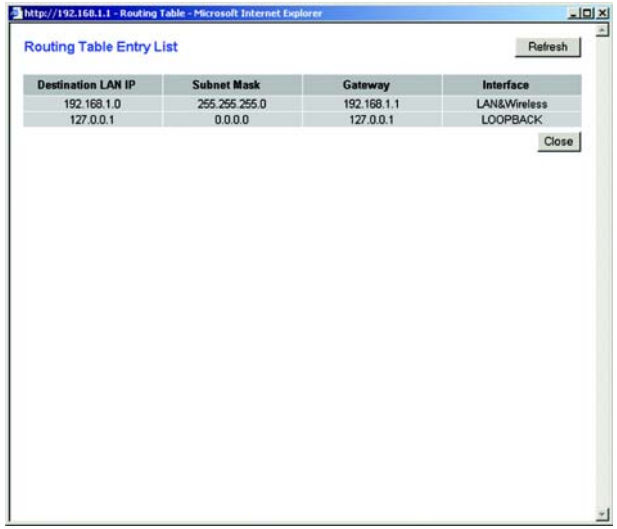


Figure 6-10: Routing Table

The Wireless Tab

Basic Wireless Settings (See Figure 6-11.)

This screen allows you to choose your wireless network mode and wireless security.

Wireless Network

- Wireless Network Mode. If you have Wireless-G and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you want to disable wireless networking, select **Disable**.
- Wireless Network Name. Enter the **Wireless Network Name (SSID)** into the field. The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. For added security, Linksys recommends that you change the default SSID (linksys) to a unique name of your choice.
- Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly.

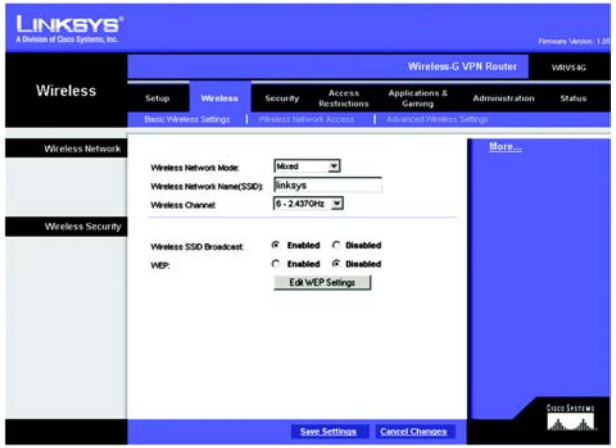


Figure 6-11: Basic Wireless

Wireless Security

- Wireless SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

- WEP. An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices-Wireless-G and 802.11b-in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. To enable WEP encryption, click the **Enabled** radio button. Then click the **Edit WEP Settings** button to configure the WEP settings. To disable WEP encryption, keep the default setting, **Disabled**.

WEP (See Figure 6-12.)

The WEP screen allows you to configure your WEP settings. WEP encryption should always be enabled to increase the security of your wireless network. Default Transmit Key Select which WEP key (1-4) will be used when the Router sends data. Make sure the receiving device is using the same key.

- WEP Encryption. Select the level of WEP encryption you wish to use, 64-bit 10 hex digits or 128-bit 26 hex digits. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

- Passphrase. Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- Keys 1-4. WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

  If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.

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

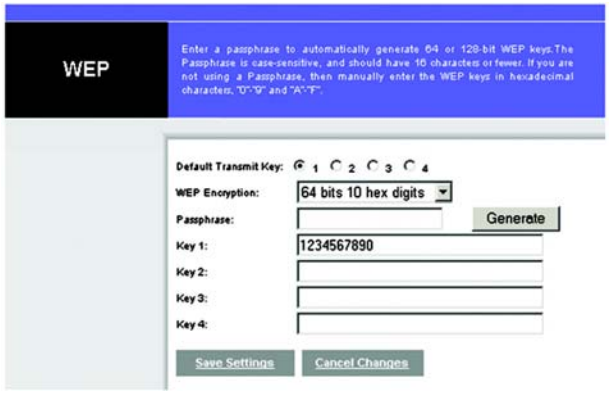


Figure 6-12: WEP

Wireless Network Access (See Figure 6-13.)

Wireless Network Access. If this function is enabled, only the computers on the list will be allowed access to the wireless network. To add a computer to the network, click the **Permit to access** button, and enter the MAC address in the fields. Click the **Select MAC Address From Networked Computers** button, and the screen in Figure 6-15 will appear.

Select the **MAC Address** from the list and click the **Select** button.

To prevent access, click the **Prevent from accessing** button, then click **Select MAC Address from the list.** From the screen in Figure 6-14, select the **MAC Address** from the list, and click the **Select** button.

Click the **Refresh** button if you want to refresh the screen. Click the **Close** button to return to th previous screen.

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

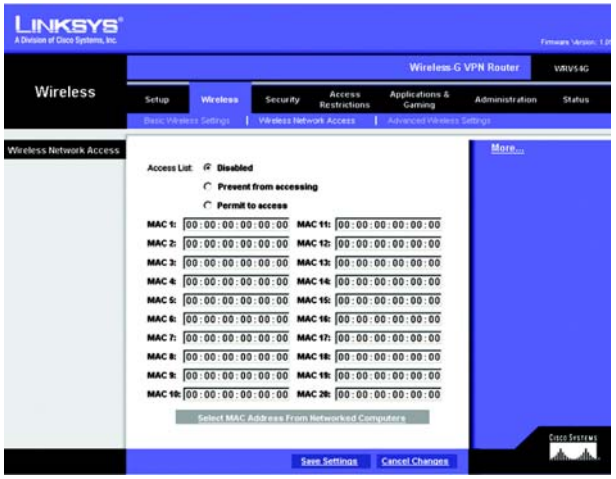


Figure 6-13: Wireless Network Access

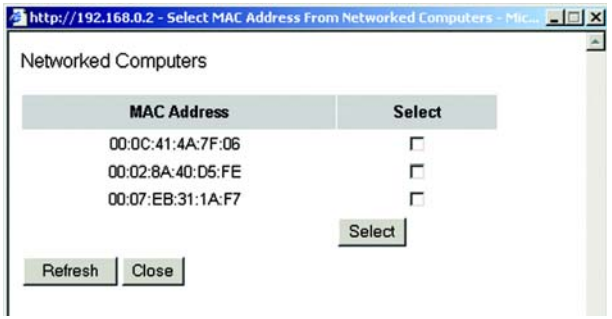


Figure 6-14: Networked Computers

Advanced Wireless Settings (See Figure 6-15.)

On this screen you can access the Advanced Wireless features, including Authentication Type, Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, RTS Threshold, and Fragmentation Threshold.

- Authentication Type. The default is set to Auto, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. If you want to use only Shared Key authentication, then select **Shared Key**.
- Basic Data Rates. Select **1-2 Mbps**, **All**, or **Default**, from the drop-down menu.
- Control Tx Rates. The default transmission rate is Auto. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.
- Beacon Interval. The default value is 100. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.
- DTIM Interval The default value is 3. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
- RTS Threshold This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
- Fragmentation Threshold This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

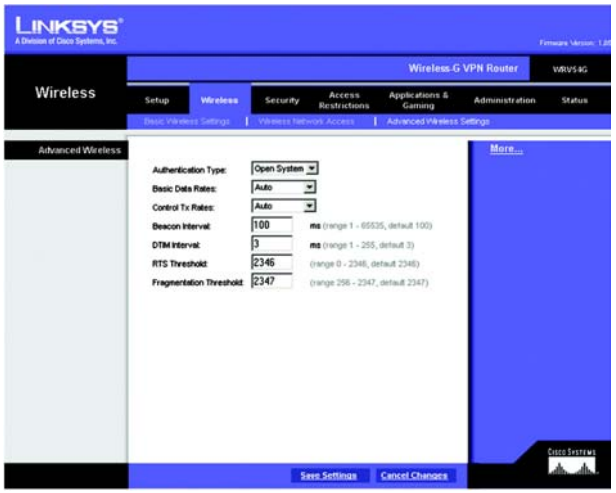


Figure 6-15: Advanced Wireless Settings

The Security Tab

Firewall

When you click the Security tab, you will see the Firewall screen (see Figure 6-16). This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests and/or multicasting.

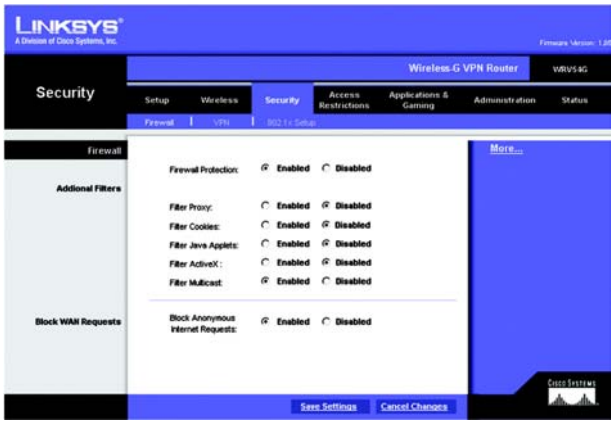


Figure 6-16: Firewall

When you click the Security tab, you will see the Firewall screen (see Figure 6-16). This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests and/or multicasting.

