

LINKSYS®

A Division of Cisco Systems, Inc.



2.4GHz 802.11g **Wireless-G**

WIRELESS

VPN Broadband Router

Model No. **WRV54G**

CISCO SYSTEMS



Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2006 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

How to Use this Guide

This User Guide has been designed to make understanding networking with the Router easier than ever. Look for the following items when reading this 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
Network Topology	4
Ad-Hoc versus Infrastructure Mode	4
Network Layout	4
Chapter 3: Planning Your Virtual Private Network (VPN)	6
Why do I need a VPN?	6
What is a VPN?	7
Chapter 4: Getting to Know the Wireless-G VPN Broadband Router	9
The Back Panel	9
The Front Panel	10
Chapter 5: Connecting the Wireless-G VPN Broadband Router	11
Overview	11
Wired Connection to a PC	11
Wireless Connection to a PC	12
Chapter 6: Configuring the Wireless-G VPN Broadband Router	13
Overview	13
How to Access the Web-based Utility	15
The Setup Tab - Basic Setup	15
The Setup Tab - DDNS	19
The Setup Tab - MAC Address Clone	20
The Setup Tab - Advanced Routing	21
The Setup Tab - Hot Spot	23
The Wireless Tab - Basic Wireless Settings	24
The Wireless Tab - Wireless Security	25
The Wireless Tab - Wireless Network Access	27
The Wireless Tab - Advanced Wireless Settings	28

The Security Tab - Firewall	30
The Security Tab - VPN	31
The Access Restrictions Tab - Internet Access	37
The Access Restrictions Tab - VPN Client Access	40
The Applications and Gaming Tab - Port Range Forwarding	41
The Applications and Gaming Tab - Port Triggering	42
The Applications and Gaming Tab - UPnP Forwarding	43
The Applications and Gaming Tab - DMZ	44
The Administration Tab - Management	45
The Administration Tab - Log	47
The Administration Tab - Diagnostics	49
The Administration Tab - Factory Defaults	50
The Administration Tab - Firmware Upgrade	51
The Status Tab - Router	52
The Status Tab - Local Network	53
The Status Tab - System Performance	55
The Status Tab - VPN Clients	57
Chapter 7: Boingo™ Hot Spot in a Box® Program for Hot Spot Businesses	58
Program Overview	58
Simple Hot Spot in a Box Program	58
How the Boingo Hot Spot in a Box Feature Impacts the Linksys Wireless-G Broadband Router	59
Excellent Customer Support	60
Getting Started	60
Administration Site	71
Appendix A: Troubleshooting	78
Common Problems and Solutions	78
Frequently Asked Questions	86
Appendix B: Wireless Security	94
Security Precautions	94
Security Threats Facing Wireless Networks	94

Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP	97
Overview	97
Before You Begin	97
Installing the Linksys QuickVPN Software	97
Using the Linksys QuickVPN Software	98
Appendix D: Configuring IPSec between a Windows 2000 or XP Computer and the Router	99
Introduction	99
Environment	99
How to Establish a Secure IPSec Tunnel	100
Appendix E: Configuring VPN Tunnels	110
Overview	110
Before You Begin	110
Configuring the VPN Settings for the VPN Routers	111
Configuring the Key Management Settings	113
Configuring PC 1 and PC 2	114
Connecting a VPN Client	114
Appendix F: Finding the MAC Address and IP Address for Your Ethernet Adapter	117
Windows 98 or Me Instructions	117
Windows 2000 or XP Instructions	118
Appendix G: SNMP Functions	119
Appendix H: Upgrading Firmware	120
Appendix I: Windows Help	121
Appendix J: Glossary	122
Appendix K: Specifications	127
Appendix L: Warranty Information	128
Appendix M: Regulatory Information	129
Appendix N: Contact Information	135

List of Figures

Figure 2-1: Network Diagram	5
Figure 3-1: VPN Router to VPN Router	8
Figure 3-2: Computer to VPN Router	8
Figure 4-1: Back Panel	9
Figure 4-2: Front Panel	10
Figure 5-1: Connect to LAN Ports	11
Figure 5-2: Connect to Internet Port	11
Figure 5-3: Connect to Power Port	11
Figure 5-4: Connect to Internet Port	12
Figure 5-5: Connect to Power Port	12
Figure 6-1: Login Screen	15
Figure 6-2: Setup Tab - Automatic Configuration - DHCP	15
Figure 6-3: Internet Connection Type - Static IP	16
Figure 6-4: Internet Connection Type - PPPoE	16
Figure 6-5: Internet Connection Type - PPTP	17
Figure 6-6: DDNS Tab - DynDNS.org	19
Figure 6-7: DDNS Tab - TZ0.com	19
Figure 6-8: Setup Tab - MAC Address Clone	20
Figure 6-9: Setup Tab - Advanced Routing	21
Figure 6-10: Routing Table Entry List	22
Figure 6-11: Setup Tab - Hot Spot in a Box	23
Figure 6-12: Wireless Tab - Basic Wireless Settings	24
Figure 6-13: Wireless Security - WPA Pre-Shared Key	25
Figure 6-14: Wireless Security - WPA RADIUS	25
Figure 6-15: Wireless Security - RADIUS	26
Figure 6-16: Wireless Security - WEP	26
Figure 6-17: Wireless Tab - Wireless Network Access	27
Figure 6-18: Networked Computers	27
Figure 6-19: Wireless Tab - Advanced Wireless Settings	28
Figure 6-20: Security Tab - Firewall	30

Figure 6-21: Security Tab - VPN	31
Figure 6-22: Local Secure Group - Subnet and Remote Secure Group - Subnet	31
Figure 6-23: Local Secure Group - IP Address and Remote Secure Group - IP Address	32
Figure 6-24: Local Secure Group - IP Range and Remote Secure Group - IP Range	32
Figure 6-25: Local Secure Group - Host and Remote Secure Group - Host	32
Figure 6-26: Local Secure Group - Subnet and Remote Secure Group - Any	32
Figure 6-27: Remote Secure Group - Any and Remote Secure Gateway - FQDN	33
Figure 6-28: Remote Security Group - Any and Remote Secure Gateway - Any	33
Figure 6-29: Key Exchange Method - Auto(IKE)	33
Figure 6-30: Key Exchange Method - Manual	34
Figure 6-31: Advanced VPN Tunnel Setup	35
Figure 6-32: Access Restrictions Tab - Internet Access	37
Figure 6-33: Internet Filter Summary	37
Figure 6-34: List of PCs	38
Figure 6-35: Blocked Services	38
Figure 6-36: Access Restrictions Tab - VPN Client Access	40
Figure 6-37: Applications & Gaming Tab - Port Range Forwarding	41
Figure 6-38: Applications & Gaming Tab - Port Triggering	42
Figure 6-39: Applications & Gaming Tab - UPnP Forwarding	43
Figure 6-40: Applications & Gaming Tab - DMZ	44
Figure 6-41: Administration Tab - Management	45
Figure 6-42: Administration Tab - Log	47
Figure 6-43: Administration Tab - Diagnostics	49
Figure 6-44: Administration Tab - Factory Default	50
Figure 6-45: Administration Tab - Firmware Upgrade	51
Figure 6-46: Status Tab - Router	52
Figure 6-47: Status Tab - Local Network	53
Figure 6-48: DHCP Active IP Table	53
Figure 6-49: Status Tab - Wireless	54
Figure 6-50: Status Tab - System Performance	55
Figure 6-51: Status Tab - VPN Clients	57
Figure 7-1: Registration Login	61
Figure 7-2: Welcome	61

Figure 7-3: Operator Agreement	62
Figure 7-4: Business Contact Information	62
Figure 7-5: Credit Card Information	63
Figure 7-6: Select a Username and Password	63
Figure 7-7: Confirmation	64
Figure 7-8: Registration Complete	64
Figure 7-9: Device Location	65
Figure 7-10: Onsite Contact	65
Figure 7-11: Device Configuration	66
Figure 7-12: View/Edit Settings	66
Figure 7-13: Your Location Page	67
Figure 7-14: Sample Page	67
Figure 7-15: Free Access	68
Figure 7-16: Confirmation	69
Figure 7-17: Almost Done	70
Figure 7-18: Administration Login	72
Figure 7-19: Home	72
Figure 7-20: Device View	73
Figure 7-21: Edit Current Configuration	74
Figure 7-22: Map	74
Figure 7-23: User Statistics	75
Figure 7-24: Device Statistics	75
Figure 7-25: Device Performance	76
Figure 7-26: Device Alerts	77
Figure C-1: Setup Wizard - Welcome Screen	97
Figure C-2: QuickVPN Desktop Icon	98
Figure C-3: QuickVPN Tray Icon - No Connection	98
Figure C-4: QuickVPN Software - Profile	98
Figure C-5: QuickVPN Software - Status	98
Figure C-6: QuickVPN Tray Icon - Connection Available	98
Figure C-7: QuickVPN Software - Change Password	98
Figure D-1: Local Security Screen	100
Figure D-2: Rules Tab	100

Figure D-3: IP Filter List Tab	100
Figure D-4: IP Filter List	101
Figure D-5: Filters Properties	101
Figure D-6: New Rule Properties	101
Figure D-7: IP Filter List	102
Figure D-8: Filters Properties	102
Figure D-9: New Rule Properties	102
Figure D-10: IP Filter List Tab	103
Figure D-11: Filter Action Tab	103
Figure D-12: Security Methods Tab	103
Figure D-13: Authentication Methods	104
Figure D-14: Preshared Key	104
Figure D-15: New Preshared Key	104
Figure D-16: Tunnel Setting Tab	105
Figure D-17: Connection Type Tab	105
Figure D-18: Properties Screen	105
Figure D-19: IP Filter List Tab	106
Figure D-20: Filter Action Tab	106
Figure D-21: Authentication Methods Tab	106
Figure D-22: Preshared Key	107
Figure D-23: New Preshared Key	107
Figure D-24: Tunnel Setting Tab	107
Figure D-25: Connection Type	108
Figure D-26: Rules	108
Figure D-27: Local Computer	108
Figure D-28: VPN Tab	109
Figure E-1: Diagram of All VPN Tunnels	110
Figure E-2: Login Screen	111
Figure E-3: Setup - Basic Setup (Internet Setup)	111
Figure E-4: Security - VPN Screen (VPN Tunnel)	111
Figure E-5: Setup - Basic Setup (Internet Setup)	112
Figure E-6: Security - VPN Screen (VPN Tunnel)	112
Figure E-7: Diagram of VPN Tunnel between VPN Routers	113

Figure E-8: Security - VPN Screen (Key Management)	113
Figure E-9: Advanced Tunnel Setup Screen	114
Figure E-10: Access Restrictions - VPN Client Access Screen	115
Figure E-11: Diagram of VPN Tunnel between VPN Router 1 and VPN Client	115
Figure E-12: QuickVPN Desktop Icon	115
Figure E-13: QuickVPN Software - Profile	115
Figure E-14: Connecting	116
Figure E-15: Activating Policy	116
Figure E-16: Verifying Network	116
Figure E-17: QuickVPN Software - Status	116
Figure E-18: QuickVPN Tray Icon - Connection	116
Figure E-19: QuickVPN Tray Icon - No Connection	116
Figure F-1: IP Configuration Screen	117
Figure F-2: MAC Address/Adapter Address	117
Figure F-3: MAC Address/Physical Address	118
Figure H-1: Upgrade Firmware	120

Chapter 1: Introduction

Welcome

Thank you for choosing the Linksys Wireless-G VPN Broadband Router. The Wireless-G VPN Broadband Router will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely.

How does the Wireless-G VPN Broadband Router do all of this? A router is a device that allows access to an Internet connection over a network. With the Wireless-G VPN Broadband Router, this access can be shared over the four switched ports or via the wireless network, broadcast at either 11Mbps for Wireless-B or 54Mbps for Wireless-G.

To protect your data and privacy, the Wireless-G VPN Broadband Router can encrypt all wireless transmissions with up to 128-bit WEP encryption and supports the WPA standard, which provides greater security opportunities. The Router also has a powerful Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology to protect your PCs against intruders and most known Internet attacks. Its Virtual Private Network (VPN) function creates encrypted “tunnels” through the Internet so up to 50 remote or traveling users can securely connect to your office network from off-site, or users in your branch office can connect to a corporate network. All of these security features, as well as full configurability, are accessed through the easy-to-use browser-based utility.

But what does all of this mean?

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun.

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called “wired”.

PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. The Wireless-G VPN Broadband Router bridges wireless networks of both 802.11b and 802.11g standards and wired networks, allowing them to communicate with each other.

With your networks all connected, wired, wireless, and the Internet, you can now share files and Internet access—and even play games. All the while, the Wireless-G VPN Broadband Router protects your networks from unauthorized and unwelcome users.

vpn (virtual private network): A security measure to protect data as it leaves one network and goes to another over the Internet

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

wpa (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server

nat (network address translation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet

spi (stateful packet inspection) firewall: A technology that inspects incoming packets of information before allowing them to enter the network

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

lan (local area network): The computers and networking products that make up the network in your home or office

You should always use the Setup CD-ROM when you first install the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then use the instructions in this Guide to help you connect the Wireless-G VPN Broadband Router, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-G VPN Broadband Router.

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: Planning Your Virtual Private Network (VPN)**
This chapter describes a VPN and its various applications.
- **Chapter 4: Getting to Know the Wireless-G VPN Broadband Router**
This chapter describes the physical features of the Router.
- **Chapter 5: Connecting the Wireless-G VPN Broadband Router**
This chapter instructs you on how to connect the Router to your network.
- **Chapter 6: Configuring the Wireless-G VPN Broadband Router**
This chapter explains how to use the Web-Based Utility to configure the settings on the Router.
- **Chapter 7: Boingo Hot Spot in a Box for Hot Spot Businesses**
This chapter explains how to sign up for the Boingo Hot Spot in a Box program.
- **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: Using the Linksys QuickVPN Software for Windows 2000 or XP**
This appendix instructs you on how to use the Linksys QuickVPN software if you are using a Windows 2000 or XP PC.

- **Appendix D: Configuring IPSec between a Windows 2000 or XP 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 E: Configuring VPN Tunnels**
This appendix describes how to configure VPN IPSec tunnels using the VPN Routers and a VPN client.
- **Appendix F: Finding the MAC Address and IP Address for your Ethernet Adapter.**
This appendix 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. It also explains how to find the IP address for your computer.
- **Appendix G: SNMP Functions**
This appendix explains SNMP (Simple Network Management Protocol).
- **Appendix H: Upgrading Firmware**
This appendix instructs you on how to upgrade the firmware on your Router should you need to do so.
- **Appendix I: Windows Help**
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- **Appendix J: Glossary**
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix K: Specifications**
This appendix provides the technical specifications for the Router.
- **Appendix L: Warranty Information**
This appendix supplies the warranty information for the Router.
- **Appendix M: Regulatory Information**
This appendix supplies the regulatory information regarding the Router.
- **Appendix N: Contact Information**
This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers in a WLAN share the same frequency channel and SSID, which is an identification name shared by the wireless devices belonging to the same wireless network.

Ad-Hoc versus Infrastructure Mode

Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. An ad-hoc configuration is wireless-equipped computers communicating directly with each other. Choosing between these two modes depends on whether or not the wireless network needs to share data or peripherals with a wired network or not.

If the computers on the wireless network need to be accessible by a wired network or need to share a peripheral, such as a printer, with the wired network computers, the wireless network should be set up in Infrastructure mode. The basis of Infrastructure mode centers around an access point or wireless router, such as the Wireless-G VPN Broadband Router, which serves as the main point of communications in a wireless network. The Router transmits data to PCs equipped with wireless network adapters, which can roam within a certain radial range of the Router. You can arrange the Router and multiple access points to work in succession to extend the roaming range, and you can set up your wireless network to communicate with your Ethernet hardware as well.

If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the Ad-Hoc mode can be used. Ad-Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for a wireless router or access point. The drawback of this mode is that in Ad-Hoc mode, wireless-equipped computers are not able to communicate with computers on a wired network. And, of course, communication between the wireless-equipped computers is limited by the distance and interference directly between them.

Network Layout

The Wireless-G VPN Broadband Router has been specifically designed for use with both your 802.11b and 802.11g products. Now, products using these standards can communicate with each other.

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

lan (local area network): The computers and networking products that make up the network in your home or office

ssid: your wireless network's name

ad-hoc: a group of wireless devices communicating directly to each other (peer-to-peer) without the use of an access point

infrastructure: a wireless network that is bridged to a wired network via an access point

adapter: a device that adds network functionality to your PC

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

access point: a 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

Wireless-G VPN Broadband Router

The Wireless-G VPN Broadband Router is compatible with all 802.11b and 802.11g adapters, such as the Notebook Adapters (WPC54G, WPC11) for your laptop computers, PCI Adapter (WMP54G, WMP11) for your desktop PC, and USB Adapter (WUSB54G, WUSB11) when you want to enjoy USB connectivity. The Broadband Router will also communicate with the Wireless PrintServer (WPS54GU2, WPS11) and Wireless Ethernet Bridges (WET54G, WET11).