- Firewall. To add Firewall Protection, click **Enabled**. If you do not want Firewall Protection, click **Disabled**.
- Filter Proxy. Use of WAN proxy servers may compromise the Router's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.
- Filter Cookies. A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.
- Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click **Enabled**.
- Filter 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. To enable ActiveX filtering, click **Enabled**.
- Filter Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enabled** to filter multicasting, or **Disabled** to disable this feature.
- Block Anonymous Internet Requests. This keeps your network from being “pinged” or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to work their way into your network. Select **Enabled** to block anonymous Internet requests, or **Disabled** to allow anonymous Internet requests.

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

VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. This connection is very specific as far as its settings are concerned; this is what creates the security. The VPN screen, shown in Figure 6-17, allows you to configure your VPN settings to make your network more secure.

Figure 6-17: VPN

VPN PassThrough

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

- PPTP Pass Through. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.

- L2TP Pass Through. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by to enable the operation of a virtual private network (VPN) over the Internet.To allow L2TP Passthrough, click the **Enabled** button. To disable L2TP Passthrough, click the **Disabled** button.

VPN Tunnel

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

- To establish this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to 50 simultaneous tunnels. Then click **Enabled** to enable the tunnel. Once the tunnel is enabled, enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

- Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your LAN that can access the tunnel. The Remote Secure Group is the computer (s) on the remote end of the tunnel that can access the tunnel. Enter the **IP Address** and **Subnet Mask** of the local VPN Router in the fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).

- Remote Security Gateway. The Remote Security Gateway is the VPN device, such as a second VPN Router, on the remote end of the VPN tunnel. Enter the IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the

settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Router, but the IP Address of the remote VPN Router or device with which you wish to communicate.

- Encryption. Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable. In Figure 6-18, DES (which is the default) has been selected.

- Authentication. Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication. In Figure 6-18, MD5 (the default) has been selected.

- Key Management. Key Exchange Method. Select **Auto (IKE)** or **Manual** for the Key Exchange Method. The two methods are described below.

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

  Manual (See Figure 6-18.)
  Select **Manual,** then select the Encryption Algorithm from the drop-down menu. Enter the Encryption Key in the field (If, for your Encryption Algorithm, you chose DES, enter 16 hexadecimal characters. If you chose 3DES, enter 48 hexadecimal characters.) Select the Authentication Algorithm from the drop-down menu. Enter the Authentication Key in the field (If, for your Authentication Algorithm, you chose MD5, enter 32 hexadecimal characters. If you chose SHA1, enter 40 hexadecimal characters.) . Enter the Inbound and Outbound SPIs in the respective fields.

- Status. Click the **Advanced VPN Tunnel Setup** key and the Advanced VPN Tunnel Setup screen will appear. See Figure 6-20.

Figure 6-18: Manual Key Management

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

From the Advance VPN Tunnel Setup screen, shown in Figure 6-19, you can adjust the settings for specific VPN tunnels.

Figure 6-19: Advanced VPN Tunnel Setup

Phase 1

- Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.
- Operation Mode. There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device.
- Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.
- Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- Key Life Time. 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

- Encryption. The encryption method selected in Phase 1 will be displayed.
- Authentication. The authentication method selected in Phase 1 will be displayed.
- 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 Life Time. 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 Options

- Unauthorized IP Blocking. Click **Enabled** to block unauthorized IP addresses. Enter in the Rejects Number field to specify how many times IKE must fail before blocking that unauthorized IP address. Enter the length of time that you specify (in seconds) in the Block Period field.

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

Security

802.1x (See Figure 6-20.)

- Radius Server IP Address. Enter the Radius Server IP Address in the fields.
- Radius Server Port. Enter the Radius Server Port in the field.
- Shared Secret. Enter the Shared Secret in the field.
- Authentication Type. To enable EAP-TLS, click EAP-TLS. To enable EAP-TTLS, click EAP-TTLS. To enable EAP-MD5, click **EAP-MD5**,. To disable authentication, click **Disable**.
- WEP Settings. Click the **WEP Settings** button to edit the settings and Figure 7-22 will appear.
- Dynamic WEP Key Length. Select **64** or **128** bits from the drop-down menu.
- Key Renewal Timeout. Enter the time in seconds for key renewal.
- Port Inactivity Timeout. Enter the time in seconds for port inactivity.
- Port Connectivity Timeout. Enter the time in seconds for port connectivity.

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

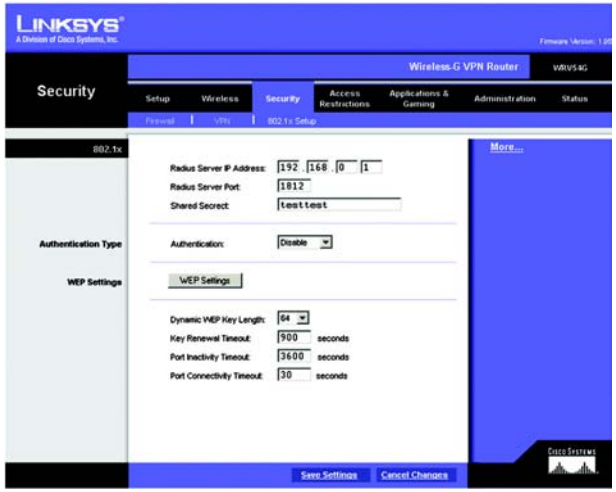


Figure 6-20: 802.1x

WEP

The WEP screen allows you to configure your WEP settings. (See Figure 6-21.) WEP encryption should always be enabled to increase the security of your wireless network. Default Transmit Key. Select which WEP key (1-4) will be used when the Router sends data. Make sure that the receiving device is using the same key.

- WEP Encryption. Select the level of WEP encryption you wish to use, **64-bit 10 hex digits** or 1**28-bit 26 hex digits.** Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

- Passphrase. Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- Keys 1-4. WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

  If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.

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

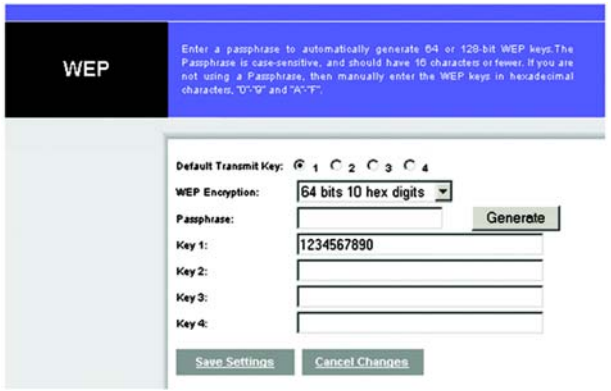


Figure 6-21: WEP

The Access Restrictions Tab

Access Restriction

The Access Restrictions tab, shown in Figure 6-22, allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

- Internet Access Policy. Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the **Delete** button. To see a summary of all Policies, click the **Summary** button.

  The summaries are listed on this screen, shown in Figure 7-23, with their name and settings. To return to the Filters tab, click the **Close** button.

- Enter Policy Name. Policies are created from the fields presented here.

  To create an Internet Access policy:

1. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.

Figure 6-22: Access Restriction

2. Click the **Edit List** button. This will open the List of PCs screen, shown in Figure 6-24. From this screen, you can enter the IP address or MAC address of any PC to which this policy will apply. You can even enter ranges of PCs by IP address. Click the **Apply** button to save your settings, the **Cancel** button to undo any changes, and the **Close** button to return to the Filters tab.

3. If you wish to Deny or Allow Internet access for those PCs you listed on the List of PCs screen, click the option.

4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add Service** button to open the Service screen, shown in Figure 6-25, and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.

5. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.

6. Lastly, click the **Save Settings** button to activate the policy.

To create an Inbound Traffic Policy

1. Enter a Policy Name in the field provided. Select **Inbound Traffic** as the Policy Type.

2. Enter the **IP Address** from which you want to block. Select the Protocol: **TCP**, **UDP**, or **Both**. Enter the **port** number or select **Any**. Enter the IP Address to which you want to block.

3. Select **Deny** or **Allow** as appropriate.

4. By selecting the appropriate setting next to Days and Time, choose when the Inbound Traffic will be filtered.

Lastly, click the **Save Settings** button to activate the policy.

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

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by Keyword fields.

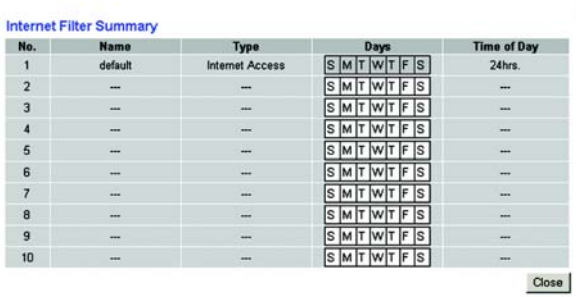


Figure 6-23: Internet Filter Summary

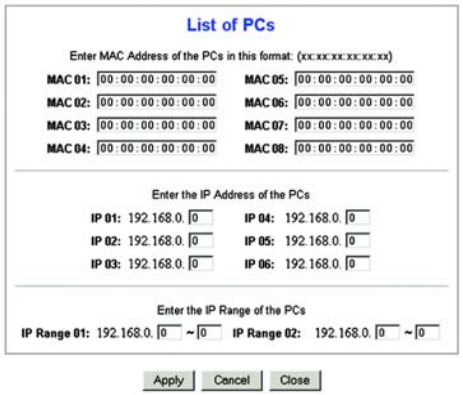


Figure 6-24: List of PCs

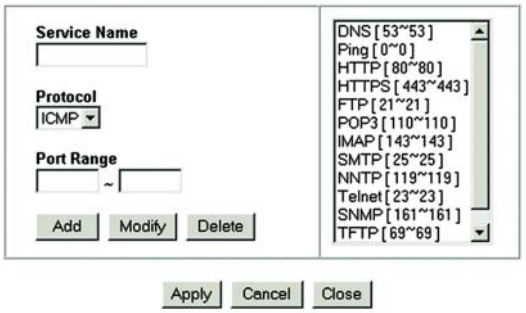


Figure 6-25: Blocked Services

The Applications and Gaming Tab

Port Range Forwarding

The Port Forwarding screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) (See Figure 6-26.)

When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Application. Enter the name you wish to give each application.
- Start and End. Enter the starting and ending numbers of the port you wish to forward.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address and Click **Enabled**.

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

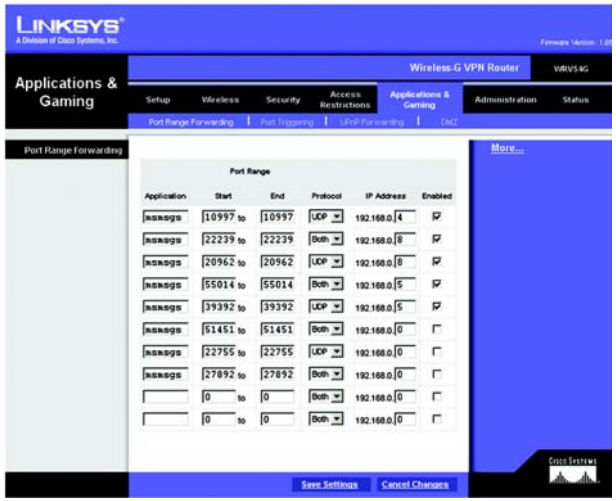


Figure 6-26: Port Range Forwarding

Port Triggering

Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the Router will watch outgoing data for specific port numbers. (See Figure 6-27.) The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

- Application. Enter the name you wish to give each application.
- Start Port and End Port. Enter the starting and ending Triggered range numbers and the Forwarded Range numbers of the port you wish to forward.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- Click **Enabled**.

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

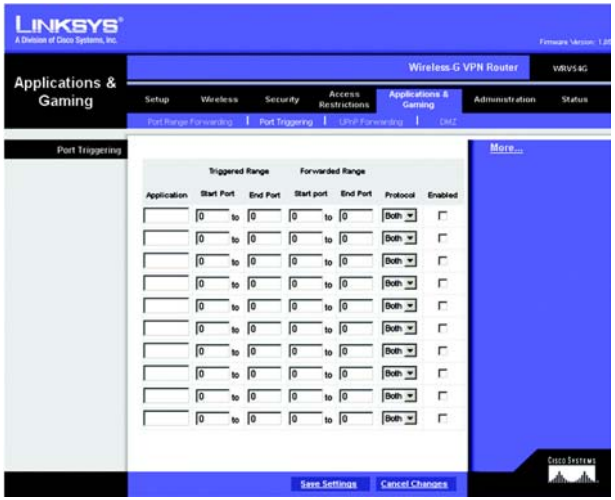


Figure 6-27: Port Triggering

UPnP Forwarding

The UPnP screen provides options for customization of port services for applications. (See Figure 6-28.)

Enter the Application in the field. Then, enter the External and Internal Port numbers in the fields. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**. Enter the IP Address in the field. Click **Enabled** to enable UPnP Forwarding for the chosen application.

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

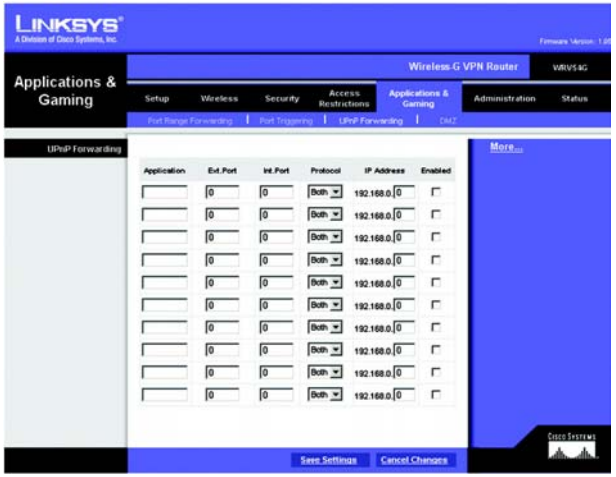


Figure 6-28: UPnP Forwarding

DMZ

The DMZ screen (see Figure 6-29) allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing, through Software DMZ, or a user can use LAN Port 4 as a DMZ Port, through Hardware DMZ. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.

Figure 6-29: DMZ

- Software DMZ. This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- DMZ Host IP Address. To expose one PC, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter." Deactivate DMZ by entering a 0 in the field.
- Hardware DMZ. This feature allows a user to use LAN Port 4 as a DMZ Port. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- Hardware DMZ IP Address. Enter the IP Address of the computer in the fields.
- Hardware DMZ Netmask. Enter the Netmask in the fields.
- Destination IP Address. Enter the IP Address of the destination in the fields.
- Subnet Mask. Enter the Subnet Mask of the destination in the fields.
- Default Gateway. Enter the Default Gateway in the fields.
- metric. Enter the metric in the field.

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

The Administration Tab

Management

The Management screen, shown in Figure 6-30, allows you to change the Router's access settings as well as configure the SNMP and UPnP (Universal Plug and Play) features.

Figure 6-30: Management

Router Password

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

- User Name. Enter the default **admin**.
- Router Password. It is recommended that you change the default password to one of your choice.
- Re-enter to confirm. Re-enter the Router's new Password to confirm it.

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

- Remote Management. This feature allows you to manage the Router from a remote location, via the Internet. To enable Remote Management, click **Enabled**.
- Mangagement Port. Select the port number you will use to remotely access the Router from the drop-down menu.

SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**.

- Identification. In the Contact field, enter contact information for the Router. In the Device Name field, enter the name of the Router. In the Location field, specify the area or location where the Router resides.
- Get Community. Enter the password that allows read-only access to the Router's SNMP information.
- Set Community. Enter the password that allows read/write access to the Router's SNMP information.
- SNMP Trusted Host. You can restrict access to the Router's SNMP information by IP address. Enter the IP address in the SNMP Trusted Host field. If this field is left blank, then access is permitted from any IP address.

- SNMP Trap-Community. Enter the password required by the remote host computer that will receive trap messages or notices sent by the Router.
- SNMP Trap-Destination. Enter the IP address of the remote host computer that will receive the trap messages.

UPnP

UPnP allows Windows XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, click **Enabled**.

- Allow User to make Configuration Changes. When enabled, this feature allows you to make manual changes while still using the UPnP feature.
- Allow users to disable Internet access. When enabled, this feature allows you to prohibit any and all Internet connections.

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

Log

The Log tab, shown in Figure 6-31, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Email Alert

To enable E-Mail Alert, click **Enabled**.

- E-Mail Address for General Logs. Enter the **E-Mail Address for General Logs** in the field.
- E-Mail Address for Alert Logs. Enter the **E-Mail Address for Alert Logs** in the field.
- Return E-Mail address. Enter the **address for the return E-Mail**.
- E-Mail Server IP Address. Enter the **IP Address of the E-Mail Server** in the fields.

Syslog Notification

To enable Syslog, click **Enabled**.

- Device Name. Enter the **Device Name** in the field.

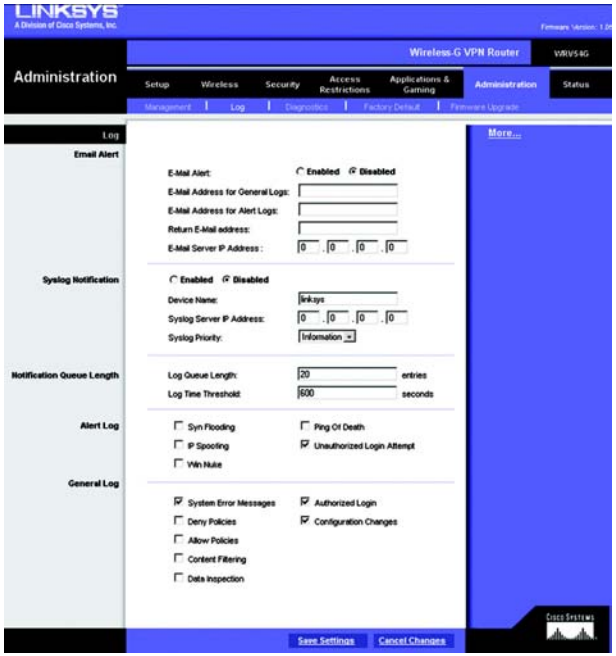


Figure 6-31: Log

- Syslog Server IP Address. Enter the I**P Address of the Syslog Server**.
- Syslog Priority. Select the **priority** from the drop-down list.

Notification Queue Length

- Log queue Length. Enter the **number** of entries in the log queue in the field.
- Log Time Threshold. Enter the **time** for the threshold in the field.