When you wish to connect your wireless network with your wired network, you can use the Broadband Router's three LAN ports. To add more ports, any of the Broadband Router's LAN ports can be connected to any of Linksys's switches (such as the EZXS55W or EZXS88W).

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 Wireless-G VPN Broadband Router.



Figure 2-1: Network Diagram

Chapter 3: Planning Your Virtual Private Network (VPN)

Why do I need a VPN?

Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when e-mails 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 e-mail 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

***vpn** (virtual private network): a security measure to protect data as it leaves one network and goes to another over the Internet*

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

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 the Linksys VPN client software.)

There are two basic ways to create a VPN connection:

- VPN Router to VPN Router
- Computer (using the Linksys VPN client software) to VPN Router



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

The VPN Router creates a “tunnel” or channel between two endpoints, so that data transmissions between them are secure. A computer with the Linksys VPN client software can be one of the two endpoints (refer to “Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP”). If you choose not to run the VPN client software, 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 D: Configuring IPSec between a Windows 2000 or XP PC

encryption: encoding data transmitted in a network

ip (internet protocol): a protocol used to send data over a network

software: instructions for the computer

and the Router”). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

VPN Router to VPN Router

An example of a VPN Router-to-VPN Router VPN would be as follows. At home, a telecommuter uses his VPN Router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected. For more information, refer to “Appendix E: Configuring VPN Tunnels.”

Computer (using the Linksys VPN client software) to VPN Router

The following is an example of a computer-to-VPN Router VPN. In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has the Linksys VPN client software, which is configured with her office's IP address. She accesses the Linksys VPN client software 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. You can also refer to “Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP”, “Appendix D: Configuring IPSec between a Windows 2000 or XP PC and the Router,” and “Appendix E: Configuring VPN Tunnels.”



Figure 3-1: VPN Router to VPN Router



Figure 3-2: Computer to VPN Router

Chapter 4: 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 4-1: Back Panel

Internet	The Internet port connects to your cable or DSL modem.
LAN (1-4)	The LAN (Local Area Network) ports connect to your PCs and other network devices.
Reset Button	There are two ways to reset the Router's factory defaults. Either press the Reset Button , for approximately five seconds, or restore the defaults from the Administration tab - Factory Defaults in the Router's Web-based Utility.
Power	The Power port is where you will connect the power adapter.



IMPORTANT: If you reset the Router, all of your settings, including Internet connection, wireless, and security, will be deleted and replaced with the factory defaults. Do not reset the Router if you want to retain these settings.

The Front Panel

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

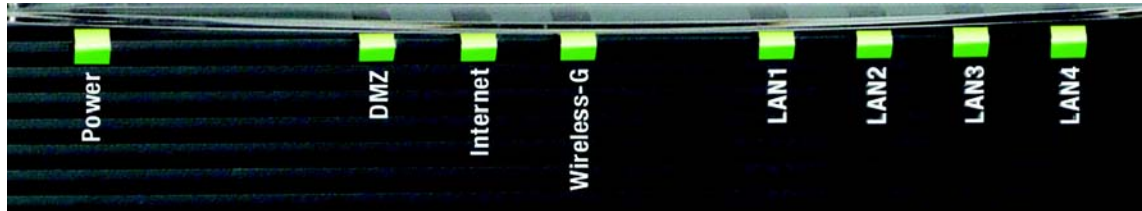


Figure 4-2: Front Panel

Power	Green. The Power LED lights up when the Router is powered on.
DMZ	Red. The DMZ LED lights up when the Router has an available DMZ port. If the LED is flashing, the Router is sending or receiving data over the DMZ port.
Internet	Green. The Internet LED lights up when the Router is connected to your cable or DSL modem. If the LED is flashing, the Router is sending or receiving data over the Internet port.
Wireless-G	Green. The Wireless-G LED lights whenever there is a successful wireless connection. If the LED is flashing, the Router is actively sending or receiving data over the wireless network.
LAN (1-4)	Green. The LAN LED serves two purposes. If the LED is solidly lit, the Router is connected to a device through the corresponding port (LAN 1, 2, or 3). If the LED is flashing, the Router is sending or receiving data over that port.

Chapter 5: Connecting the Wireless-G VPN Broadband Router

Overview

To begin installation of the Router, you will connect the Router to your PCs, other network devices, and cable or DSL modem. 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. 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. Then connect the other end to an Ethernet port on a PC.
3. Repeat step 2 to connect additional PCs 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.
5. Power on the cable or DSL modem.
6. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet.



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

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, and then it will be solidly lit 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.

The Router's hardware installation is now complete.

Go to “Chapter 6: Configuring the Wireless-G VPN Broadband Router.”



Figure 5-1: Connect to LAN Ports



Figure 5-2: Connect to Internet Port



Figure 5-3: Connect to Power Port

Wireless Connection to a PC

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

1. 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.
3. Power on the cable or DSL modem.
4. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet.



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

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, and then it will be solidly lit 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 disabled. After you have accessed the Router, you can change the Router and this PC's adapter settings to match your usual network settings.

The Router's hardware installation is now complete.

Go to "Chapter 6: Configuring the Wireless-G VPN Broadband Router."



Figure 5-4: Connect to Internet Port



Figure 5-5: Connect to Power Port



NOTE: You should change the SSID from its default, **linksys**, and enable WEP encryption after you have accessed the Router.

Chapter 6: Configuring the Wireless-G VPN Broadband Router

Overview

Linksys recommends using the Setup CD-ROM for first-time installation of the Router. 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. For advanced users, you may configure the Router's advanced settings through the Web-based Utility.

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.** On this screen, enable the Router's Dynamic Domain Name System (DDNS) feature.
- **MAC Address Clone.** If you need to clone a MAC address onto the Router, use this screen.
- **Advanced Routing.** On this screen, configure the dynamic and static routing configuration.
- **Hot Spot.** To enable the Hot Spot in a Box feature and turn your Router into a commercial Hot Sport, register with your Hot Spot service provider on this screen.

Wireless

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



NOTE: When first installing the Router, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the Web-based Utility.



HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix I: 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.** For advanced users, you can alter data transmission settings on this screen.

Security

- **Firewall.** On this screen, you can configure a variety of filters to enhance the security of your network.
- **VPN.** To enable or disable IPSec, L2TP, and/or PPTP Pass-through, and set up VPN tunnels, use this screen.

Access Restrictions

- **Internet Access.** This screen allows you to permit or block specific users from connecting to your network.
- **VPN Client Access.** Use this screen to designate VPN clients and their passwords.

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.** Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services.

Administration

- **Management.** Alter the Router's password, its access privileges, SNMP settings, 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 the Router and a 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.

Status

- **Router.** This screen provides status information about the Router.

- **Local Network.** This provides status information about the local network.
- **Wireless.** Status information about the wireless network is displayed here.
- **System Performance.** Status information is provided for all network traffic.
- **VPN Clients.** This screen provides status information about the Router's VPN clients.

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 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.

Make the necessary changes through the Utility. When you have finished making changes to a screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

The Setup Tab - Basic Setup

The first screen that appears is the Basic Setup tab. This tab allows you to change the Router's general settings.

Internet Setup

The Internet Setup section configures the Router for your Internet connection type. This information can be obtained from your ISP.

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 6-1: Login Screen

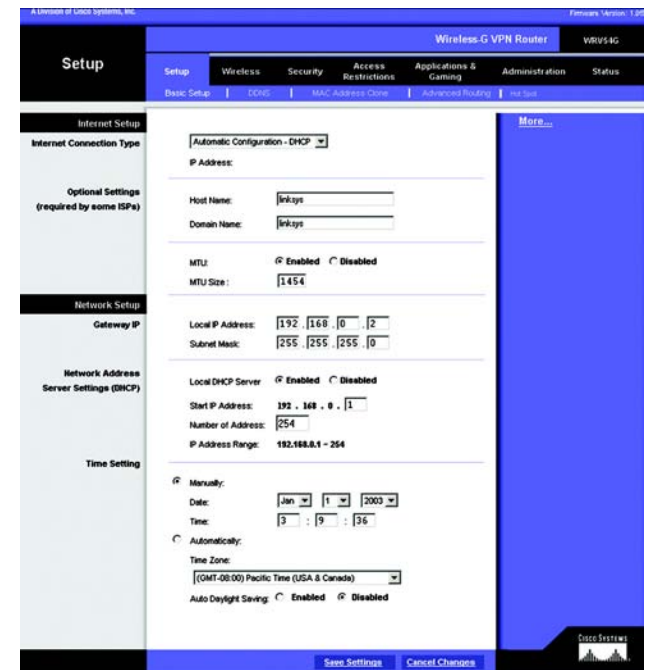


Figure 6-2: Setup Tab - Automatic Configuration - DHCP

Static IP

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 you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

PPPoE

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 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 you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

Static IP

IP Address: 10 . 0 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

Primary DNS : 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Figure 6-3: Internet Connection Type - Static IP

static ip address: a fixed address assigned to a computer or device connected to a network.

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

default gateway: a device that forwards Internet traffic from your local area network

PPPoE

User Name: linksys

Password:

☐ Connect on Demand: Max Idle Time 5 Min.

☒ Keep Alive : Redial Period 30 Sec.

Figure 6-4: Internet Connection Type - PPPoE

pppoe: a type of broadband connection that provides authentication (username and password) in addition to data transport

PPTP

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

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.

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**. 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 you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

Optional Settings (Required by some ISPs)

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.

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.

PPTP

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

User Name:

Password:

☐ Connect on Demand: Max Idle Time 5 Min.

☒ Keep Alive : Redial Period 30 Sec.

Figure 6-5: Internet Connection Type - PPTP

packet: a unit of data sent over a network

Network Setup

The Network Setup section allows you to change the Router's local network settings.

Gateway IP

The Router's Local IP Address and Subnet Mask are shown here. In most cases, you should keep the defaults.

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)

The Router can be used as your network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each PC on your network. 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 **Disabled**. If you disable DHCP, 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, but smaller than 192.168.1.254, 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.

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

Time Setting

This is where you set the time for the Router. You can set the time and date manually or automatically.

Manually. Select the date from the *Date* drop-down menus. Then enter the time in the *Time* fields.

Automatically. Select your time zone from the *Time Zone* drop-down menu. If you want to enable the Automatic Daylight Savings feature, click the **Enabled** radio button.

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

The Setup Tab - DDNS

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

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

DDNS

If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** in the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. 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 you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

TZO.com

Email, 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 you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

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



Figure 6-6: DDNS Tab - DynDNS.org



Figure 6-7: DDNS Tab - TZO.com

The Setup Tab - MAC Address Clone

The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. Some ISPs require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router using the MAC Address Clone feature. If you need to find your adapter's MAC address, follow the instructions in "Appendix F: Finding the MAC Address and IP Address for Your Ethernet Adapter."

MAC Clone

To use MAC address cloning, select **Enabled**.

MAC Clone Address. Enter the MAC Address registered with your ISP. 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 you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

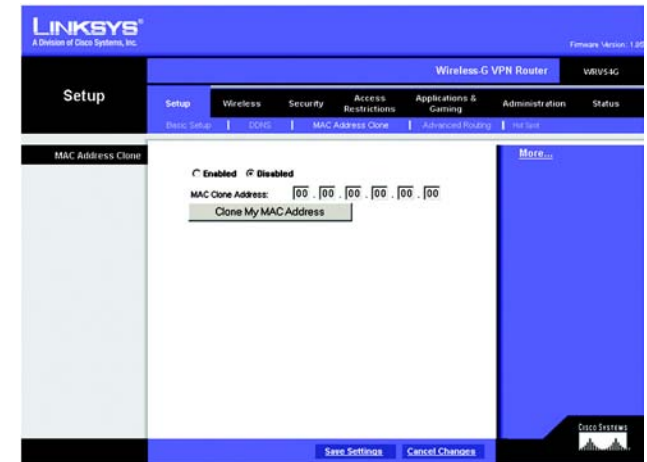


Figure 6-8: Setup Tab - MAC Address Clone

***mac address:** the unique address that a manufacturer assigns to each networking device.*

The Setup Tab - Advanced Routing

The *Advanced Routing* screen allows you to configure the dynamic and static routing settings.

Advanced Routing

Operating Mode. Select **Gateway** or **Router** from the drop-down menu. If this Router is hosting your network's connection to the Internet, keep the default, **Gateway**. If you have a different router hosting your Internet connection, then select **Router**.

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.

RIP. To use dynamic routing, click the **Enabled** radio button.

Receive RIP Version. To use dynamic routing for reception of network data, select the protocol you want: **Both RIP v1 and v2**, **RIPv1**, or **RIPv2**. If you do not want to use this feature, select **None**.

Transmit RIP Version. To use dynamic routing for transmission of network data, select the protocol you want: **RIPv1**, **RIPv2-Broadcast**, or **RIPv2-Multicast**. If you do not want to use this feature, select **None**.

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 This 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

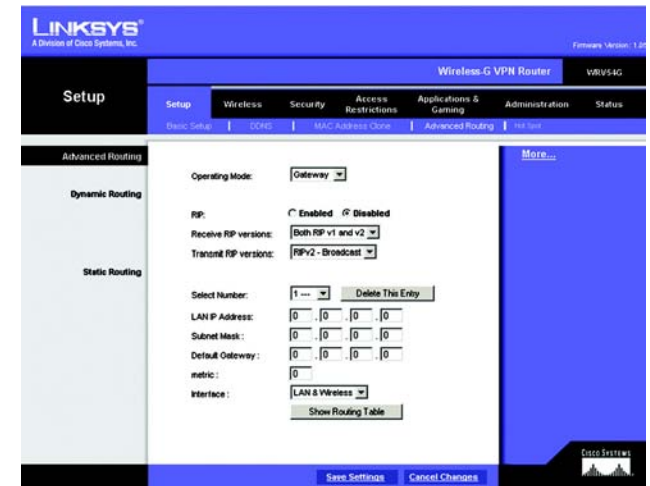


Figure 6-9: Setup Tab - Advanced Routing

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.

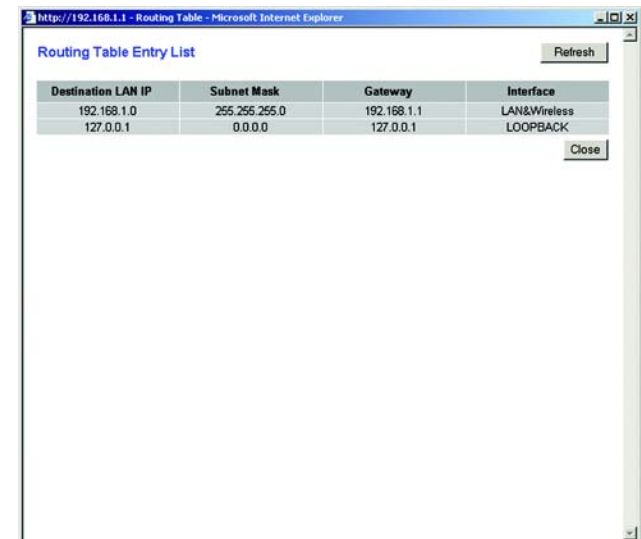
Default Gateway. Enter the IP address of the gateway device that allows for contact between the Router and the remote network or host.

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 (WAN)**, 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 local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to exit this screen.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.



Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	192.168.1.1	LAN&Wireless
127.0.0.1	0.0.0.0	127.0.0.1	LOOPBACK

Figure 6-10: Routing Table Entry List

The Setup Tab - Hot Spot

The Hot Spot tab is for business owners who want to generate revenue by turning the Router into a commercial Hot Spot using Boingo™ Hot Spot in a Box®.

For additional information, click the **More Info** button or refer to “Chapter 7: Boingo™ Hot Spot in a Box® Program for Hot Spot Businesses.”

To start the registration process, click the **Register** button.

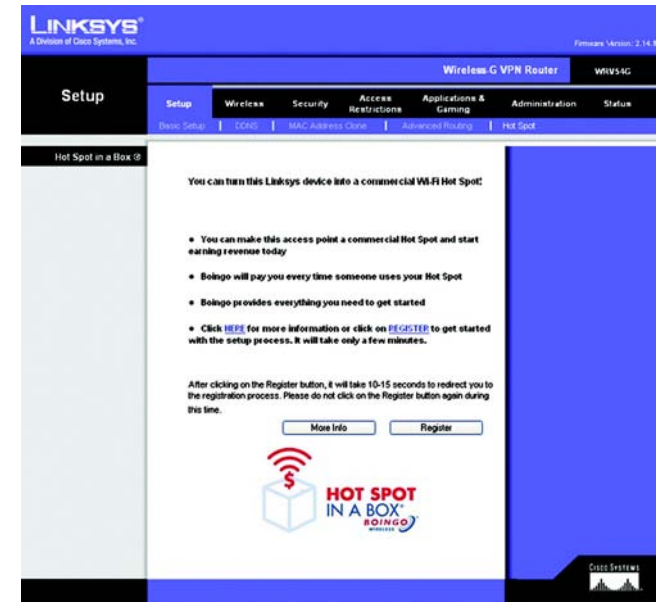


Figure 6-11: Setup Tab - Hot Spot in a Box

The Wireless Tab - Basic Wireless Settings

The basic settings for wireless networking are configured on this screen.

Wireless Network

Wireless Network Mode. From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed**. If you have only 802.11g devices, select **G-Only**. If you have only 802.11b devices, select **B-Only**. If you do not have any 802.11g and 802.11b devices in your network, select **Disable**.

Wireless Network Name (SSID). The SSID is the network name shared among all points 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 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (**linksys-g**) to a unique name.

Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

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, **Enable**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

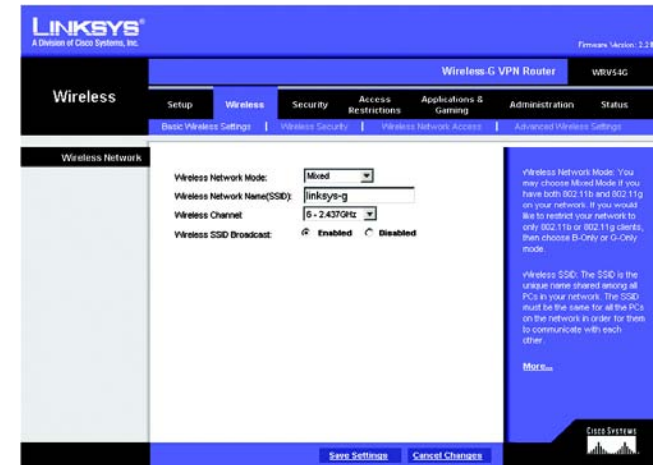


Figure 6-12: Wireless Tab - Basic Wireless Settings

The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are four wireless security mode options supported by the Router: WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These four are discussed here. Select the appropriate security mode for your network. For detailed instructions on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.”

WPA Pre-Shared Key. WPA gives you one encryption method, TKIP, with dynamic encryption keys. Select **TKIP** or **AES** from the *WPA Algorithm* drop-down menu. Enter a WPA Shared Key of 8-32 characters. Then enter the Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

WPA RADIUS. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Enter the RADIUS server's IP address. Select **TKIP** or **AES** from the *WPA Algorithm* drop-down menu. Enter the RADIUS server's port number, along with the Shared Secret key, which is the key shared between the Router and the server. Last, enter the Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

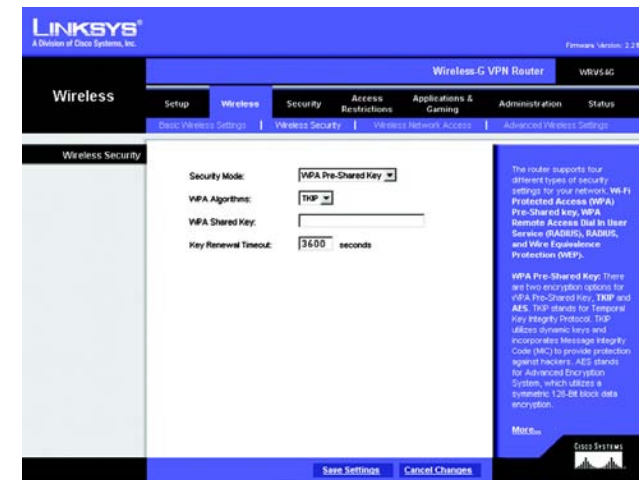


Figure 6-13: Wireless Security - WPA Pre-Shared Key

***wpa** (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server*

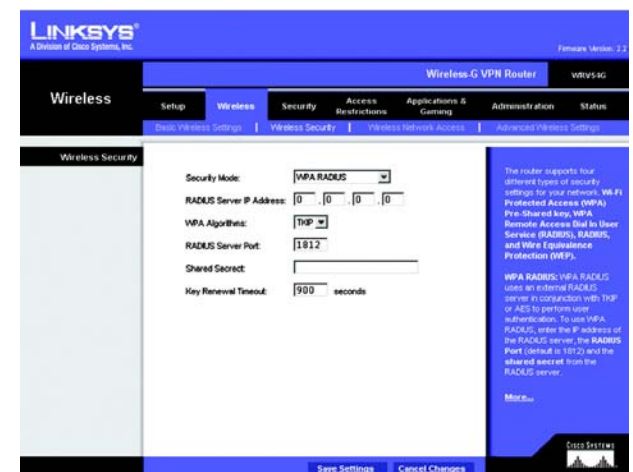


Figure 6-14: Wireless Security - WPA RADIUS

***radius:** a protocol that uses an authentication server to control network access*

RADIUS. This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) First, enter the RADIUS server's IP address and port number in the *RADIUS Server IP Address* and *RADIUS Server Port* fields. Enter the key shared between the Router and the server in the *Shared Secret* field.

To indicate which WEP key to use, select the appropriate *Default Transmit Key* number. Then, select the level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

Instead of manually entering WEP keys, you can enter a Passphrase to generate one or more WEP keys. The Passphrase is case-sensitive and should have no more than 32 alphanumeric characters. If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button.

If you want to enter the WEP key(s) manually, then enter it in the *Key 1-4* field(s). (Do not leave a field blank, and do not enter all zeroes; they are not valid key values.) If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0" to "9" and "A" to "F".

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

WEP. WEP is a basic encryption method, which is not as secure as WPA. To indicate which WEP key to use, select the appropriate *Default Transmit Key* number. Then, select the level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

Instead of manually entering WEP keys, you can enter a Passphrase to generate one or more WEP keys. The Passphrase is case-sensitive and should have no more than 32 alphanumeric characters. If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button.

If you want to enter the WEP key(s) manually, then enter it in the *Key 1-4* field(s). (Do not leave a field blank, and do not enter all zeroes; they are not valid key values.) If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0" to "9" and "A" to "F".

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

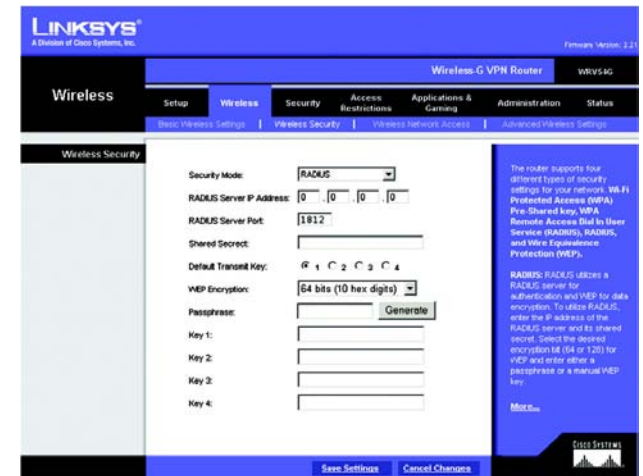


Figure 6-15: Wireless Security - RADIUS



Figure 6-16: Wireless Security - WEP

wep (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security

The Wireless Tab - Wireless Network Access

This screen allows you to control access to your wireless network.

Wireless Network Access

Access List. To allow the designated computers to access your network, select the **Permit to access** radio button. To block the designated computers from accessing your wireless network, select the **Prevent from accessing** radio button. Click **Disabled** to disable the access function.

MAC 1-20. Enter the MAC addresses of the designated computers. For a more convenient way to add MAC addresses, click the **Select MAC Address From Networked Computers** button. The *Networked Computers* screen will appear. Select the MAC Addresses you want. Then click the **Select** button. Click the **Refresh** button if you want to refresh the screen. Click the **Close** button to return to the previous screen.

If you want detailed instructions on how to find the MAC address of a specific computer, refer to “Appendix F: Finding the MAC Address or IP Address for Your Ethernet Adapter.”

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

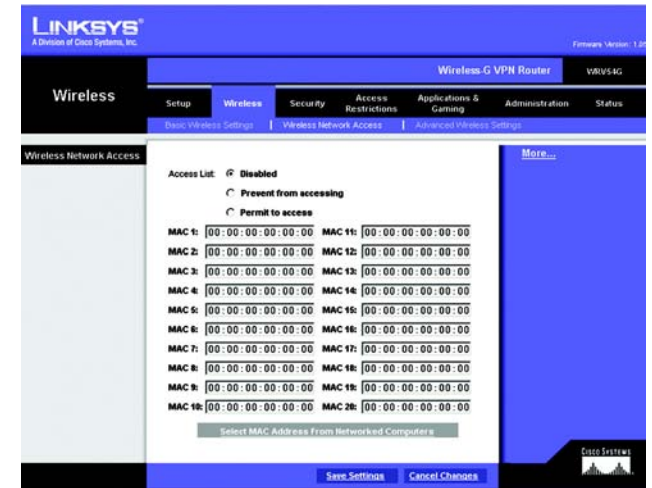


Figure 6-17: Wireless Tab - Wireless Network Access

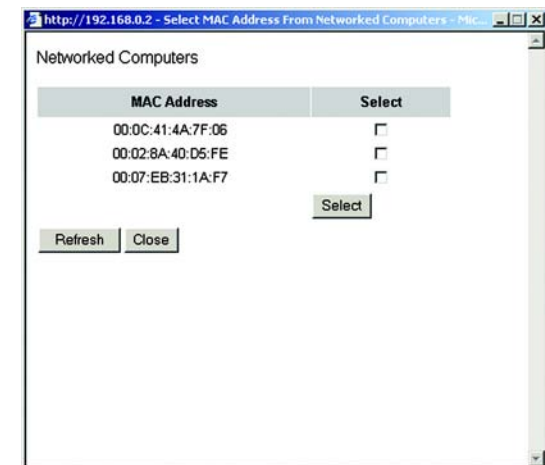


Figure 6-18: Networked Computers

The Wireless Tab - Advanced Wireless Settings

This tab is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an advanced user as incorrect settings can reduce wireless performance.

Advanced Wireless

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. Select the appropriate authentication type for your network. 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.

Basic Data Rates. Select **1-2 Mbps**, **All (1-2-5.5-6-11-24)**, or **Default (1-2-5.5-11)**, from the drop-down menu. The Basic Data Rates setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Data Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates (1-2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 24Mbps). The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Control Tx Rate setting.

Control Tx Rates. The default value 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, 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. The RTS Threshold value should remain at its default value of **2347**. Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is

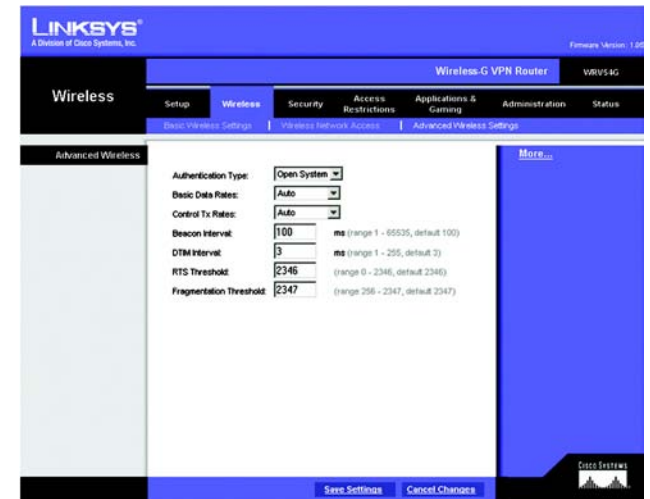


Figure 6-19: Wireless Tab - Advanced Wireless Settings

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

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. In most cases, this value should remain at its default value of **2346**. 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 reduction of the default value is recommended.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

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

The Security Tab - Firewall

When you click the Security tab, you will see the *Firewall* screen. The Router's firewall enhances the security of your network. You can also enable a variety of filters to further protect your network.

Firewall

Firewall Protection. The firewall uses Stateful Packet Inspection (SPI) to check the incoming data transmissions before allowing them to enter your network. To use the Router's firewall, click **Enabled**. If you do not want firewall protection, click **Disabled**.

Additional Filters

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 WAN Requests

Block Anonymous Internet Requests. This keeps your network from being “pinged” or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to work their way into your network. Select **Enabled** to block anonymous Internet requests, or **Disabled** to allow anonymous Internet requests.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

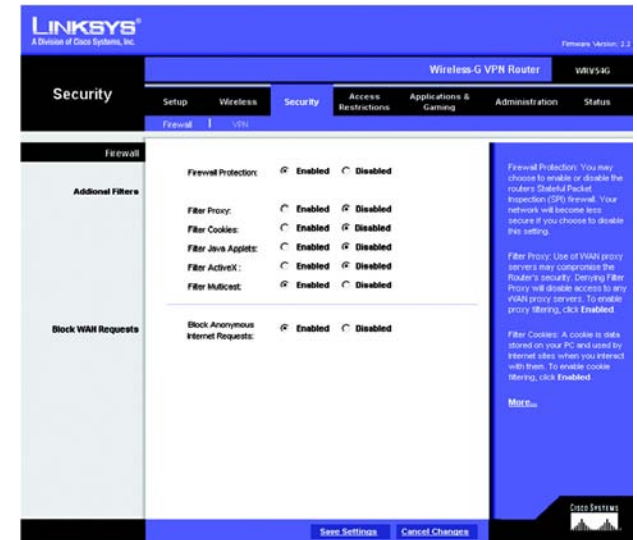


Figure 6-20: Security Tab - Firewall

***spi (stateful packet inspection) firewall:** A technology that inspects incoming packets of information before allowing them to enter the network*

The Security Tab - 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 allows you to configure your VPN settings to make your network more secure.

VPN PassThrough

IPSec Passthrough. IPSec (Internet Protocol Security) 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. PPTP (Point-to-Point Tunneling Protocol) Passthrough allows the Point-to-Point (PPP) to be tunneled through an IP network. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.

L2TP Passthrough. Layer 2 Tunneling Protocol Passthrough is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP Passthrough, click the **Enabled** button. To disable L2TP Passthrough, click the **Disabled** button.

VPN Tunnel

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

Select Tunnel Entry. To establish this tunnel, select the tunnel you wish to create from the drop-down box. It is possible to create up to 100 simultaneous tunnels.

VPN Tunnel. Click **Enabled** to enable the selected VPN Tunnel.

VPN Gateway. If you want to route all the traffic through the tunnel, and not just the ones destined for the remote secure group, click **Enabled**.

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

Local Secure Group

The Local Secure Group is the computer(s) on your LAN that can access the tunnel. From the drop-down menu, select **Subnet**, to include the entire network for the tunnel; select **IP Address** if you want a specific computer; **IP Range**, if you want to include a range of IP addresses; or select **Host**, which is used with Port Forwarding to

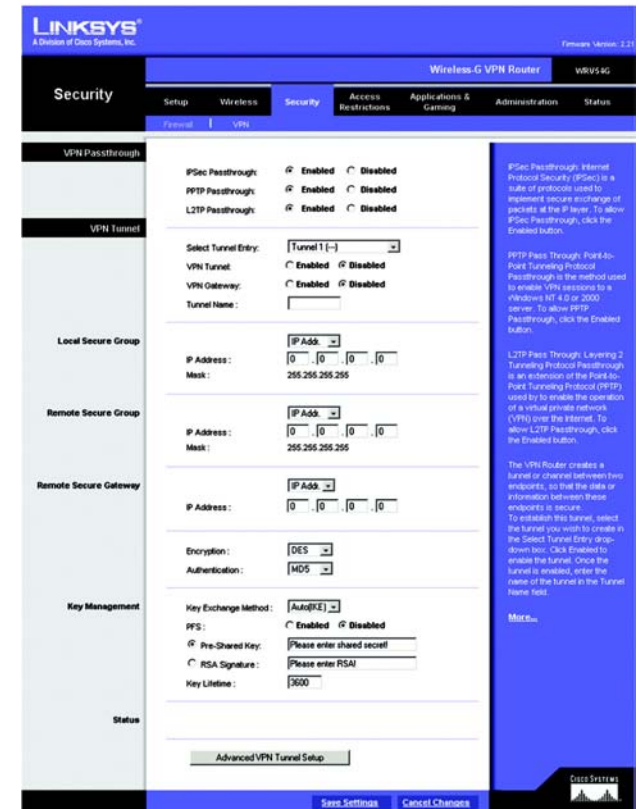


Figure 6-21: Security Tab - VPN



Figure 6-22: Local Secure Group - Subnet and Remote Secure Group - Subnet

direct the traffic to the correct computer. The screen will change depending on the selected option. The options are described below.