Alert Log

Select the type of attacks that you want to be alerted to. Select Syn Flooding, IP Spoofing, Win Nuke, Ping of Death, or Unauthorized Login attempt.

General Log.

Select the type of activity you would like to log. Select System Error Messages, Deny Policies, Allow Policies, Content Filtering, Data Inspection, authorized Login, or Configuration Changes.

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

Diagnostics

Ping Test (See Figure 6-32.)

Ping Test Parameters

Ping Target IP. Enter the IP Address that you want to ping in the field.

No. of Pings. Enter the number of times that you want to ping.

Ping Size. Enter the size of the ping packets.

Ping Interval. Enter the ping interval in Milliseconds.

Ping Timeout. Enter the time in Milliseconds.

Click the **Start Test** button to start the Ping Test. Click the **Abort Test** button to stop the test. Click the **Clear Result** button to clear the results. The results of the test will display in the window.

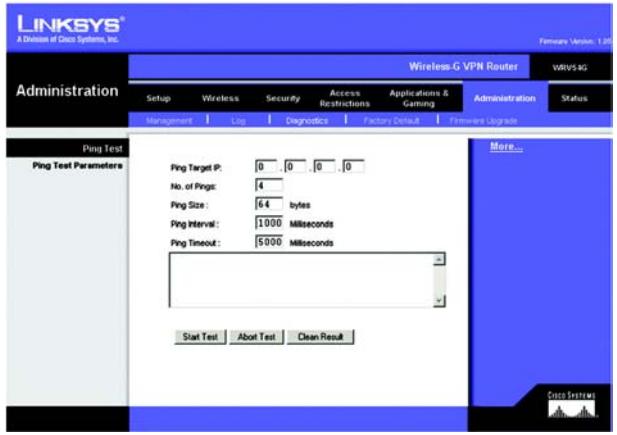


Figure 6-32: Ping Test

Factory Default (See Figure 6-33.)

If you have exhausted all other options and wish to restore the Router to its factory default settings and lose all your settings, click **Yes**.

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

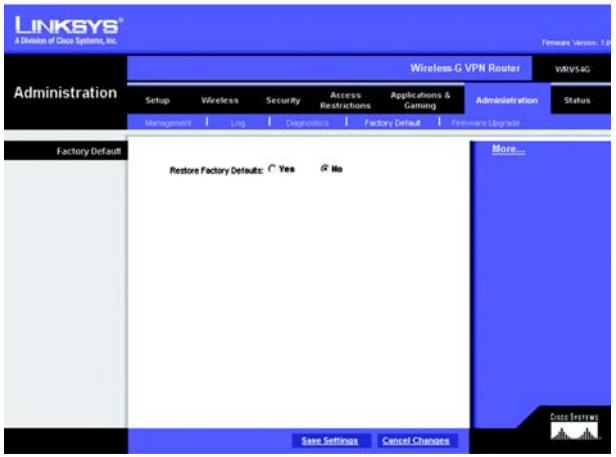


Figure 6-33: Factory Default

Firmware Upgrade (See Figure 6-34.)

To upgrade the Router's firmware:

1. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.
2. Double-click the firmware file you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.

Figure 6-34: Firmware Upgrade

Status

Router

This screen displays information about your Router and its WAN (Internet) Connections. (See Figure 6-35.)

Information

The information displayed is the Hardware Version, Software Version, MAC Address, Local MAC Address, and System Up Time.

WAN Connections

The WAN Connections displayed are the Network Access, WAN IP Address, Subnet Mask, Default Gateway, and DNS.

Click the **Refresh** button if you want to Refresh your screen.

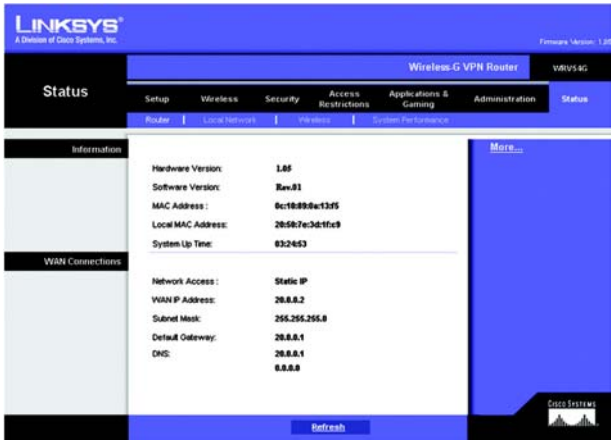


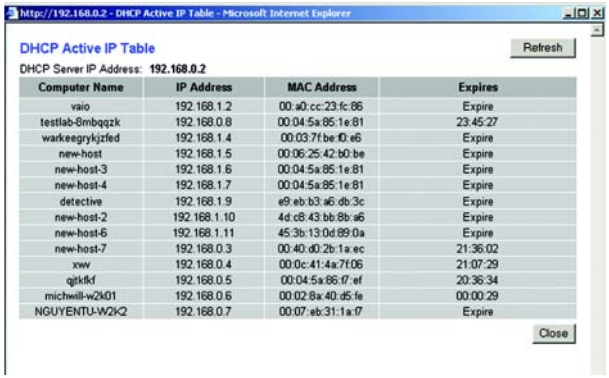
Figure 6-35: Router

Local Network

The Local Network information that is displayed is the IP Address, Subnet Mask, DHCP Server, and DHCP Client Lease Info. To view the DHCP Clients Table, click the **DHCP Clients** button. See Figure 6-36.

The DHCP Active IP Table, Figure 6-37, displays the computer name, IP Address, MAC Address and the expiration time. Click the **Close** button to return to the Local Network screen.

Figure 6-36: Local Network



Computer Name	IP Address	MAC Address	Expires
vaio	192.168.1.2	00:a0:cc:23:fc:86	Expire
testlab-8mbqqzk	192.168.0.8	00:04:5a:85:1e:81	23:45:27
warkeegrykjzfed	192.168.1.4	00:03:7f:be:f0:e6	Expire
new-host	192.168.1.5	00:06:25:42:b0:be	Expire
new-host-3	192.168.1.6	00:04:5a:85:1e:81	Expire
new-host-4	192.168.1.7	00:04:5a:85:1e:81	Expire
detective	192.168.1.9	e9:eb:b3:a6:db:3c	Expire
new-host-2	192.168.1.10	4d:c8:43:bb:8b:a6	Expire
new-host-6	192.168.1.11	45:3b:13:0d:89:0a	Expire
new-host-7	192.168.0.3	00:40:d0:2b:1a:ec	21:36:02
xww	192.168.0.4	00:0c:41:4a:7f:06	21:07:29
qjtkfkf	192.168.0.5	00:04:5a:86:f7:ef	20:36:34
michwill-w2k01	192.168.0.6	00:02:8a:40:d5:fe	00:00:29
NGUYENTU-W2K2	192.168.0.7	00:07:eb:31:1a:f7	Expire

Figure 6-37: DHCP Active IP Table

Wireless

The Wireless Network information that is displayed is the MAC Address, Mode, SSID, Channel, and Encryption Function. (See Figure 6-38.)

Click the **Refresh** button if you want to Refresh your screen.

Figure 6-38: Wireless

System Performance

The System Peformance information that is displayed is the Wireless, Internet, and/or LAN information for the IP Address, MAC Address, Connection Status, Packets Received, Packets Sent, Bytes Received, Bytes Sent, Error Packes Received, and Dropped Packets Received. (See Figure 6-39.)

Click the **Refresh** button if you want to Refresh your screen.

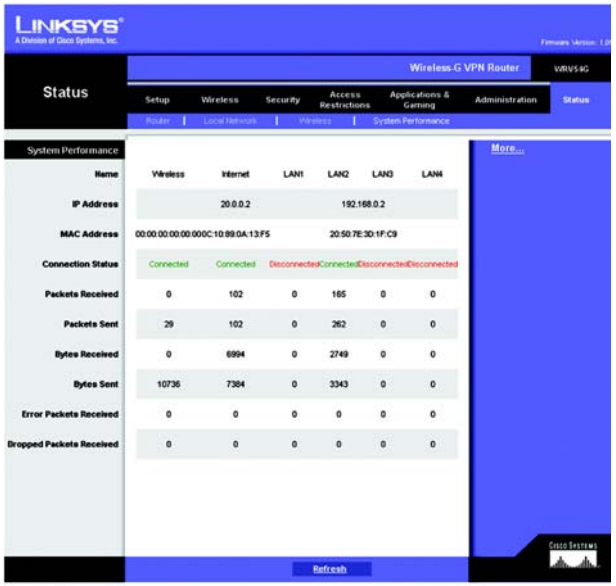


Figure 6-39: System Performance

Appendix A: Troubleshooting

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” Provided are possible solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help you solve your problems. If you can’t find an answer here, check the Linksys website at www.linksys.com.

Common Problems and Solutions

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

You can assign a static IP address to a PC by performing the following steps:

- For Windows 98 and Me:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
  2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
  3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Router. Make sure that each IP address is unique for each PC or network device.
  4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Router. Click the Add button to accept the entry.
  5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
  6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
  7. Restart the computer when asked.
- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.1.1 (Router’s default IP address).

7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
9. 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.