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

IP Address. Enter the IP Address of the local VPN Broadband Router. The Mask will be displayed.

IP Range. Enter the starting and ending numbers for the IP address range.

Host. The VPN tunnel will terminate at the router with this setting. Use Port Range Forwarding to direct traffic to the correct computer. Refer to the Port Range Forwarding tab of the Applications and Gaming tab.

Remote Secure Group

The Remote Secure Group is the computer(s) on the remote end of the tunnel that can access the tunnel. From the drop-down menu, select **Subnet**, to include the entire network for the tunnel; select **IP address** if you want a specific computer; IP Range, if you want to include a range of IP addresses; select **Host**, if the VPN will terminate at the Router, instead of the PC; or **Any**, to allow any computer to access the tunnel. The screen will change depending on the selected option. The options are described below.

Subnet. Enter the IP Address and Mask of the remote VPN router in the fields provided. To allow access to the entire IP subnet, enter **0** for the last set of IP Addresses. (e.g. 192.168.1.0).

IP Address. Enter the IP Address of the remote VPN router. The Mask will be displayed.

IP Range. Enter the starting and ending numbers for the IP Address range.

Remote Secure Gateway

The Remote Secure 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, depending on the settings of the remote VPN device.

If the IP Address is static, select **IP Addr.** and enter the IP address. 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 Broadband Router; it is the IP address of the remote VPN router or device with which you wish to communicate. If the IP address is dynamic, select **FQDN** for DDNS or **Any**. If FQDN is selected, enter the domain name of the remote router, so the Router can locate a current IP address using DDNS. If Any is selected, then the Router will accept requests from any IP address.

Figure 6-23: Local Secure Group - IP Address and Remote Secure Group - IP Address

Figure 6-24: Local Secure Group - IP Range and Remote Secure Group - IP Range

Figure 6-25: Local Secure Group - Host and Remote Secure Group - Host

Figure 6-26: Local Secure Group - Subnet and Remote Secure Group - Any

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 to disable this feature.

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

Key Management

Key Exchange Method. Select **Auto (IKE)** or **Manual** for the Key Exchange Method. Both ends of a VPN tunnel must use the same mode of key management. The two methods are described below. After you have selected the method, the settings available on this screen may change, depending on the selection you have made.

Auto (IKE)

IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Pre-shared Key to authenticate the remote IDE peer.

PFS. PFS (Perfect Forward Secrecy) ensures that the initial key exchange and IKE proposals are secure. To use PFS, click the **Enabled** radio button.

Pre-shared Key. You can choose to use a Pre-shared Key or RSA Signature. To use the Pre-shared Key, click its radio button. enter a series of numbers or letters in the *Pre-shared Key* field. Based on this word, which **MUST** be entered at both ends of the tunnel, 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.

RSA Signature. You can choose to use a Pre-shared Key or RSA Signature. To use the RSA Signature, click its radio button. Enter the RSA Signature in the field provided. (This is similar to a Pre-shared Key. Make sure it matches the RSA Signature entered at the remote end of the tunnel.s

Key Lifetime. 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

If you select Manual, you generate the key yourself, and no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes.

Figure 6-27: Remote Secure Group - Any and Remote Secure Gateway - FQDN

Figure 6-28: Remote Security Group - Any and Remote Secure Gateway - Any

Figure 6-29: Key Exchange Method - Auto(IKE)

Encryption Algorithm. Select a method of encryption, **DES** or **3DES**. This determines the length of the key used to encrypt or decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

Encryption Key. This field specifies a key used to encrypt and decrypt IP traffic. Enter a key of hexadecimal values. If DES is selected, the Encryption Key is 16-bit, which requires 16 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Encryption Key will be 16-bit. If 3DES is selected, the Encryption Key is 48-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Encryption Key will be 48-bit. Make sure both ends of the VPN tunnel use the same Encryption Key.

Authentication Algorithm. Select a method of authentication, **MD5** or **SHA1**. The Authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

Authentication Key. This field specifies a key used to authenticate IP traffic. Enter a key of hexadecimal values. If MD5 is selected, the Authentication Key is 32-bit, which requires 32 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes until it has 32 hexadecimal values. If SHA is selected, the Authentication Key is 40-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes until it has 40 hexadecimal values. Make sure both ends of the VPN tunnel use the same Authentication Key.

Inbound & Outbound SPI (Security Parameter Index). SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to select the SA, under which a packet should be processed. Hexadecimal values is acceptable, and the valid range is 100~ffffff. Each tunnel must have a unique Inbound SPI and Outbound SPI. No two tunnels share the same SPI. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.

Status

The status information for the Router's VPN tunnels is displayed here. Click the **Disconnect** button to terminate the VPN connection.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

Key Exchange Method :	<input type="text" value="Manual"/>
Encryption Algorithm:	<input type="text" value="DES"/> (DES:16 HEX 3DES:48 HEX)
Encryption Key:	<input type="text" value="0000000000000000"/>
Authentication Algorithm:	<input type="text" value="MD5"/> (MD5:32 HEX SHA1:40 HEX)
Authentication Key:	<input type="text" value="000000000000000000000000"/>
Inbound SPI:	<input type="text" value="100"/> (HEX, 100-FFFFFF)
Outbound SPI:	<input type="text" value="100"/> (HEX, 100-FFFFFF)

Figure 6-30: Key Exchange Method - Manual

Advanced VPN Tunnel Setup

Click the **Advanced VPN Tunnel Setup** button, and the *Advanced VPN Tunnel Setup* screen will appear.

These advanced IPSec settings are for advanced users.

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 or 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 SHA1. SHA1 is recommended because it is more secure.

Group. There are three Diffie-Hellman Groups to choose from: 768-bit, 1024-bit, and 1536-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.

PFS. The status of the PFS (Perfect Forward Secrecy) feature will be displayed.

Group. There are three Diffie-Hellman Groups to choose from: 768-bit, 1024-bit, and 1536-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

The screenshot shows the 'Advanced VPN Tunnel Setup' interface. At the top, there's a blue header with the title 'Advanced VPN Tunnel Setup'. Below it, the 'Tunnel 1' configuration is displayed. Phase 1 settings include 'Operation Mode' set to 'Main', 'Proposal' with 'Encryption' as 'DES', 'Authentication' as 'MD5', 'Group' as '768-bit', and 'Key Life Time' as '3600'. A note below Phase 1 states: '(Note: Following three additional proposals are also proposed in Main mode: DES/MD5/768, 3DES/SHA1/1024 and 3DES/MD5/1024)'. Phase 2 settings show 'Proposal' with 'Encryption' as 'DES', 'Authentication' as 'MD5', 'PFS' as 'Enabled', 'Group' as '768-bit', and 'Key Life Time' as '28000'. At the bottom, there's an 'Other Options' section with checkboxes for 'NetBIOS broadcast' (unchecked), 'Anti-replay' (checked), 'Keep Alive' (unchecked), and 'If IKE failed more than 5 times, block this unauthorized IP for 60 seconds' (checked). At the very bottom are three buttons: 'Save Settings', 'Cancel Changes', and 'Help'.

Figure 6-31: Advanced VPN Tunnel Setup

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

NetBIOS broadcast. Click the checkbox if you want NetBIOS traffic to pass through the VPN tunnel. By default, the Router blocks these broadcasts.

Anti-replay. This protects the Router from anti-replay attacks, when people try to capture your authentication packets in an attempt to gain access. The feature is enabled by default.

Keep Alive. This feature helps maintain the connections of IPSec tunnels. Whenever a connection is dropped and the drop is detected, then the connection will be re-established immediately. Click the checkbox to enable this feature.

If IKE failed more than -- times, block this unauthorized IP for -- seconds. This feature is enabled by default. It enables the Router to block unauthorized IP addresses. Specify the number of times IKE must fail before the Router blocks that unauthorized IP address. Then specify how many seconds you want the unauthorized IP address to be blocked.

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

The Access Restrictions Tab - Internet Access

The *Internet Access* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, websites, and inbound traffic during specific days and times.

Internet Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete** button. To view all the policies, click the **Summary** button.

Status. Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside *Enable*.

You can create two kinds of policies, one kind to manage Internet access and another kind to manage inbound traffic.

To create an Internet Access Policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.
4. Select **Internet Access** as the Policy Type.
5. Click the **Edit List** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Apply** button to apply your changes or **Cancel** to cancel your changes. Then click the **Close** button.
6. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
7. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
8. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. (You can block up to 20 services.)

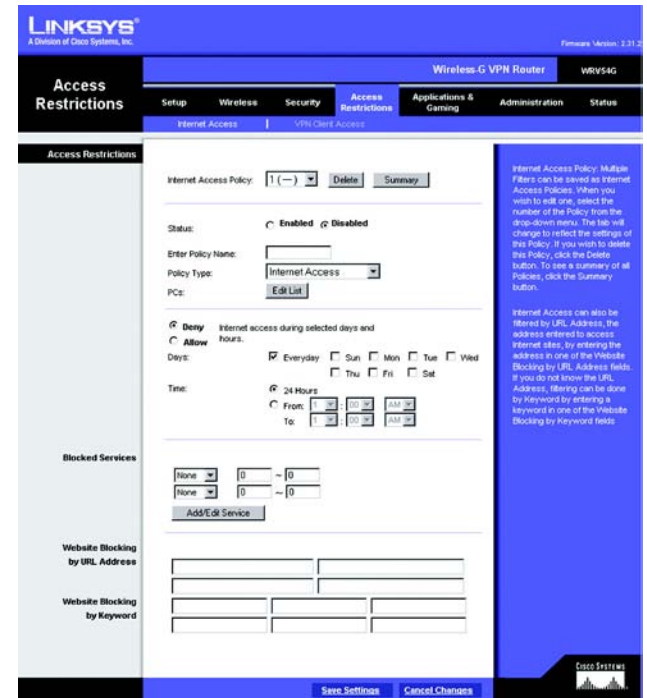


Figure 6-32: Access Restrictions Tab - Internet Access

http://192.168.0.2 - Filter Settings Summary - Microsoft Internet Explorer

No.	Name	Type	Days	Time of Day
1	default	Internet Access	S M T W T F S	24hrs.
2	---	---	S M T W T F S	---
3	---	---	S M T W T F S	---
4	---	---	S M T W T F S	---
5	---	---	S M T W T F S	---
6	---	---	S M T W T F S	---
7	---	---	S M T W T F S	---
8	---	---	S M T W T F S	---
9	---	---	S M T W T F S	---
10	---	---	S M T W T F S	---

Close

Figure 6-33: Internet Filter Summary

9. Then enter the range of ports you want to filter.

If the service you want to block is not listed or you want to edit a service's settings, then click the **Add/Edit Service** button. Then the *Port Services* screen will appear.

To add a service, enter the service's name in the *Service Name* field. Select its protocol from the *Protocol* drop-down menu, and enter its range in the *Port Range* fields. Then click the **Add** button.

To modify a service, select it from the list on the right. Change its name, protocol setting, or port range. Then click the **Modify** button.

To delete a service, select it from the list on the right. Then click the **Delete** button.

When you are finished making changes on the *Port Services* screen, click the **Apply** button to save changes. If you want to cancel your changes, click the **Cancel** button. To close the *Port Services* screen and return to the *Access Restrictions* screen, click the **Close** button.

10. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.
11. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.
12. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

To create an Inbound Traffic Policy:

1. Select **Inbound Traffic** as the Policy Type.
2. Select a number from the *Internet Access Policy* drop-down menu.
3. To enable this policy, click the radio button beside *Enable*.
4. Enter a Policy Name in the field provided.
5. Enter the source IP address whose traffic you want to manage. Select the appropriate protocol: **TCP**, **UDP**, or **Both**. Enter the appropriate port range, or select **Any**. Enter the destination IP address whose traffic you want to manage, or select **Any**.
6. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow network traffic.

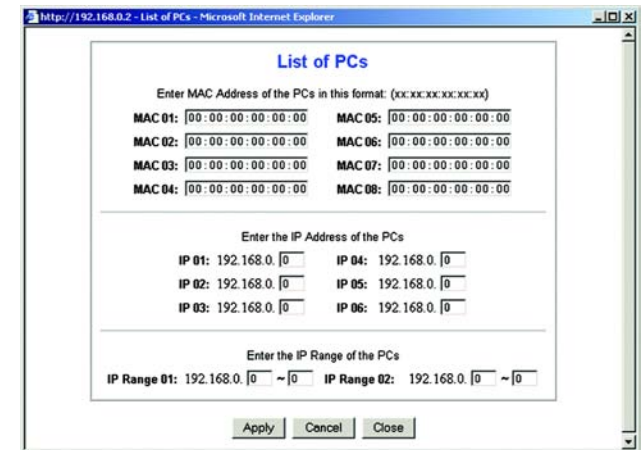


Figure 6-34: List of PCs

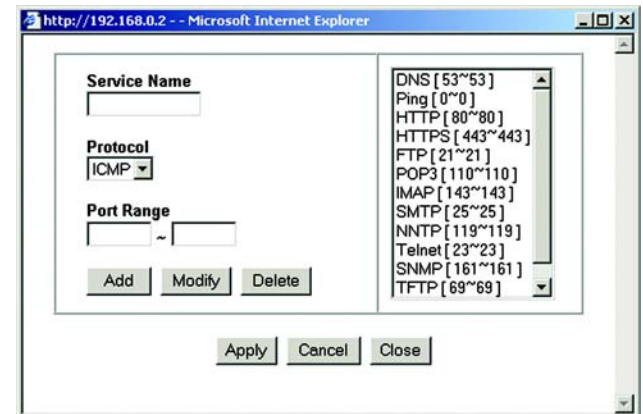


Figure 6-35: Blocked Services

7. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
8. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is shown on the right-hand side of a screen. For additional information, click **More**.

The Access Restrictions Tab - VPN Client Access

The Wireless-G VPN Broadband Router offers a free Linksys QuickVPN utility for Windows 2000 or XP. (For more information, refer to “Appendix D: Using the Linksys QuickVPN Software for Windows 2000 or XP.”) If the Router has VPN clients using this utility, then you can designate the VPN clients and their passwords on this screen.



NOTE: If you want VPN clients to use the Linksys QuickVPN utility, then the Router must have the *VPN Client Access* screen as part of its Web-based Utility. If you do not see this screen, then you must upgrade the Router's firmware. Refer to “Appendix H: Upgrading Firmware” for further instructions. (Before upgrading its firmware, write down the Router's settings. You will need to reset the Router to its factory defaults after you upgrade its firmware.)

VPN Client Status

User Name. Enter a name for the VPN client.

Password. Enter a password for the VPN client.

Re-enter to confirm. Enter the password again to confirm it.

Allow user to change password? If you want to let the user change his or her password, click the **Yes**.

When you have finished setting up a VPN client, click the **Add/Save** button to add the VPN client to your list and save the new settings.

VPN Client List Table

VPN Client Users. Select the appropriate group of users from the drop-down menu.

No. This is the number assigned to this VPN client.

Active. If you want to activate this VPN client, click the **Active** checkbox.

Username. The Username assigned to this VPN client will be displayed here.

Password. The Password assigned to this VPN client will be displayed here.

Edit/Remove. If you want to change the settings for a VPN client, click the **Edit** button and then make your changes. If you want to delete a VPN client from your list, click the **Remove** button.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

Figure 6-36: Access Restrictions Tab - VPN Client Access

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.)

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.

Port Range Forwarding

Application. In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Start/End. This is the port range. Enter the number that starts the port range under **Start** and the number that ends the range under **End**.

Protocol. Enter the protocol used for this application, either **TCP** or **UDP**, or **Both**.

IP Address. For each application, enter the IP Address of the PC running the specific application.

Enabled. Click the **Enabled** checkbox to enable port forwarding for the relevant application.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

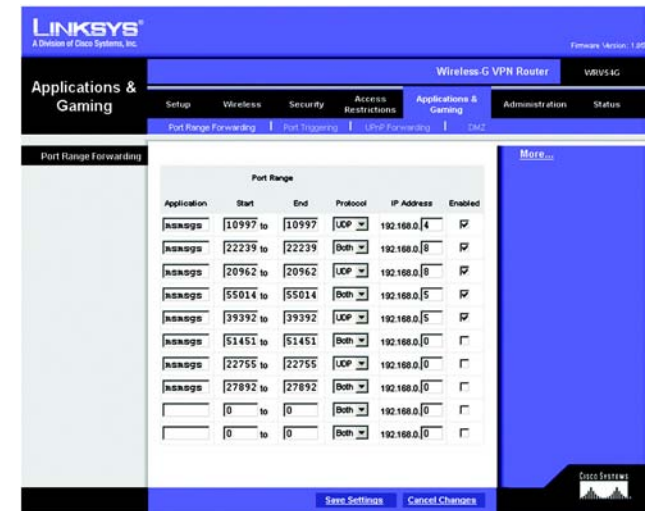


Figure 6-37: Applications & Gaming Tab - Port Range Forwarding

The Applications and Gaming Tab - 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. 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.