  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
  4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  6. Enter the Subnet Mask, 255.255.255.0.
  7. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
  8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

2. I want to test my Internet connection.

A Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Refer to "Chapter 4: Configure the PCs" for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

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

B Open a command prompt.

For Windows 98 and Me:

- Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

- Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button. In the command prompt, type ping 192.168.1.1 and press the Enter key.
- If you get a reply, the computer is communicating with the Router.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C In the command prompt, type ping followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Router's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.

- If you get a reply, the computer is connected to the Router.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D In the command prompt, type ping www.yahoo.com and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

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

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
  1. If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix D: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of "Chapter 6: The Router's Web-based Utility" for details.
  2. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: The Router's Web-based Utility" for details on Internet connection settings.
  3. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
  4. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's web-based utility shows a valid IP address from your ISP.
  5. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Router's web-based utility.

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

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

Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router, and go to the Security tab. Make sure you have IPsec pass-through and/or PPTP pass-through enabled.

- VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab
- of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.
- Check the Linksys website for more information at www.linksys.com.

6. I need to set up a server behind my Router and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

- Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.
  1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications and Gaming => Port Forwarding tab.

2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the Enable option for the port services you want to use. Consider the example below:

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

When you have completed the configuration, click the **Save Settings**button.

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

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

1. Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications and Gaming => Port Forwarding tab.
2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

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

When you have completed the configuration, click the **Save Settings** button.

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

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

- Follow these steps to set DMZ hosting:
  1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications and Gaming => DMZ tab.
  2. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

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

- Reset the Router to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:
  1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Enter the default password admin, and click the **Administrations** => **Management** tab.
  2. Enter a different password in the Router Password field, and enter the same password in the second field to confirm the password.
  3. Click the **Save Settings** button.

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

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

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start, Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
- For Netscape 4.7 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

11. To start over, I need to set the Router to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

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

- Follow these steps:
  1. Go to the Linksys website at http://www.linksys.com and download the latest firmware.
  2. To upgrade the firmware, follow the steps in the System section found in "Chapter 6: The Router's Web-based Utility."

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

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

- 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.
- Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:
  IP Address: 192.168.1.50
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Router's web-based utility through its Administration tab.

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

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.
  1. To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
  4. Click the **Save Settings** button.
  5. Click the **Status** tab, and click the **Connect** button.
  6. 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.
- Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

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

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:

  1462
  1400
  1362
  1300

16. The Power LED flashes continuously.

The Power 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 remains steady to show that the system is working fine. If the LED continues to flash 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.

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

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

Frequently Asked Questions

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

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

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

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

Does the Internet connection of the Router support 100Mbps Ethernet?
The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

What is Network Address Translation and what is it used for?

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

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

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

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

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

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

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

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com for more information.

If all else fails in the installation, what can I do?

Reset the Router by holding down the reset button until the Power LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, www.linksys.com.

How will I be notified of new Router firmware upgrades?

All Linksys firmware upgrades are posted on the Linksys website at www.linksys.com, where they can be downloaded for free. To upgrade the Router's firmware, use the System tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment?

Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?

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

If DMZ Hosting is used, does the exposed user share the public IP with the Router?

No.

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

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

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

What are the advanced features of the Router?
The Router's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

What is the maximum number of VPN sessions allowed by the Router?
The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.

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

Can the Router act as my DHCP server?
Yes. The Router has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming

- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Will the information be intercepted while it is being transmitted through the air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is 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. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Router?

Press the Reset button on the back panel for about ten seconds. This will reset the Router to its default settings.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Router and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Router and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.
WEP is probably enabled on the Router, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Router?
There are eleven available channels, ranging from 1 to 11 (in North America).

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

Appendix B: Wireless Security

A Brief Overview

Whenever data - in the form of files, emails, or messages - is transmitted over your wireless network, it is open to attacks. Wireless networking is inherently risky because it broadcasts information on radio waves. Just like signals from your cellular or cordless phone can be intercepted, signals from your wireless network can also be compromised. What are the risks inherent in wireless networking? Read on.

What Are The Risks?

Computer network hacking is nothing new. With the advent of wireless networking, hackers use methods both old and new to do everything from stealing your bandwidth to stealing your data. There are many ways this is done, some simple, some complex. As a wireless user, you should be aware of the many ways they do this.

Every time a wireless transmission is broadcast, signals are sent out from your wireless PC or router, but not always directly to its destination. The receiving PC or router can hear the signal because it is within that radius. Just as with a cordless phone, cellular phone, or any kind of radio device, anyone else within that radius, who has their device set to the same channel or bandwidth can also receive those transmission.

Wireless networks are easy to find. Hackers know that, in order to join a wireless network, your wireless PC will typically first listen for "beacon messages". These are identifying packets transmitted from the wireless network to announce its presence to wireless nodes looking to connect. These beacon frames are unencrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier) and the IP address of the network PC or router. The SSID is analogous to the network's name. With this information broadcast to anyone within range, hackers are often provided with just the information they need to access that network.

One result of this, seen in many large cities and business districts, is called "Warchalking". This is the term used for hackers looking to access free bandwidth and free Internet access through your wireless network. The marks they chalk into the city streets are well documented in the Internet and communicate exactly where available wireless bandwidth is located for the taking.

Even keeping your network settings, such as the SSID and the channel, secret won't prevent a hacker from listening for those beacon messages and stealing that information. This is why most experts in wireless networking strongly recommend the use of WEP (Wireless Equivalent Privacy). WEP encryption scrambles your wireless signals so they can only be recognized within your wireless network.

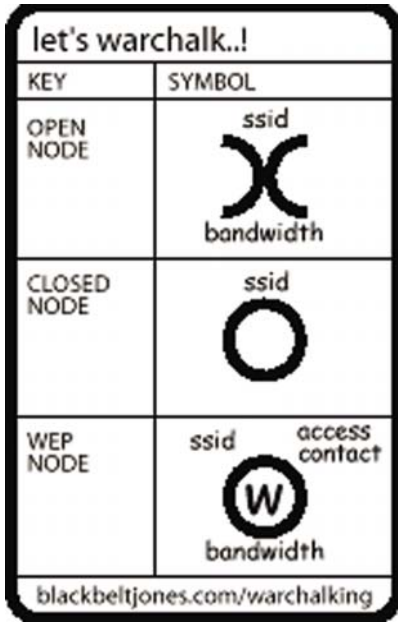


Figure B-1: Warchalking

But even WEP has its problems. WEP's encryption algorithm is referred to as "simple", which also means "weak", because the technology that scrambles the wireless signal isn't too hard to crack for a persistent hacker.

There are five common ways that hackers can break into your network and steal your bandwidth as well as your data. The five attacks are popularly known as:

1. Passive Attacks
2. Jamming Attacks
3. Active Attacks
4. Dictionary-building or Table Attacks
5. Man-in-the-Middle Attacks

Passive Attacks

There's no way to detect a passive attack because the hacker is not breaking into your network. He is simply listening (eavesdropping, if you will) to the information your network broadcasts. There are applications easily available on the Internet that can allow a person to listen into your wireless network and the information it broadcasts. Information such as MAC addresses, IP addresses, usernames, passwords, instant message conversations, emails, account information, and any data transmitted wirelessly, can easily be seen by someone outside of your network because it is often broadcast in clear text. Simply put, any information transmitted on a wireless network leaves both the network and individual users vulnerable to attack. All a hacker needs is a "packet sniffer", software available on the Internet, along with other freeware or shareware hacking utilities available on the Internet, to acquire your WEP keys and other network information to defeat security.

Jamming Attacks

Jamming Attacks, when a powerful signal is sent directly into your wireless network, can effectively shut down your wireless network. This type of attack is not always intentional and can often come about simply due to the technology. This is especially possible in the 2.4 GHz frequency, where phones, baby monitors, and microwave ovens can create a great deal of interference and jam transmissions on your wireless network. One way to resolve this is by moving your wireless devices into the 5 GHz frequency, which is dedicated solely to information transmissions.

Active Attacks

Hackers use Active Attacks for three purposes: 1) stealing data, 2) using your network, and 3) modifying your network so it's easier to hack in the next time.

In an Active Attack, the hacker has gained access to all of your network settings (SSID, WEP keys, etc.) and is in your network. Once in your wireless network, the hacker has access to all open resources and transmitted data on the network. In addition, if the wireless network's router is connected to a switch, the hacker will also have access to data in the wired network.

Further, spammers can use your Internet connection and your ISP's mail server to send tens of thousands of e-mails from your network without your knowledge.

Lastly, the hacker could make hacking into your network even easier by changing or removing safeguards such as MAC address filters and WEP encryption. He can even steal passwords and user names for the next time he wants to hack in.

Dictionary-Building or Table Attacks

Dictionary-building, or Table attacks, is a method of gaining network settings (SSID, WEP keys, etc.) by analyzing about a day's worth of network traffic, mostly in the case of business networks. Over time, the hacker can build up a table of network data and be able to decrypt all of your wireless transmissions. This type of attack is more effective with networks that transmit more data, such as businesses.

Man-in-the-Middle Attacks

A hacker doesn't need to log into your network as a user - he can appear as one of the network's own routers, setting himself up as the man-in-the-middle. To do this, the hacker simply needs to rig an router with your network's settings and send out a stronger signal that your router. In this way, some of your network's PCs may associate with this rogue router, not knowing the difference, and may begin sending data through it and to this hacker.