Port Triggering

Application. In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Triggered Range Start Port/End Port. Enter the number that starts the triggered port range under **Start Port** and the number that ends the range under **End Port**.

Forwarded Range Start Port/End Port. Enter the number that starts the forwarded port range under **Start Port** and the number that ends the range under **End Port**.

Protocol. Enter the protocol used for this application, either **TCP** or **UDP**, or **Both**.

Enabled. Click the **Enabled** checkbox to enable port triggering for the relevant application.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

Application	Triggered Range		Forwarded Range		Protocol	Enabled
	Start Port	End Port	Start Port	End Port		
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>
	0	0	0	0	Both	<input type="checkbox"/>

Figure 6-38: Applications & Gaming Tab - Port Triggering

The Applications and Gaming Tab - UPnP Forwarding

The *UPnP Forwarding* screen provides options for customization of port services for applications.

UPnP Forwarding

Application. In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

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

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

Protocol. Enter the protocol used for this application, either **TCP** or **UDP**, or **Both**.

IP Address. For each application, enter the IP Address of the server that you want the Internet users to be able to access.

Enabled. Click the **Enabled** checkbox to enable UPnP forwarding for the relevant application.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

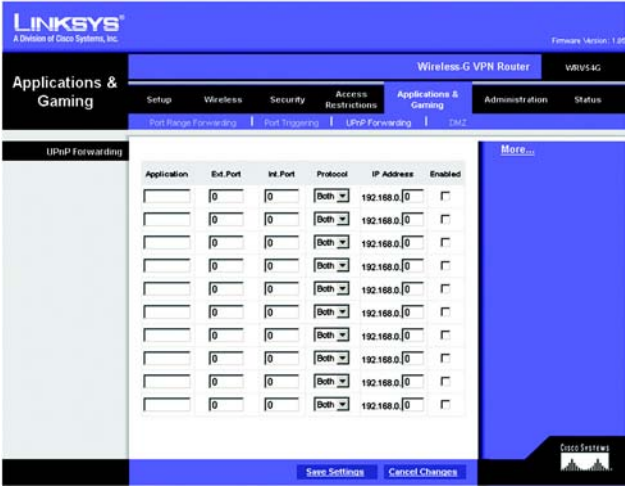


Figure 6-39: Applications & Gaming Tab - UPnP Forwarding

The Applications and Gaming Tab - DMZ

The *DMZ* screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing, 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.

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 the Software DMZ feature, 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 F: 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 the Hardware DMZ feature, select **Disabled**.

Hardware DMZ IP Address. Enter the IP Address of the local computer.

Hardware DMZ Netmask. Enter the Netmask (also known as Subnet Mask) of the local computer.

Destination IP Address. Enter the IP Address of the destination.

Subnet Mask. Enter the Subnet Mask of the destination.

Default Gateway. Enter the IP address of the Default Gateway.

metric. Enter the metric in the field provided.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

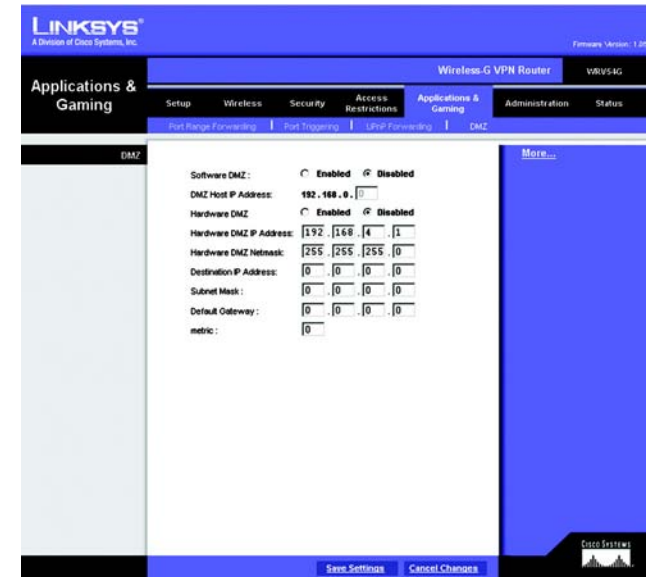


Figure 6-40: Applications & Gaming Tab - DMZ

The Administration Tab - Management

The *Management* screen allows you to change the Router's access settings as well as configure the SNMP and UPnP (Universal Plug and Play) features.

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 user name and password is **admin**.

User Name. It is recommended that you change the default user name to one of your choice.

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 the **Enabled** radio button.

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



Note: When you are in a remote location and wish to manage the Router, enter *http://<Internet IP Address>: port*. Enter the Router's specific Internet IP address in place of *<Internet IP Address>*, and enter the Administration Port number in place of the word *port*.

SNMP

SNMP, Simple Network Management Protocol, is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network.

To enable SNMP, check the **Enabled** box. To configure SNMP, complete all fields on this screen. To disable the SNMP agent, remove the checkmark.

The screenshot displays the 'Administration' tab in the Linksys web interface, specifically the 'Management' sub-tab. The interface is divided into several sections: 'Router Password' (Local Router Access), 'Remote Router Access', 'SNMP', and 'UPnP'. The 'Remote Router Access' section is currently active, showing options to enable or disable remote management and set a management port. The 'SNMP' section is also expanded, showing options to enable or disable SNMP and configure various parameters like contact, device name, location, and trap destination. The 'UPnP' section is also visible at the bottom.

Figure 6-41: Administration Tab - Management

Identification

Contact. Enter the name of the network administrator for the Router, as well as a contact number or e-mail address.

Device Name. Enter the name of the Router.

Location. Enter the location of the Router. For example, you could include the name of the building, floor number, and room location, such as Head Office - Floor 5 - Networking 3.

Get Community. Enter the password that allows read-only access to the Router's SNMP information. The default name is **public**.

Set Community. Enter the password that allows read/write access to the Router's SNMP information. The default name is **private**. A name must be entered in this field.

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 and Windows Me to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, check the **Enabled** box.

Allow Users 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 you have finished making changes on this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

The Administration Tab - Log

When you click the Administration tab, you will see the *Log* screen. The *Log* screen provides you with options for email alerts and a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Log

Email Alert

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

Email Address for General Logs. This is the e-mail address where you would like the general logs sent.

Email Address for Alert Logs. This is the e-mail address where you would like the alert logs sent.

Return E-Mail address. Your mail server may require a return email address. Enter that here. If you're unsure as to what address to enter, enter the same email address for *Email Address for Alert Logs*.

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

Syslog Notification

Syslog is a standard protocol used to capture information about network activity. The Router supports this protocol and can send its activity logs to an external server. To enable Syslog, click **Enabled**. Otherwise, select **Disabled**.

Device Name. Enter a name for the Router in the field provided.

Syslog Server IP Address. Enter the IP Address of the Syslog server in the *Syslog Server IP Address* field. In addition to the standard event log, the Router can send a detailed log to an external Syslog server. The Router's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP service, and number of bytes transferred.

Syslog Priority. Select the appropriate priority from the drop-down list. The default is *Information*.

Notification Queue Length

Log Queue Length. You can designate the length of the log that will be e-mailed to you. The default is **50** entries, so unless you change this setting, the Router will e-mail the log to you when there are more than 50 log entries.

Figure 6-42: Administration Tab - Log

Log Time Threshold. You can designate how often the log will be e-mailed to you. The default is **10** minutes, so unless you change this setting, the Router will e-mail the log to you every 10 minutes.

The Router will e-mail the log every time the Log Queue Length or Log Time Threshold is reached.

Alert Log

You can receive alert logs for specific types of Internet attacks and events: Syn Flooding, IP Spoofing, Win Nuke, Ping of Death, and Unauthorized Login Attempt. To be notified of a specific event, click its checkbox.

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 you have finished making changes on this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

The Administration Tab - Diagnostics

The ping test allows you to check the connections of your network components.

Ping Test

Ping Test Parameters

Ping Target IP. Enter the IP address of the network device whose connection you wish to test.

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

Ping Size. Enter the size of the ping packets.

Ping Interval. Enter the ping interval in milliseconds (how often you want the device to be pinged).

Ping Timeout. If there is no response the ping test will time out after a specified length of time. Enter the timeout period in milliseconds.

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

For help information, click **More**.

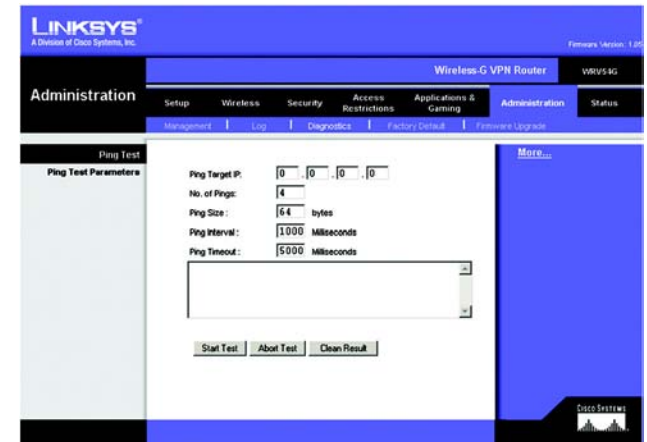


Figure 6-43: Administration Tab - Diagnostics

The Administration Tab - Factory Defaults

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

Factory Defaults

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



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

Click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For help information, click **More**.

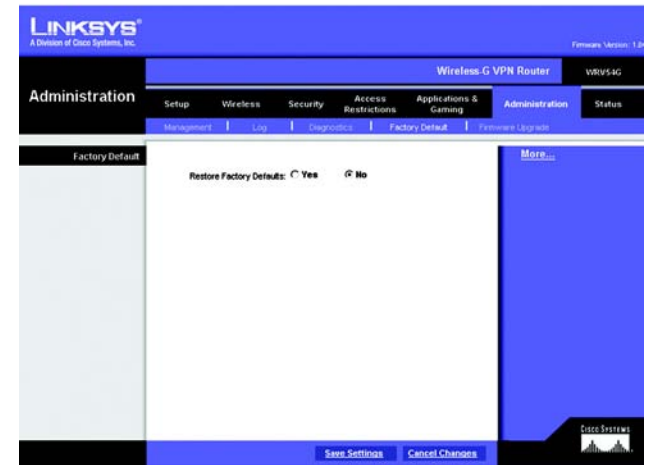


Figure 6-44: Administration Tab - Factory Default

The Administration Tab - Firmware Upgrade

The *Firmware Upgrade* screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.



Note: The Router will lose all of the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.

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

Upgrade Firmware

In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file. After you have selected the appropriate file, click the **Upgrade** button, and follow the on-screen instructions.

For help information, click **More**.

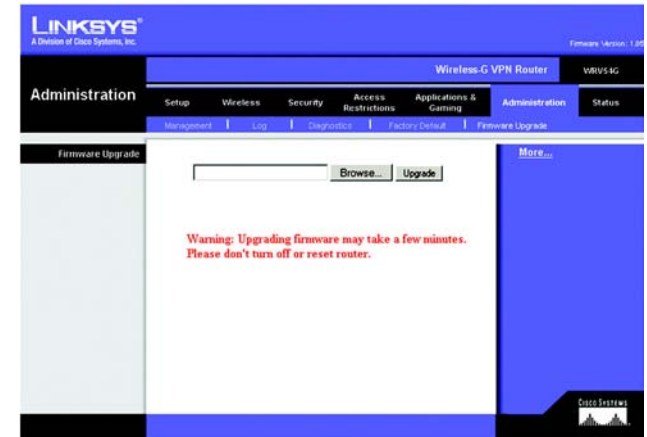


Figure 6-45: Administration Tab - Firmware Upgrade

firmware: the programming code that runs a networking device

download: to receive a file transmitted over a network

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

The Status Tab - Router

The *Router* screen displays information about the Router and its current settings. The on-screen information will vary depending on the Internet Connection Type selected on the *Setup* screen.

Information

Hardware Version. This shows the installed version and date of the hardware.

Software Version. This shows the installed version and date of the software.

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

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

System Up Time. The length of time the Router has been running is indicated here.

WAN Connections

Network Access. This indicates the type of Internet connection you are using.

Login Status. The status of the connection is displayed only for PPPoE or PPTP connections. For these dial-up style connections, there is a Connect button to click if there is no connection and you want to establish an Internet connection.

WAN IP Address. The Router's Internet IP Address is displayed here.

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

DNS. Shown here are the DNS (Domain Name System) IP addresses currently used by the Router.

DHCP Release. Available for a DHCP connection, click the **DHCP Release** button to release the current IP address of the device connected to the Router's Internet port.

DHCP Renew. Available for a DHCP connection, click the **DHCP Renew** button to replace the current IP address—of the device connected to the Router's Internet port—with a new IP address.

Click the **Refresh** button to update the on-screen information. For help information, click **More**.

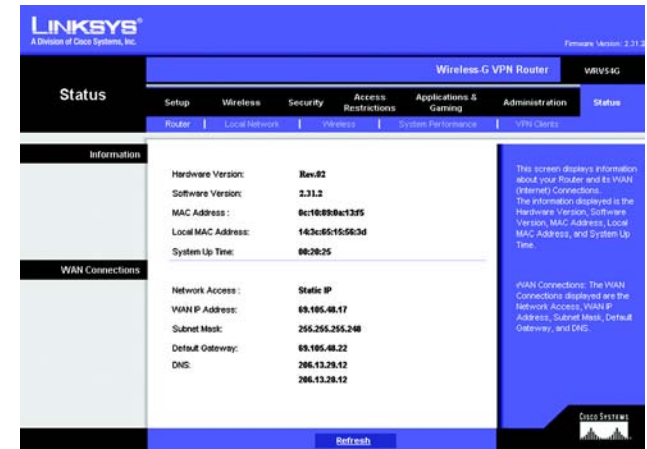


Figure 6-46: Status Tab - Router

The Status Tab - Local Network

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

Local Network

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

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

DHCP Server. The status of the DHCP server is displayed here.

DHCP Client Lease Info. Click the **DHCP Clients Table** button to view a list of PCs that have been assigned IP addresses by the Router. The *DHCP Active IP Table* screen lists the DHCP Server IP Address, Computer Names, IP Addresses, MAC Addresses, and length of time until a computer's assigned IP address expires. Click the **Close** button to return to the *Local Network* screen. Click the **Refresh** button to update the information.

Click the **Refresh** button to update the on-screen information. For help information, click **More**.



Figure 6-47: Status Tab - Local Network

The screenshot shows the 'DHCP Active IP Table' screen. At the top, it says 'DHCP Server IP Address: 192.168.0.2'. Below this is a table with the following columns: Computer Name, IP Address, MAC Address, and Expires. The table contains 15 rows of data. At the bottom right, there are 'Refresh' and 'Close' buttons.

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:d0:a6	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:99:0a	Expire
new-host-7	192.168.0.3	00:40:d0:2b:1a:ec	21:36:02
xwv	192.168.0.4	00:0c:41:4a:7f:06	21:07:29
qtkkcf	192.168.0.5	00:04:5a:86:d7: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:d7	Expire

Figure 6-48: DHCP Active IP Table

The Status Tab - Wireless

The *Wireless* screen displays status information about your wireless network.

Wireless

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

Mode. As selected from the Wireless tab, this will display the wireless mode (Mixed, G-Only, or Disabled) used by the network.

SSID. As entered on the Wireless tab, this will display the wireless network name or SSID.

Channel. As entered on the Wireless tab, this will display the channel on which your wireless network is broadcasting.

Encryption Function. As selected on the Wireless Security tab, this will display what type of encryption the Router uses for security.

Click the **Refresh** button to update the on-screen information. For help information, click **More**.



Figure 6-49: Status Tab - Wireless

The Status Tab - System Performance

The *System Performance* screen displays status information about network traffic for the Internet, wireless activities, and wired connectivity.

System Performance

Internet/Wireless

Statistics for the network traffic on the Internet connection and wireless connectivity are shown in two separate columns.

IP Address. The IP address of the Router's interface is displayed here.

MAC Address. The MAC address of the Router's interface is shown here.

Connection. The status of the connection is shown here.

Packets Received. The number of packets received is displayed here.

Packets Sent. The number of packets sent is displayed here.

Bytes Received. The number of bytes received is shown here.

Bytes Sent. The number of bytes sent is shown here.

Error Packets Received. The number of error packets received is displayed here.

Dropped Packets Received. The number of dropped packets received is displayed here.

LAN

Statistics for the network traffic on each of the four LAN ports are shown in four separate columns.

IP Address. The IP address of the Router's interface is displayed here.

MAC Address. The MAC address of the Router's interface is shown here.

Connection. The status of the connection is shown here.

Packets Received. The number of packets received is displayed here.

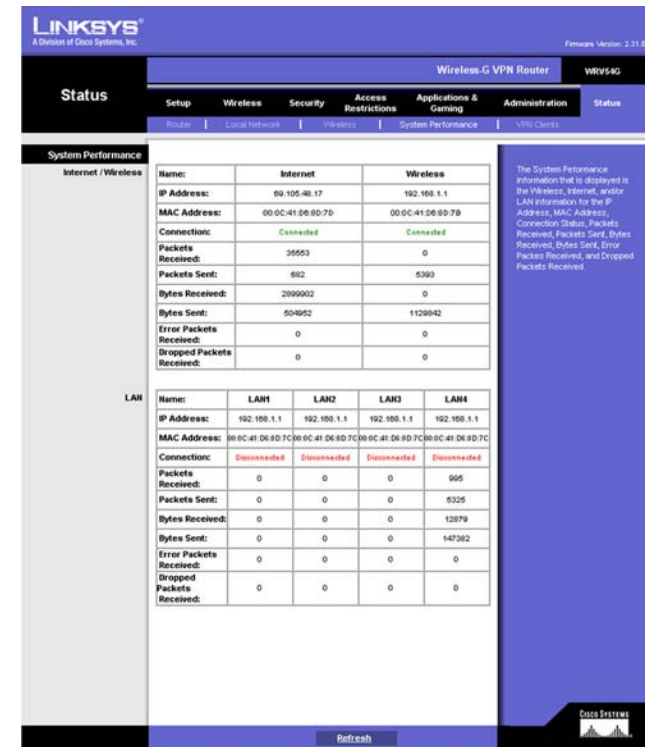


Figure 6-50: Status Tab - System Performance

Packets Sent. The number of packets sent is displayed here.

Bytes Received. The number of bytes received is shown here.

Bytes Sent. The number of bytes sent is shown here.

Error Packets Received. The number of error packets received is displayed here.

Dropped Packets Received. The number of dropped packets received is displayed here.

Click the **Refresh** button to update the on-screen information. Help information is shown on the right-hand side of the screen.

The Status Tab - VPN Clients

The *VPN Client Status* screen displays status information about the Router's VPN clients.

VPN Client Status

VPN Client Users Display. Select the group of VPN client users whose information you wish to see.

No. This is the number assigned to the VPN client.

Username. The Username assigned to the VPN client will be displayed here.

Status. This is the status of the VPN connection.

Start Time. The time the VPN connection began is displayed here.

End Time. The time the VPN connection ended is shown here.

Duration. This is the length of time the VPN connection has lasted.

Disconnect. If you want to disconnect a VPN client, click this checkbox.

Click the **Refresh** button to update the on-screen information. Click the **Disconnect** button to disconnect the VPN clients whose *Disconnect* checkboxes have been checked. For help information, click the **More** button.

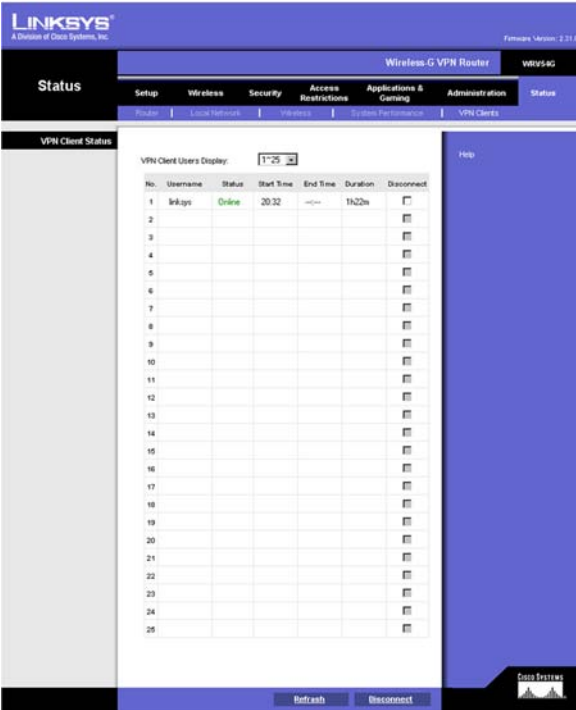


Figure 6-51: Status Tab - VPN Clients

Chapter 7: Boingo™ Hot Spot in a Box® Program for Hot Spot Businesses

Program Overview

Boingo Hot Spot in a Box is a program for businesses that want to offer wireless networking services for their customers. Enabling the Boingo Hot Spot in a Box feature will turn the Linksys Wireless-G VPN Broadband Router into a commercial hot spot. The service is powered by Boingo Wireless, the leading Wi-Fi service provider, and has been designed for small business that need a single hot spot installation.

Wi-Fi is the fastest growing segment of the Internet industry and there are already millions of people carrying Wi-Fi enabled notebooks and PDAs. Now you can harness Wi-Fi to make money and provide a valuable service to your customers. Wi-Fi service will grow to hundreds of millions of dollars over the next few years. Notebook manufacturers are already building Wi-Fi capability into their machines, rapidly making Wi-Fi a standard computer component similar to the way the 56k modem is standard today.



IMPORTANT: Make sure to check with your Internet Service Provider's terms of service agreement to see if they allow hot spots on your plan before you continue.

Simple Hot Spot in a Box Program

The Boingo Hot Spot in a Box simplifies your process to become part of this exciting technology movement. Here is the program:

1. Enable the Boingo Hot Spot in a Box feature during the setup of the Linksys Wireless-G Broadband Router.
2. Register as a Boingo Hot Spot in a Box owner and configure your Hot Spot in a Box using Boingo's online setup wizard. Your location will be listed in the Boingo directory, which is available on our website and in the Boingo client software, which will reside on the notebooks and handhelds of millions of mobile users.
3. Market the program with the Hot Spot in a Box marketing kit that Boingo will send you. This kit includes everything you need to sell access in your location, including 300 brochures explaining the service and technology, 20 table tents promoting the service, as well as 10 Boingo stickers and CDs to sign up additional customers. Boingo will also send you a presentation describing the most effective ways to promote your location, and Boingo will advise you along the way.
4. Collect a check that Boingo will send you every month for aggregate customer connections and customers you sign up to the service.

- Boingo will pay you \$1.00 every day that a Boingo monthly subscriber or roaming system user connects to one of your locations and \$4.00 every day that someone connects using a Boingo AsYouGo day connection.
- Boingo will pay you \$20 every time you sign up a new Boingo monthly subscriber who remains a member for 60 days.

Boingo will track your sign-ups with a sales channel code that is assigned to the Router when you register with Boingo, and Boingo will send you a usage statement and commission check every month. You can track your usage and account sign-ups through Boingo's convenient Hot Spot in a Box Administration website.

How the Boingo Hot Spot in a Box Feature Impacts the Linksys Wireless-G Broadband Router

The Linksys Wireless-G VPN Broadband Router is a highly advanced networking solution that combines a Wi-Fi access point, a built-in 4-port, full-duplex 10/100 switch to connect your wired Ethernet devices, and a router that ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

If you enable the Hot Spot in a Box feature, the Router can only be used wirelessly as a public commercial hot spot device, and you will no longer have access to your private network wirelessly—you will only have wired access. For security reasons, the wired and wireless sides of your device are kept separate when the Hot Spot in a Box feature is enabled. You can provide a public hot spot while simultaneously maintaining security and privacy on your private wired network, and both share the same Internet connection.

To maintain wireless access to your private network, you can simply add a wireless access point, like the Linksys WAP54G, to one of the wired Ethernet LAN ports.

You will still be able to use the wireless interface of the Router to access the Internet when Hot Spot in a Box is enabled. During the Hot Spot in a Box registration process, you can enter the MAC addresses (unique serial numbers) of your wireless adapters or cards so that you can access the Internet without a Boingo subscription or day account. Of course, you can also still access the Internet and your local network through any one of the four LAN ports on the Router.

Once the Router has been registered with Boingo as a Hot Spot in a Box, you can easily unregister the device and restore the factory default settings by going back to the “Hot Spot” tab on the web-based utility interface and checking the **Disable** box. If you decide to re-register your device, you can do so by repeating the Boingo registration process.

Excellent Customer Support

Toll-free technical support is available from Boingo's staff of Wi-Fi experts. For questions or problems related to the Boingo Hot Spot in a Box program, the Boingo Wi-Fi service, or your sales/usage commissions, please contact Boingo Wireless Customer Support at:

Phone: 1-800-380-4082 Monday through Friday 4:00 am to 10:00 pm (Pacific Standard Time)
Saturday and Sunday 6:00 am to 3:00 pm (Pacific Standard Time)

Address: Boingo Wireless
1601 Cloverfield Boulevard
Suite 570 South
Santa Monica, CA 90404

Web: www.boingo.com or www.boingo.com/servicecenter.html

E-mail: service@boingo.com

Getting Started

Setting up your first Hot Spot in a Box device is a fast and simple process. To begin, make sure you have the following:

- Boingo Hot Spot in a Box device
- DSL, cable, or T1 connectivity
- A notebook or desktop computer with a wireless 802.11b or 802.11g adapter (such as a PCMCIA card) or built-in 802.11b or 802.11g capabilities



IMPORTANT: Make sure to check with your Internet Service Provider's terms of service agreement to see if they allow hot spots on your plan before you continue.

Step 1: Setup of Your First Hot Spot in a Box Device

Set up the Wireless-G VPN Broadband Router using the Setup Wizard on the Setup CD-ROM. Boingo recommends that you use a wired connection to configure the Router for Hot Spot in a Box. Then, click the **Register** button on the Hot Spot tab of the Setup tab in the Router's Web-based Utility (refer to "Chapter 6: Configuring the Wireless-G VPN Broadband Router").

Step 2: Registration Process

1. The *Registration Login* screen will appear. In the *First Hot Spot in a Box Registration Process* section, click the **Register as a Hot Spot in a Box Owner** button to register for the first time, and then go to the next step on this page (step 2).

If you already have a Hot Spot in a Box account and want to add another Router, enter your user name and password in the *Already have a Hot Spot in a Box® Account* section. Click the **Login** button, and then skip ahead to Step 3: Device Configuration Wizard. (The Boingo system will detect that a device is set up and will go directly to the Device Configuration Wizard.)



Figure 7-1: Registration Login

2. When the *Welcome* screen appears, read the general information, and then click the **Register your Hot Spot in a Box now!** button at the bottom of the screen.

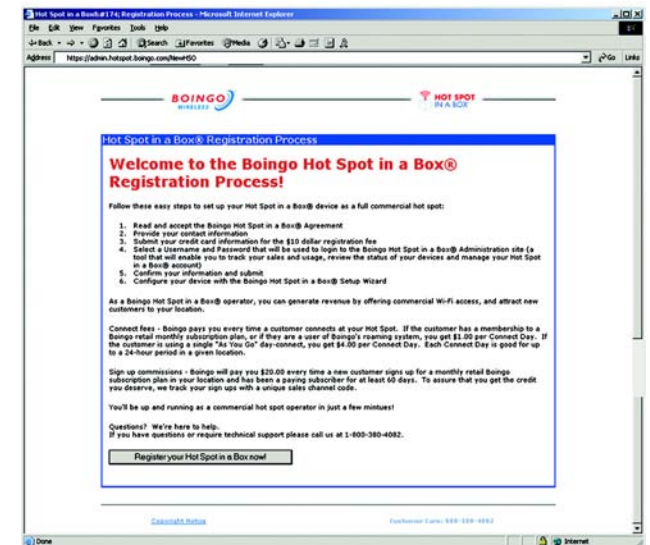


Figure 7-2: Welcome

3. The *Hot Spot Operator Agreement* will appear. Read the terms of the agreement, and then if you agree with the terms, click the **I Agree** button.

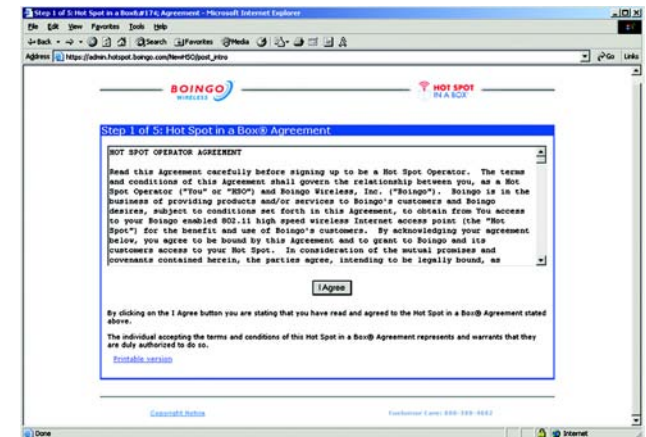


Figure 7-3: Operator Agreement

4. The *Business Contact Information* screen will appear. Enter the contact information for the person who will receive commission checks and correspondence from Boingo. Enter the Contact Name, Company Name, Tax ID/Social Security Number, Address, City, State, Zip Code, Country, Telephone Number, Fax Number, and Email address information. Then select the appropriate Time Zone. When finished, click the **Continue** button.

Figure 7-4: Business Contact Information

5. The *Credit Card Information* screen will appear. Enter the Name, Address, City, State, and Zip Code.

Then select the appropriate Card Type. Enter the Card Number, and select the Expiration Date. When finished, click the **Continue** button.

You will be charged a one-time fee of \$10.00 for marketing materials. (If you add more devices to your account, you will not be charged a fee for marketing materials.)

Step 3 of 5: Enter Credit Card Information

There is a \$10.00 registration fee for your first Hot Spot in a Boingo device. You will not be charged additional fees if you register other Hot Spots in a Boingo device. The address information must match what appears on your credit card statement. Fields marked with an asterisk (*) are required.

Name: William Wireless

Address 1: 123 Main Street

Address 2:

City: Anywhere

State/Provinces: California

Zip/Postal Code: 90204

Card Type: Visa

Card Number: 44443332221111

Expiration Date: Month: 6 Year: 2008

Continue

Figure 7-5: Credit Card Information

6. Select a user name and password to use when you access your account. The user name can include numbers, lowercase letters, and periods. It must begin with a lowercase letter, and it must have at least four characters but not more than sixteen characters. Your password must contain at least six characters.

Enter a user name and password in the fields provided. Enter the password again in the *Repeat Password* field. When finished, click the **Continue** button.

Step 4 of 5: Select a Username and Password

Your username can include numbers, lowercase letters and periods ("."). The username must begin with a lowercase letter, and must be between 4 and 16 characters in length. Your password must contain at least 6 characters. All fields are required.

Username: wireless

Password: 123456

Repeat Password: 123456

Continue

Figure 7-6: Select a Username and Password

7. The *Confirmation* screen will appear. Review your Business Contact Information and Credit Card Information. If you want to make any changes, click the **Edit** button under the section that you want to edit. When finished, click the **Continue** button.

Figure 7-7: Confirmation

8. The *Registration Complete* screen will appear when you have finished the registration process. Click the **Setup New Device** button to continue with the setup and begin the Device Configuration Wizard.

Figure 7-8: Registration Complete

Step 3: Device Configuration Wizard

1. The *Device Setup Location* screen will appear. Enter the Location Name. Then describe where the device is placed at the location. Select the Location Type. Enter the Phone number, Address, City, State, Postal Zip Code, and Country in the fields provided. When finished, click the **Continue** button.
2. When the *Onsite Contact Information* screen appears, enter the contact information for the person who is to be contacted if the network monitoring system detects a problem with the device. This person is a contact person only and does not need technical skills. Enter the Name, Phone number, Fax number, and Email address in the fields provided. When finished, click the **Continue** button.

Device Setup (Step 1 of 6): Location

Please enter the location information for this device. If the device is moved, please be sure to update this device profile. All fields required.

Location Name	The Coffee Shop
Describe Placement of Device Within the Location	Under the counter
Location Type	Cafe/Restaurant
Phone	310-123-4567
Address	123 Main Street
City	Santa Monica
State/Province	CA
Postal Code	90024
Country	United States

Continue

Figure 7-9: Device Location

Device Setup (Step 2 of 6): Onsite Contact Information

Please enter the contact information for the person responsible for this device at the location. Boingo may contact this person if we detect problems with your device through our network monitoring system. If the onsite contact person changes over time, please be sure to update this device profile. Name, Phone, and Email are required fields.