The trade-off for the convenience and flexibility wireless networking provides is the possibility of being hacked into through one of the methods described here. With wireless networks, even with WEP encryption, open to the persistent hacker, how can you protect your data? The following section will tell you how to do just that.

Maximizing Wireless Security

Security experts will all tell you the same thing: Nothing is guaranteed. No technology is secure by itself. An unfortunate axiom is that building the better mousetrap can often create a better mouse. This is why, in the

examples below, your implementation and administration of network security measures is the key to maximizing wireless security.

No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network. Often, hackers are looking for an easy target. Making your network less attractive to hackers, by making it harder for them to get in, will make them look elsewhere.

How do you do this? Before discussing WEP, let's look at a few security measures often overlooked.

1) Network Content

Now that you know the risks assumed when networking wirelessly, you should view wireless networks as you would the Internet. Don't host any systems or provide access to data on a wireless network that you wouldn't put on the Internet.

2) Network Layout

When you first lay out your network, keep in mind where your wireless PCs are going to be located and try to position your router towards the center of that network radius. Remember that access points transmit indiscriminately in a radius; placing an access point at the edge of the physical network area reduces network performance and leaves an opening for any hacker smart enough to discover where the router is transmitting.

This is an invitation for a man-in-the-middle attack, as described in the previous section. To perform this type of attack, the hacker has to be physically close to your network. So, monitoring both your network and your property is important. Furthermore, if you are suspicious of unauthorized network traffic, most wireless products come with a log function, with which you can view activity on your network and verify if any unauthorized users have had access.

3) Network Devices

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. If they get into the hands of a hacker, so do all of your settings. So keep an eye on them.

4) Administrator passwords

Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

5) SSID

There are a few things you can do to make your SSID more secure:

a. Disable Broadcast

b. Make it unique

c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. This is a option for convenience, allowing anyone to log into your wireless network. In this case, however, anyone includes hackers. So don't broadcast the SSID.

A default SSID is set on your wireless devices by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Changing your SSID regularly will force any hacker attempting to gain access to your wireless network to start looking for that new SSID.

With these three steps in mind, please remember that while SSIDs are good for segmenting networks, they fall short with regards to security. Hackers can usually find them quite easily.

6) MAC addresses

Enable MAC address filtering if your wireless products allow it. MAC address filtering will allow you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker using a random MAC address or spoofing (faking) a MAC address.

7) Firewalls

You can use the same firewall technology to protect your wired network from hackers coming in through your wireless network as you did for the Internet. The firewall will protect your network from any transmissions entering via your wireless network.

8) WEP

Wired Equivalent Privacy (WEP) is often looked upon as a panacea for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is

not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Programs exist on the Internet that are designed to defeat WEP. The best known of these is AirSnort. In about a day, AirSnort can analyze enough of the wireless transmissions to crack the WEP key. Just like a dictionary-building attack, the best prevention for these types of programs is by not using static settings, periodically changing WEP keys, SSID, etc.

There are several ways that WEP can be maximized:

a) Use the highest level of encryption possible

b) Use multiple WEP keys

c) Change your WEP key regularly

Current encryption technology offers 64-bit and 128-bit WEP encryption. If you are using 64-bit WEP, swap out your old wireless units for 128-bit encryption right away. Where encryption is concerned, the bigger and more complex, the better. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, nodes in your wireless network are identified with a common WEP key. Second, these WEP keys encrypt and decrypt data sent over your wireless network. So, a higher level of security ensures that hackers will have a harder time breaking into your network.

Setting one, static WEP key on your wireless network leaves your network open the threats even as you think it is protecting you. While it is true that using a WEP key increases wireless security, you can increase it further by using multiple WEP keys.

Keep in mind that WEP keys are stored in the firmware of wireless cards and access points and can be used to hack into the network if a card or access point falls into the wrong hands. Also, should someone hack into your network, there would be nothing preventing someone access to the entire network, using just one static key.

The solution, then, is to segment your network up into multiple groups. If your network had 80 users and you used four WEP keys, a hacker would have access to only ¼ of your wireless network resources. In this way, multiple keys reduce your liability.

Finally, be sure to change your WEP key regularly, once a week or once a day. Using a "dynamic" WEP key, rather than one that is static, makes it even harder for a hacker to break into your network and steal your resources.

2.4GHz/802.11b and 802.11g WEP Encryption

WEP encryption for the Wireless-G VPN Broadband Router is configured through the Web-Utility's Wireless tab. Enable **WEP** from this tab and click the **Edit WEP Settings** button, which will open the WEP screen, shown in Figure B-3.

From this screen, you can select the type of WEP encryption to use as well as set the WEP Key for that encryption.

Select which WEP key (1-4) will be used when the Router sends data, then select that number as the Default Transmit Key. Make sure the receiving device is using the same key.

Select the level of WEP encryption you wish to use, 64-bit 10 hex digits or 128-bit 26 hex digits. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

If you wish to use a WEP Passphrase, it can be a maximum of 16 alphanumeric characters. This passphrase may not work with non-Linksys products due to possible incompatibility with other vendors' passphrase generators. The WEP Key can be generated using your Passphrase or you can enter it manually.

If you wish to enter the WEP Key manually, type the key into the appropriate Key field on the left. The WEP key must consist of the letters "A" through "F" and the numbers "0" through "9" and should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption. All points in your wireless network must use the same WEP key to utilize WEP encryption.

Once the Passphrase is entered, click the **Generate** key to generate a WEP key.

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

Important: Always remember that each point in your wireless network MUST use the same WEP Encryption method and encryption key or your wireless network will not function properly.

Figure B-2: WEP

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

Introduction

This document demonstrates 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. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

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

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

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

Environment

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

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

Subnet Mask: 255.255.255.0

BEFSX41

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

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

How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the **Open** field. The Local Security Setting screen will appear as shown in Figure C-1.
2. Right-click **IP Security Policies on Local Computer**, and click **Create IP Security Policy**.
3. Click the **Next** button, and then enter a name for your policy (for example, to_router). Then, click **Next**.
4. Deselect the Activate the default response rule check box, and then click the **Next** button.
5. Click the **Finish** button, making sure the Edit check box is checked.

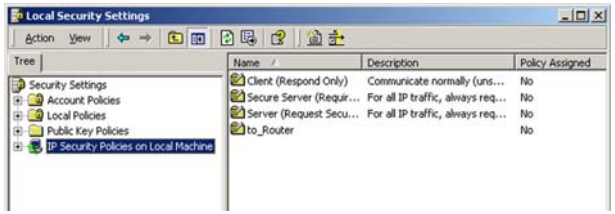


Figure C-1: Password Screen

NOTE: The references in this section to "win" are references to Windows 2000 and XP.

Step 2: Build Filter Lists

Filter List 1: win->router

1. In the new policy's properties screen, verify that the Rules tab is selected, as shown in Figure C-2. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.
2. Make sure the IP Filter List tab is selected, and click the **Add** button. (See Figure C-3.)