Name	William Wireless
Phone	310-123-4567
FAX	310-123-4568
Email	wireless@coffeeshop

Continue

Figure 7-10: Onsite Contact

3. The *Device Configuration* screen will appear. Most Hot Spot operators will not need to change the default settings. To view or edit the settings, click **View Settings**. When finished, click the **Continue** button.

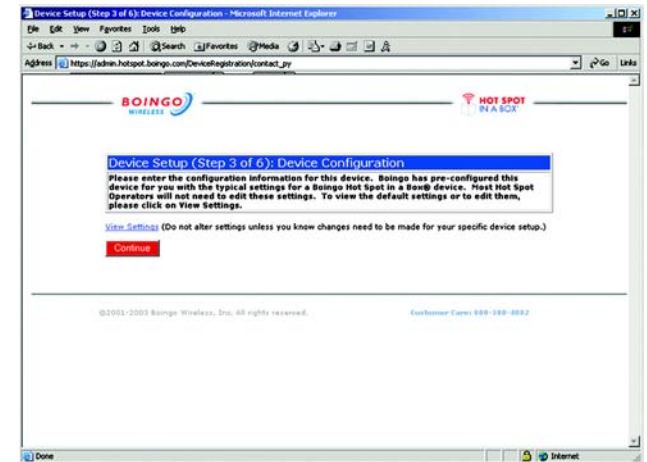


Figure 7-11: Device Configuration

4. If you click the **View Settings** button, the *View/Edit Settings* screen will appear. The Wireless Settings, Network Settings, and DNS Settings are listed. Do not change the settings unless you are sure that they need to change.

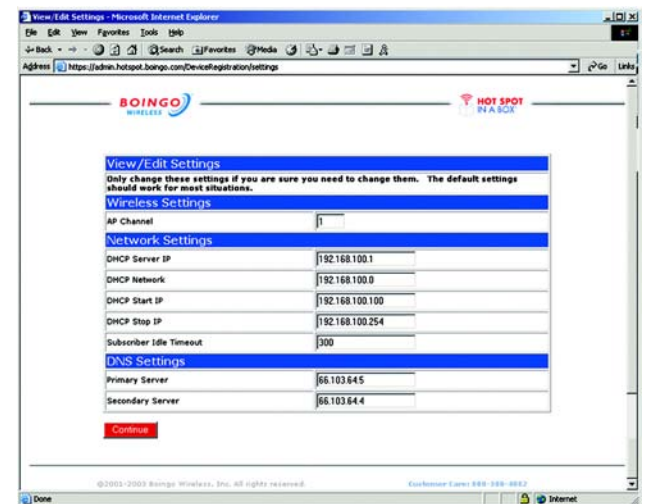


Figure 7-12: View/Edit Settings

5. The *Your Location Page* screen will appear. Enter the information that your customers will see on the webpage that they will use to log on to the Internet. You can customize the page by adding the name of your Hot Spot, a message or description (255 character limit), and your company logo.

Enter the name of your Hot Spot in the *Hot Spot Name* field. In the *Hot Spot Description* field, enter the message you want your customers to see.

To add a logo, save a copy of the logo (GIF or JPEG format only) to the computer, and then click the **New** button. Enter a name or description of the image in the *Description* field. Enter the file name in the field provided, or click the **Browse** button to locate the file. After the file is located, click the **Upload Image** button to add it to the web page.

Click the **Preview** button to view the web page that includes the information you have added. (A sample webpage is shown on the right.)

When finished, click the **Continue** button to continue with the setup.

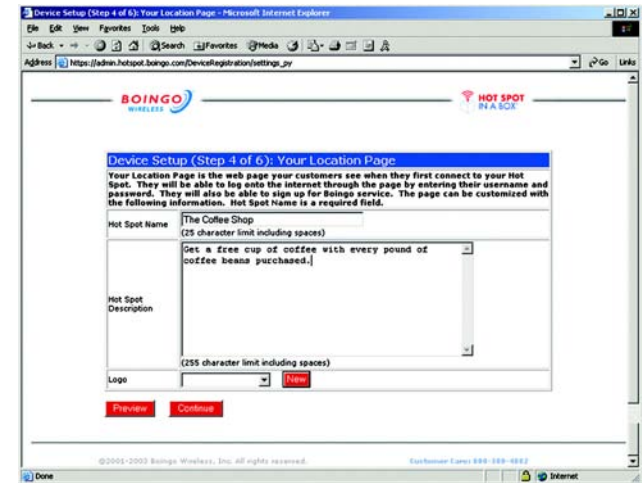


Figure 7-13: Your Location Page

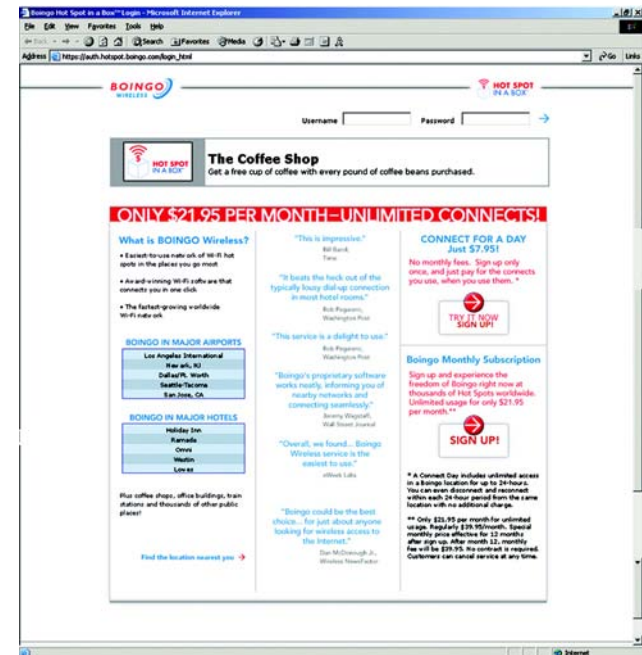


Figure 7-14: Sample Page

6. The *Free Access for Friends and Family* screen will appear. Use this feature to set up free Internet access accounts through the Hot Spot in a Box device for your family, friends, and employees. You will need the MAC Address of the wireless adapter or card for each computer that will be used. The MAC Address is usually located on the adapter's label or the bottom of the notebook computer. For each user, enter the MAC Address in the *MAC ID for User #* field.

When finished, click the **Continue** button.

Device Setup (Step 5 of 6): Free Access for Friends and Family

You can set up free accounts for your family, friends and employees to access the Internet through your Hot Spot in a Boingo device without a Boingo account by adding the MAC ID of each person's WiFi card to the list below. The MAC ID of a card can usually be found on the Wi-Fi card's label. If you have a laptop with a built in WiFi card, the MAC ID can be found on the bottom of your laptop or in the documentation that came with the machine. If you have trouble locating the MAC ID for a device, please contact the device manufacturer or call Boingo at 1-800-380-4082.

MAC ID for User # 1	67-8B-34-65-95-63
MAC ID for User # 2	00-54-93-2B-76-12
MAC ID for User # 3	
MAC ID for User # 4	
MAC ID for User # 5	
MAC ID for User # 6	
MAC ID for User # 7	
MAC ID for User # 8	
MAC ID for User # 9	
MAC ID for User # 10	

Continue

©2003-2009 Boingo Wireless, Inc. All rights reserved. Customer Support: 800-380-4082

Figure 7-15: Free Access

7. The *Confirmation* screen will appear. You may review and edit all of your settings for Location, Onsite Contact, Wireless Settings, Network Settings, DNS Settings, Location Page, and Free Access for Friends and Family.

In the Location Page section, you can add a logo if you didn't previously. To add a logo, save a copy of the logo (GIF or JPEG format only) to the computer, and then click the **New** button. Enter a name or description of the image in the *Description* field. Enter the file name in the field provided or click the **Browse** button to locate the file. After the file is located, click the **Upload Image** button to add it to the webpage.

Click the **Preview** button to view the web page that includes the information you have added.

When finished, click the **Continue** button.

Device Setup (Step 6 of 6): Confirmation
Please review your device settings. If they are all correct, click on the Continue button.

Location

Location Name	William Wireless
Describe Placement of Device Within the Location	Under the front counter
Location Type	Cafe/Restaurant
Phone	310-123-4567
Address	123 Main Street
City	Santa Monica
State/Province	CA
Postal Code	90404
Country	United States

Onsite Contact

Name	William Wireless
Phone	310-123-4567
FAX	310-123-4568
Email	jwireless@coffeeshop

Wireless Settings

AP Channel	1
------------	---

Network Settings

DHCP Server IP	192.168.100.1
DHCP Network	192.168.100.0
DHCP Start IP	192.168.100.100
DHCP Stop IP	192.168.100.254
Subscriber Idle Timeout	300

DNS Settings

Primary Server	66.103.64.5
Secondary Server	66.103.64.4

Location Page

Hot Spot Name	The Coffee Shop (25 character limit including spaces)
Hot Spot Description	Get a free cup of coffee with every pound of coffee beans purchased. (255 character limit including spaces)
Logo	[Browse] [New]

Free Access for Friends and Family

MAC ID for User # 1	67-99-3445-95-63
MAC ID for User # 2	00-54-93-29-76-12
MAC ID for User # 3	
MAC ID for User # 4	
MAC ID for User # 5	
MAC ID for User # 6	
MAC ID for User # 7	
MAC ID for User # 8	
MAC ID for User # 9	
MAC ID for User # 10	

Buttons: [Preview] [Continue]

©2003-2005 Boingo Wireless, Inc. All rights reserved. Customer Care: 888-888-8882

Figure 7-16: Confirmation

8. The *Almost Done* screen will appear. Read the information, and then click the **Complete Device Setup** button to save all of your settings.

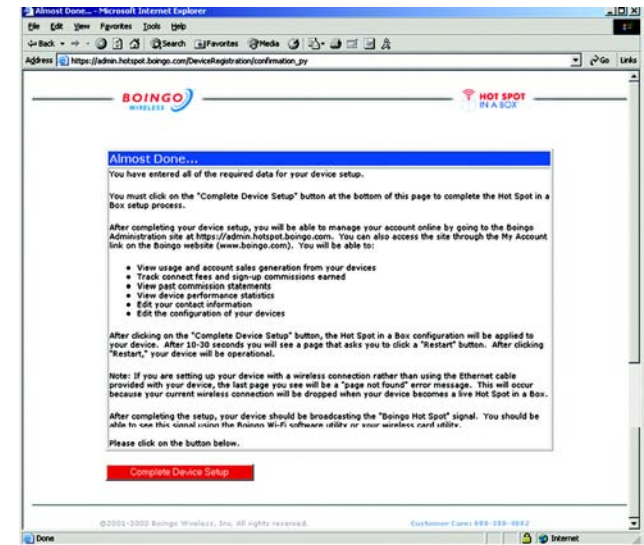


Figure 7-17: Almost Done

Step 4: Return to the Device

After the Hot Spot tab reappears, click the **Refresh** button. A screen will appear to notify you that you are online.

Complete the configuration of the Router. When finished, the setup of your first Hot Spot in a Box device is complete, and now it is an active Hot Spot location in the Boingo system.

You can manage your device (check usage, change settings, update contact information, review device statistics, etc.) by going to the Boingo Administration site at <http://admin.hotspot.boingo.com> or www.boingo.com/selfcare. Refer to the following section, "Administration Site."

Administration Site

The Boingo Hot Spot in a Box Administration site provides you with the tools you need to manage your device. The site allows you to do the following:

- Change your billing contact person
- Access online Help files
- View current and historical usage
- View revenue generated from usage and commissions
- Access your past Boingo commission statements
- View statistical and performance data on your devices
- Change/update the configuration of your devices

You can access this site in one of two ways:

Go directly to **<http://admin.hotspot.boingo.com>**.

Go to **www.boingo.com** and click the **My Account** button.

The site offers three primary screens:

- Login. This is the website's entry screen.
- Home. This is the initial screen you see after you log in. It provides general information and data on all of your live devices as a group.
- Device. This displays the system information for the device.

Login

To access the Administration site, enter your user name and password in the fields provided. Then, click the **Login** button.

Home

This is the view displayed when you log in to the Boingo Administration Site. It is also the screen you will see whenever you click on **Home** in the left column. The *Home* screen consists of three primary areas:

- **Main Window (white area)**

This screen displays a list of the Hot Spot in a Box devices that you have installed. The description includes a ball-shaped icon indicating the device's status, device's unique identification, company name, location name, description of the device's placement, city, and state. Clicking on one of the devices listed will display the *Device* screen.

The color of the status ball indicates the following:

Green. Green indicates that your device is online and connected to the Internet.

Red. Red indicates that your device is offline and is not connected to the Internet or is not configured correctly.

Gray. Gray indicates that your device is not registered. Make sure that you are connected to the Internet and register your device again.



NOTE: If any other color of status ball appears, contact Boingo Technical Support.

- **Navigation Column on the Left**

This is a list of available links. These links include the following:

- **Home.** This displays the *Home* screen.
- **Customer Support.** It provides Customer Support contact information in the main window.
- **Change Billing Contact.** This allows you to change the contact information of the person who receives the commission checks.



Figure 7-18: Administration Login

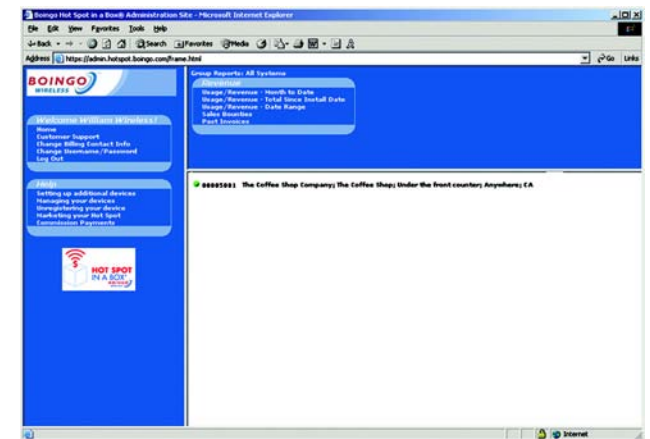


Figure 7-19: Home

- Log out. Use this screen to log you out of the Boingo Administration Site.
- Help. This screen provides additional information.
- Navigation Bar at the Top

The links in the top navigation bar vary depending on the view selected. These links may include the following:

- Usage/Revenue – Month to date. This shows usage revenue from the beginning of the month to the current day. The chart will show the number of connections from Boingo Subscription users and from As-You-Go users. It will also show the total revenue from each group and the total revenue for the time period.
- Usage/Revenue – Total Since Install Date. This screen shows the same information as above but the time period will range from the initial device installation date to the current date.
- Usage/Revenue – Date Range. It shows the same information as above but the time period will be based on a range of dates set by the user.
- Sales Commissions. This shows the total number of Boingo subscription sign-ups that have come through your device.
- Past Statements. See electronic versions of the monthly commission statements that Boingo will send to you each month.

Device

This is the view that you see when you click on a device. The Device view screen consists of three primary areas:

- Main Window (white area)

When you select a specific device, the main window will display general information about the device. At this point, all links in the top navigation bar will apply to this specific device.

- Navigation Column on the Left

The navigation column will not change.

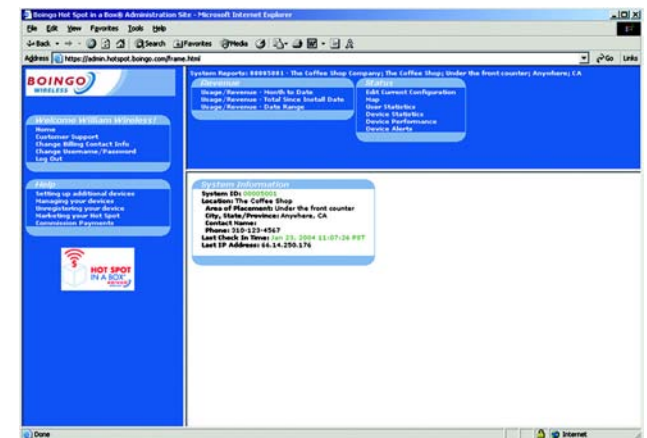


Figure 7-20: Device View

- Navigation Bar at the Top

The links in the top navigation bar will change. All of these links are now specific to the device that you selected. The “Sales Commissions” and “Past Statements” links will disappear (these reports are not device-specific). In addition, a new list of reports called “Status” will appear.

Usage Reports

- Usage/Revenue – Month to date. This shows usage revenue from the beginning of the month to the current day. The chart will show the number of connections from Boingo Subscription users and from As-You-Go users. It will also show the total revenue from each group and the total revenue for the time period.
- Usage/Revenue – Total Since Install Date. This screen shows the same information as above but the time period will range from the initial device installation date to the current date.
- Usage/Revenue – Date Range. It shows the same information as above but the time period will be based on a range of dates set by the user.