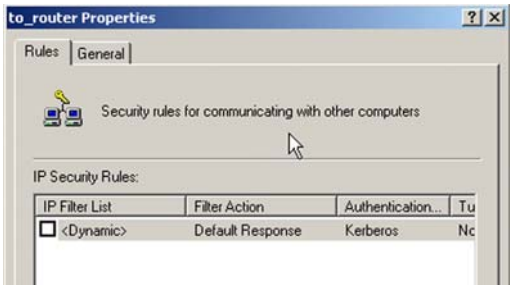


Figure C-2: Setup Tab

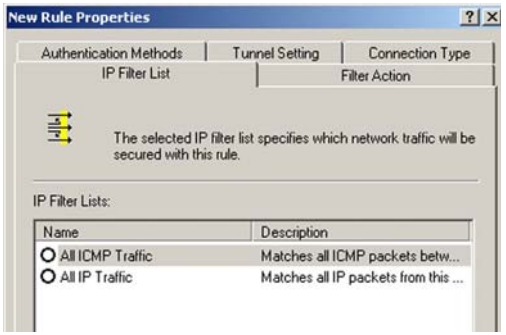


Figure C-3: IP Filter List Tab

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

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

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

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

Filter List 2: router=>win

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

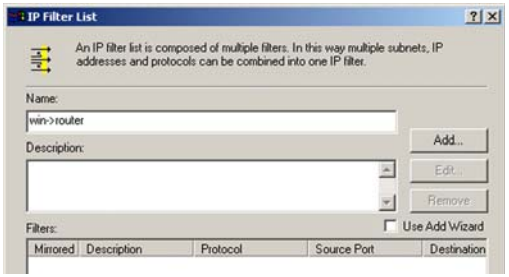


Figure C-4: IP Filter List

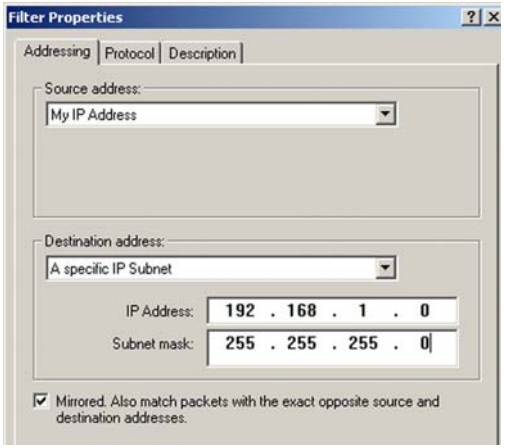


Figure C-5: Filters Properties

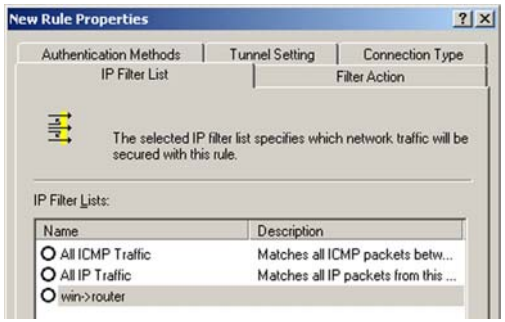


Figure C-6: New Rule Properties

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

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

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

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

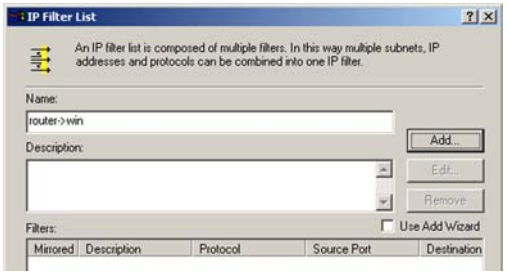


Figure C-7: IP Filter List

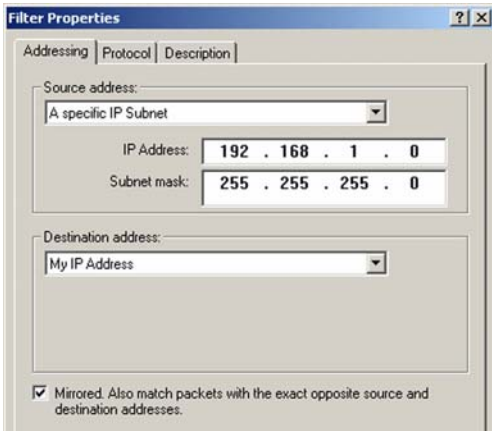


Figure C-8: Filters Properties

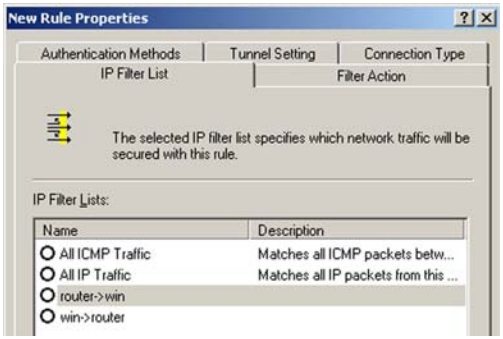


Figure C-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->router

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

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

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

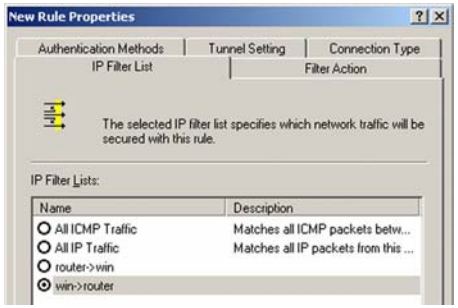


Figure C-10: IP Filter List Tab

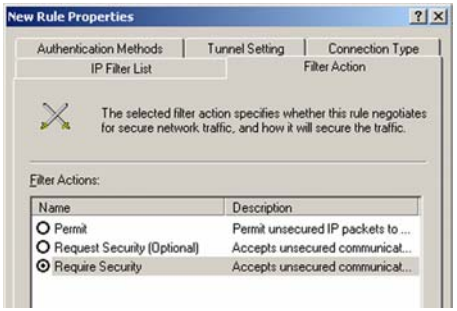


Figure C-11: Filter Action Tab

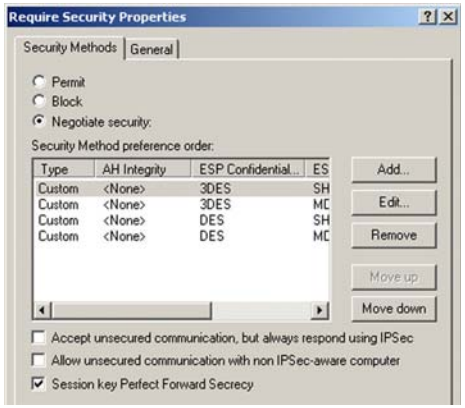


Figure C-12: Security Methods Tab

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

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

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

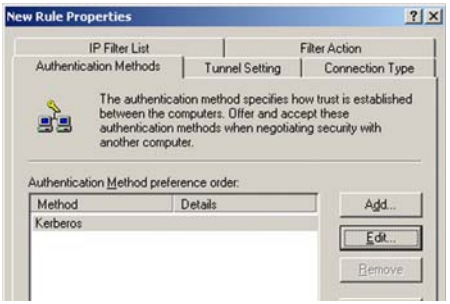


Figure C-13: Authentication Methods

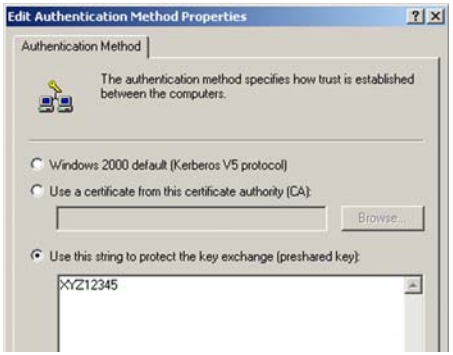


Figure C-14: Preshared Key

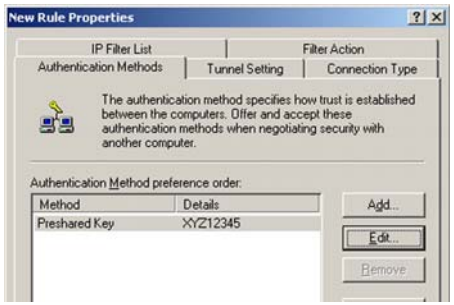


Figure C-15: New Preshared Key

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

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

Tunnel 2: router->win

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

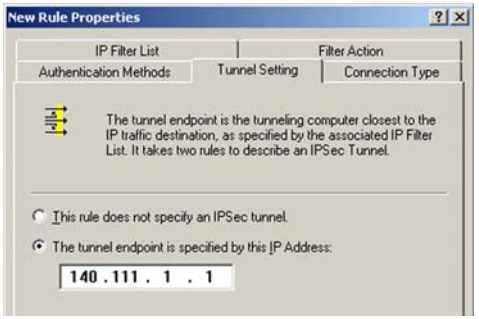


Figure C-16: Tunnel Setting Tab

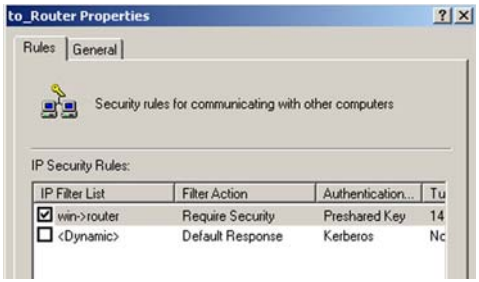


Figure C-17: Connectin Type Tab

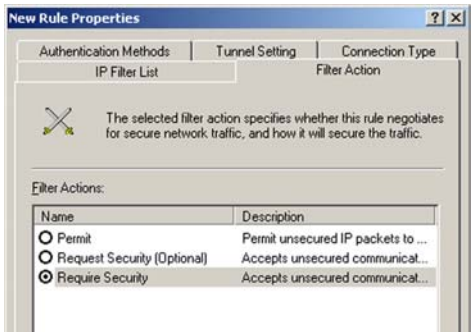


Figure C-18: Properties Screen

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

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

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

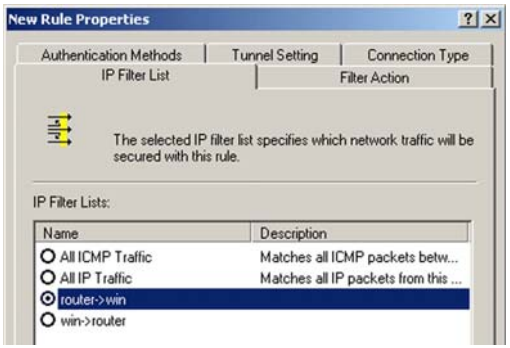


Figure C-19: IP Filter List Tab

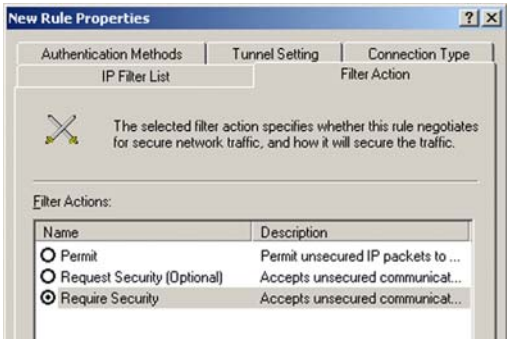


Figure C-20: Filter Action Tab

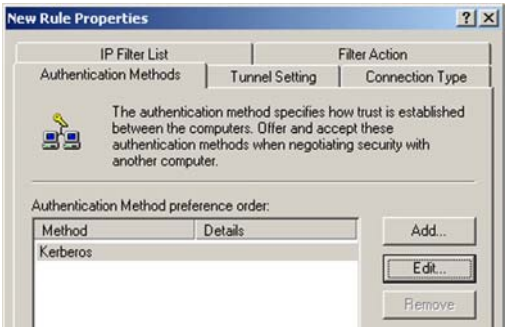


Figure C-21: Authentication Methods Tab

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

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

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

Figure C-22: Preshared Key

Figure C-23: New Preshared Key

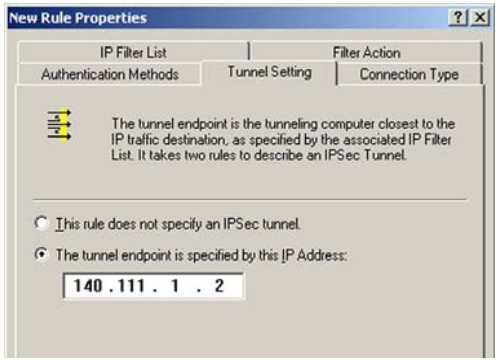


Figure C-24: Tunnel Seting Tab

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

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

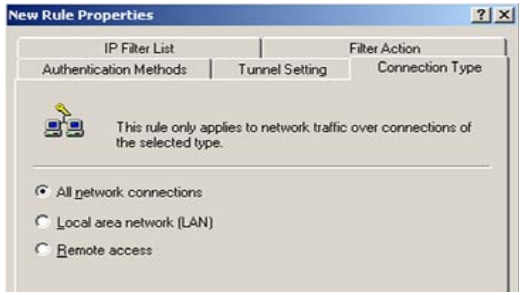


Figure C-25: Connection Type

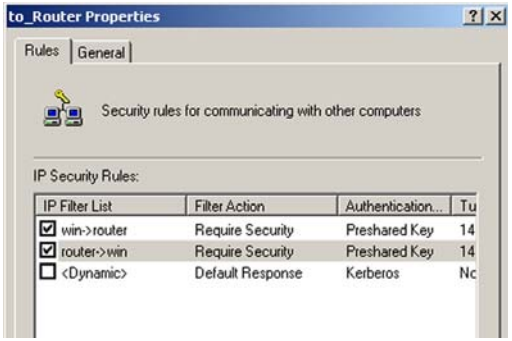


Figure C-26: Rules

Step 4: Assign New IPSec Policy

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

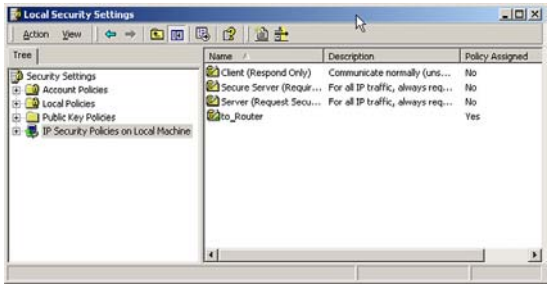


Figure C-27: Local Computer

Step 5: Create a Tunnel Through the Web-Based Utility

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

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

3. From the Setup tab, click the **VPN** tab.

4. From the VPN tab, shown in Figure C-28, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. Then click **Enabled**. Enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

5. Enter the IP Address and Subnet Mask of the local VPN Router in the Local Secure Group fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).

6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the Remote Security Gateway fields.

7. Select fromtwo 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.

8. Select from 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.

9. Select the 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. 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.

10. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

Figure C-28: VPN Tab

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

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

Figure D-1: IP Configuration Screen

Windows 98 or Me Instructions

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

   The MAC address/Adapter Address is what you will use for MAC address cloning or MAC filtering.

   The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

Figure D-2: MAC Address/Adapter Address

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

Windows 2000 or XP Instructions

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

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

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

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

   The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.

   The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

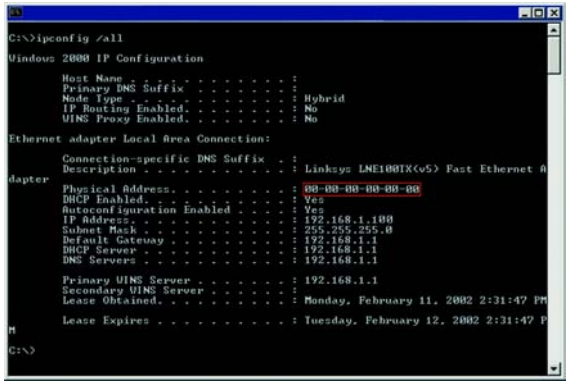


Figure D-3: MAC Address/Physical Address

Appendix E: SNMP Functions

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

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

Appendix F: Upgrading Firmware

The Router's firmware is upgraded through the Web-Utility's Firmware Upgrade tab from the Administration tab. Follow these instructions:

1. Click the Browse button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.

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

Figure F-1: Upgrade Firmware

Appendix G: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix H: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - Device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

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

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit - A binary digit.

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

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

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.

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

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

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

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

Encryption - Encoding data to prevent it from being read by unauthorized people.

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

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

Firewall - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A system that interconnects networks.

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

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

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

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

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

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio band used in wireless networking transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

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

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

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

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

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

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

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

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

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

Preamble - Part of the wireless signal that synchronizes network traffic.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

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.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

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

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set IDentifier) - Your wireless network's name.

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

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

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

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

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

Upload - To transmit a file over a network.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

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

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix I: Specifications

Standards	IEEE 802.3, 802.11b and 802.11g
Ports	One Internet, Ethernet (1-4), Power
Buttons	One Reset Button, One Power Switch
Cabling Type	UTP CAT 5 or better
Data Rate	Up to 54Mbps
Transmit Power	20dBm
LEDs	Power, Internet, Ethernet (1, 2, 3, 4), Wireless-G, DMZ
Security Features	WEP, 802.1x Authentication
WEP Key Bits	64, 128
Dimensions (W x H x D)	7.32" x 6.89" x 1.89" (186 mm x 175 mm x 48 mm)
Unit Weight	1.26 lb (0.57 kg)
Power	External, 5V DC, 2.5A
Certifications	FCC, IC-03
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	10% to 85% Non-Condensing

Cisco-Linksys, LLC declares that WRV54G ver. 2 (FCC ID: Q87-WRV54GV2) is limited in CH1~CH11 by specified firmware controlled in

Storage Humidity	5% to 90% Non-Condensing

Appendix J: Warranty Information

LIMITED WARRANTY

Linksys warrants to the original end user purchaser ("You") that, for a period of three years, (the "Warranty Period") Your Linksys product will be free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys's entire liability under this warranty will be for Linksys at its option to repair or replace the product or refund Your purchase price less any rebates.

If the product proves defective during the 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. You are responsible for shipping defective products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

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

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT.

The foregoing limitations will apply even if any warranty or remedy provided under this Section fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

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

Appendix K: Regulatory Information

FCC STATEMENT

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

INDUSTRY CANADA (CANADA)

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

Operation is subject to the following two conditions:
1) This device may not cause interference and
2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 3 dBi.
Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys Group declares that the Instant Wireless™ Series products included in the Instant Wireless™ Series conform to the specifications listed below, following the provisions of the EMC Directive 89/336/EEC and Low Voltage Directive 73/23/EEC:

ETS 300-826, 301 489-1 General EMC requirements for Radio equipment.

EN 609 50 Safety

ETS 300-328-2 Technical requirements for Radio equipment.

Note: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Linksys Corporate Compliance.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and/or the CEPT recommendation Rec 70.03. For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys Group™ vakuuttaa täten että Instant Wireless IEEE 802.11 PC Card tyyppinen laite on direktiivin 1999/5/EY, direktiivin 89/336/EEC ja direktiivin 73/23/EEC oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.
Linksys Group™ déclare que la carte PC Instant Wireless IEEE 802.11 est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC, la directive 89/336/EEC, et à la directive 73/23/EEC.
Belgique B L'utilisation en extérieur est autorisé sur le canal 11 (2462 MHz), 12 (2467 MHz), et 13 (2472 MHz). Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.
France F: Bande de fréquence restreinte: seuls les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) doivent être utilisés en France.
Toute utilisation, qu'elle soit intérieure ou extérieure, est soumise à autorisation. Vous pouvez contacter l'Autorité de Régulation des Télécommuniations
(<http://www.art-telecom.fr>) pour la procédure à suivre.
France F: Restricted frequency band: only channels 10, 11, 12, 13 (2457, 2462, 2467, and 2472 MHz respectively) may be used in France. License required for every indoor and outdoor installations. Please contact ART for procedure to follow.
Deutschland D: Anmeldung im Outdoor-Bereich notwending, aber nicht genehmigungspflichtig. Bitte mit Händler die Vorgehensweise abstimmen.
Germany D: License required for outdoor installations. Check with reseller for procedure to follow

Italia I: E' necessaria la concessione ministeriale anche per l'uso interno. Verificare con i rivenditori la procedura da seguire. L'uso per installazione in esterni non e' permessa.
Italy I: License required for indoor use. Use with outdoor installations not allowed.
the Netherlands NL License required for outdoor installations. Check with reseller for procedure to follow.
Nederlands NL Licentie verplicht voor gebruik met buitenantennes. Neem contact op met verkoper voor juiste procedure.

Appendix L: Contact Information

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