Status Reports

A variety of device status reports are offered. Details on each of these reports are provided below.

- Edit Current Configuration. This shows all of your device configuration fields and allows you to edit them.
- Map. It shows your Hot Spot location on a regional map.

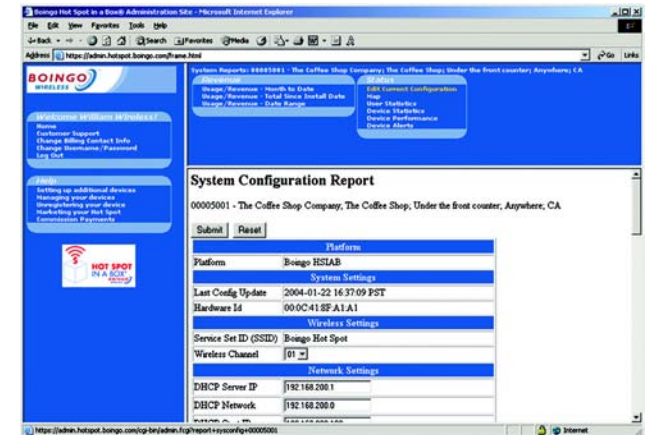


Figure 7-21: Edit Current Configuration

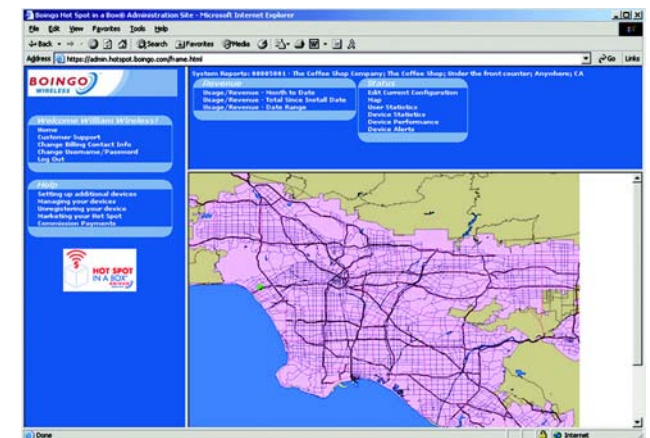


Figure 7-22: Map

- **User Statistics Report.** This shows the statistics of the subscribers that are currently accessing the Internet through the Router.

Post Time. This is the time when the user first accessed the Internet through the Router.

Idle Time. This is the length of time that the user has been idle (the session is considered inactive).

User Name. The user name of the subscriber is displayed here.

User IP. The IP address assigned to the user is shown here.

User MAC Address. This is the MAC address of the Wi-Fi adapter or card being used by the subscriber.

State. This indicates one of two states: pending (user has associated to the Router, but has not authenticated), or open (user is logged in).

Bytes In. Number of megabytes (MB) received.

Bytes Out. Number of megabytes (MB) sent.

- **Device Statistics.** This shows the device network information (identical to route command on UNIX systems).

Routing

The route information for this device is shown here.

Destination. The IP address destination network or host is displayed.

Gateway. The gateway address is shown.

Mask. This is the Netmask (or Subnet Mask) for the network.

Flags. The status of the route is indicated here.

Ref. Count. This is the number of references to this route.

Use Count. The number of lookups for the route is displayed here.

Interface. This is the number of the network interface.

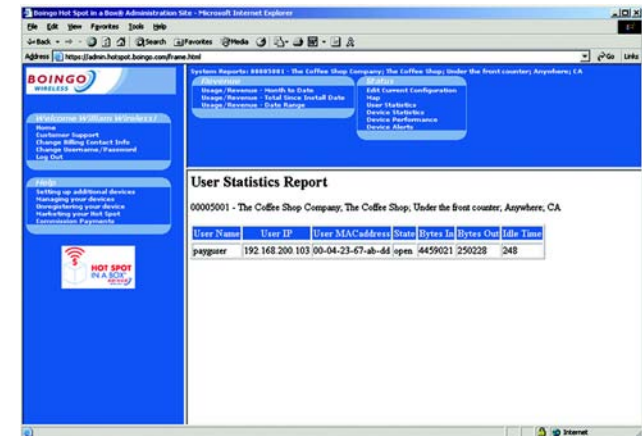


Figure 7-23: User Statistics

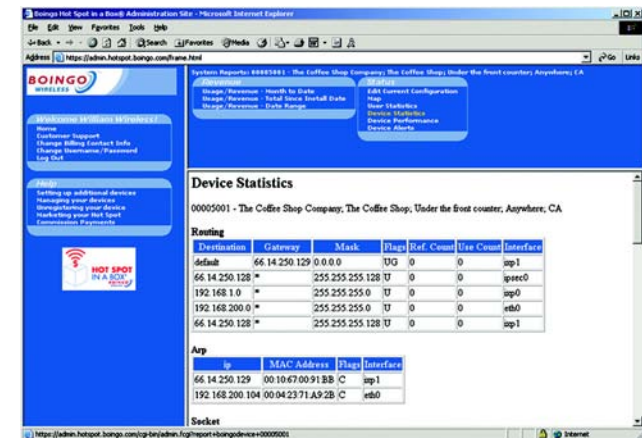


Figure 7-24: Device Statistics

Arp

This shows who is associated to a network interface; e.g., a client who associates with the access point but doesn't get an IP address.

IP. This is the IP address of the device on the network.

Mac Address. This the MAC address of the device on the network.

Flags. The type of ARP entry is shown here.

Interface. The network interface is shown here.

Socket

This shows the network connections (incoming and outgoing traffic requests).

Proto. The protocol (TCP or UDP) is displayed here.

Receiving Queue. This is the number of bytes received by the user program connected to this socket.

Send Queue. This is the number of bytes received by the user program connected to this socket.

Local Address. This is the IP address of the local end of the socket.

Local Port. This is the port number of the local end of the socket.

Foreign Address. This is the IP address of the remote end of the socket.

Foreign Port. This is the port number of the remote end of the socket.

State. Shown here is the state of the socket, e.g., OPEN, CLOSED, or TIME WAIT.

- **Device Performance**

This shows the historical view of device uptime, load, and RAM, CPU, or network usage.

Post Time. This is the time the update was made by the device.

Uptime. This is the total amount of uptime, represented in DD:HH:MM:SS (days, hours, minutes, seconds).

Load. This is the system load average, represented in typical UNIX format displaying averages for the past 1, 5, and 15 minutes.

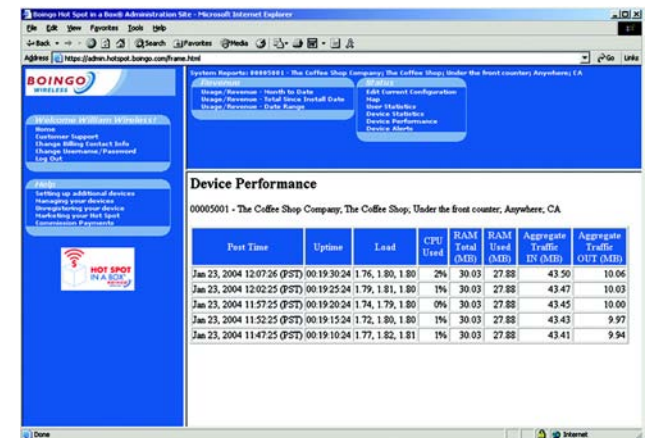


Figure 7-25: Device Performance

CPU Used. This is the percentage of the CPU's processing power currently in use.

RAM Total (MB). This is the total RAM available, represented in megabytes (MB).

RAM Used (MB). Shown here is the amount of RAM currently in use, represented in megabytes (MB).

Aggregate Traffic IN (MB). This is the total amount of incoming traffic for all users of the wired interface, represented in megabytes (MB).

Aggregate Traffic OUT (MB). This is the total amount of outgoing traffic for all users of the wired interface, represented in megabytes (MB).

- **Device Alerts**

This is a log of events, including system startup, shutdown, DHCP activities, and AAA (Administration, Authorization, and Authentication) activities.

System startup. This is a notification indicating when the device was started.

System shutdown. This is a notification indicating when the device was shut down or restarted.

DHCP offer. This is a notification indicating when a particular subscriber has obtained a DHCP lease.

DHCP release. This is a notification indicating when a particular subscriber has released a DHCP lease.

AAA login redirect. This is a notification indicating when the device has captured port 80 traffic and redirected the subscriber.

AAA logout redirect. This is a notification indicating when the device has received a logout request and redirected the subscriber to the AAA logout URL.

AAA session timeout. This is a notification indicating when the device has detected an inactive session and automatically logged the subscriber out.

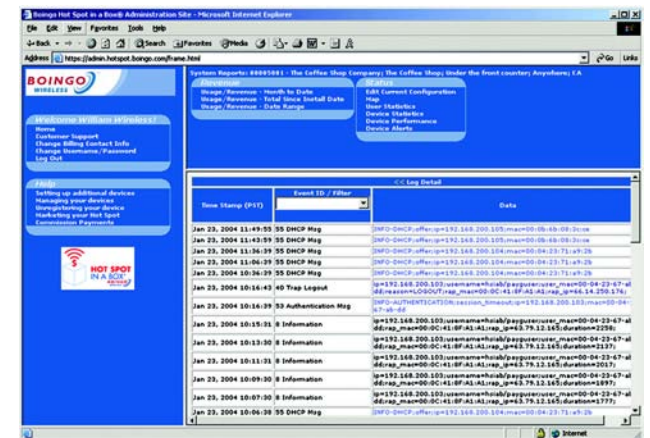


Figure 7-26: Device Alerts

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’m trying to access the Router’s Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, “404 Forbidden.”*

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility’s login screen (Netscape Navigator will require similar steps):

1. Click **File**. Make sure *Work Offline* is NOT checked.
2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
3. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

2. *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.

3. I want to test my Internet connection.

A Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Refer to Windows Help 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.

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

- Refer to "Problem #3, 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 F: 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: Configuring the Wireless-G VPN Broadband Router" 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: Configuring the Wireless-G VPN Broadband Router" 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.

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

- Refer to "Problem #3, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
 1. Refer to "Appendix F: 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 #2: I need to set a static IP address."
 3. Refer to "Problem #11: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

6. *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 #8, 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.

7. 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 F: 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:

Application	Start and End	Protocol	IP Address	Enabled
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

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

8. 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 F: 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:

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

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

9. 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.

10. 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.

11. 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.

12. 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.

13. 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: Configuring the Wireless-G VPN Broadband Router."

14. 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 #2, 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.

15. 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.

16. 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

17. 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.

18. 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 F: 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 802.11b standard?

It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

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 IEEE 802.11g features are supported?

The product supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- OFDM 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

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (as shown in this User Guide) (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

To ensure network security, steps one through five should be followed, at least.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for “beacon messages”. These messages can be easily decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator’s password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. 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.



Note: Some of these security features are available only through the network router or access point. Refer to the router or access point’s documentation for more information.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set 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.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. 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 to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all 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.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.



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

WPA Pre-Shared Key. If you do not have a RADIUS server, select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

WPA RADIUS. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP

Overview

The Linksys Wireless-G VPN Broadband Router offers a free QuickVPN software program for computers running Windows 2000 or XP. (Computers running other operating systems will have to use a third-party VPN software program.) This guide describes how to install and use the Linksys QuickVPN software.

Before You Begin

The QuickVPN software program only works with a Wireless-G VPN Broadband Router that meets these two criteria: 1) it is running firmware version 2.36 or higher, and 2) it **MUST** be properly configured to accept a QuickVPN connection. If you need to upgrade the Router's firmware or configure it for a QuickVPN connection, refer to "Appendix H: Upgrading Firmware."

After you have verified that the Router is ready for a QuickVPN connection, make sure you have the necessary information: user name, password, and server address for your QuickVPN connection. If you do not have this information, contact your system administrator.

Installing the Linksys QuickVPN Software



NOTE: If you have the Wireless-G VPN Broadband Router Setup CD-ROM available, then follow these instructions:

1. Insert the Setup CD-ROM into your CD-ROM drive. The Setup Wizard should run automatically, and the *Welcome* screen should appear. If it does not, click **Start** and then **Run**. In the field provided, enter **D:\setup.exe** (if "D" is the letter of your CD-ROM drive).
2. Click **Install QuickVPN Software**. Then follow the on-screen instructions.

1. Go to www.linksys.com and select **Products**.
2. Click **Business Solutions**.
3. Click **Router/VPN Solutions**.

vpn (virtual private network): a security measure to protect data as it leaves one network and goes to another over the Internet.

software: instructions for the computer.



Figure C-1: Setup Wizard - Welcome Screen

4. Click **WRV54G**.
5. Click **Linksys QuickVPN Utility** in the More Information section.
6. Save the zip file to your PC, and extract the .exe file.
7. Double-click the .exe file, and follow the on-screen instructions. Then proceed to the next section, "Using the Linksys QuickVPN Software."

Using the Linksys QuickVPN Software

1. Double-click the Linksys QuickVPN software icon on your desktop or in the system tray.
2. The login screen will appear. Enter a name for your profile.

Then enter the User Name and Password you have been assigned.

In the *Server Address* field, enter the IP address or domain name of the Wireless-G VPN Broadband Router.

3. To begin your QuickVPN connection, click the **Connect** button. To save this profile, click the **Save** button. To delete this profile, click the **Delete** button. For information, click the **Help** button.
4. When your QuickVPN connection is active, the status screen will appear, and the QuickVPN tray icon will turn green. It will display the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.

To terminate the VPN tunnel, click the **Disconnect** button. If you want to change your password, click the **Change Password** button. For information, click the **Help** button.



NOTE: You can change your password only if you have been granted that privilege by your system administrator.

5. If you clicked the Change Password button and have permission to change your own password, you will see the *Connect Virtual Private Connection* screen. Enter your password in the *Old Password* field. Enter your new password in the *New Password* field. Then enter the new password again in the *Confirm New Password* field. Click the **OK** button to save your new password. Click the **Cancel** button to cancel your change. For information, click the **Help** button.
6. You can create multiple profiles by repeating steps 2 and 3 for each profile.



Figure C-2: QuickVPN Desktop Icon



Figure C-3: QuickVPN Tray Icon - No Connection



Figure C-4: QuickVPN Software - Profile



Figure C-5: QuickVPN Software - Status



Figure C-6: QuickVPN Tray Icon - Connection Available



Figure C-7: QuickVPN Software - Change Password

Appendix D: Configuring IPSec between a Windows 2000 or XP Computer and the Router

Introduction

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

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

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

Environment

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

Windows 2000 or Windows XP

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

Subnet Mask: 255.255.255.0

WRV54G

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

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0



NOTE: Keep a record of any changes you make. Those changes will be identical in the Windows “secpol” application and the Router’s Web-based Utility.



NOTE: The text on your screen may differ from the text in your instructions regarding the *OK* or *Close* buttons; click the appropriate button on your screen.

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.
2. Right-click **IP Security Policies on Local Computer** (Win XP) or **IP Security Policies on Local Machine** (Win 2000), and click **Create IP Security Policy**.
3. Click the **Next** button, and then enter a name for your policy (for example, to_Router). Then, click **Next**.
4. Deselect the **Activate the default response rule** check box, and then click the **Next** button.
5. Click the **Finish** button, making sure the **Edit** check box is checked.

Step 2: Build Filter Lists

Filter List 1: win->Router

1. In the new policy's properties screen, verify that the **Rules** tab is selected. 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.

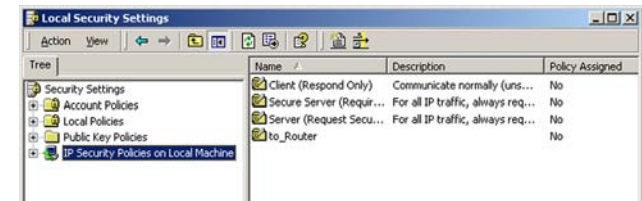


Figure D-1: Local Security Screen



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



NOTE: The text on your screen may differ from the text in your instructions regarding the *OK* or *Close* buttons; click the appropriate button on your screen.

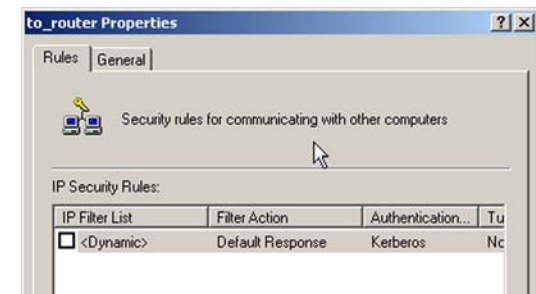


Figure D-2: Rules Tab

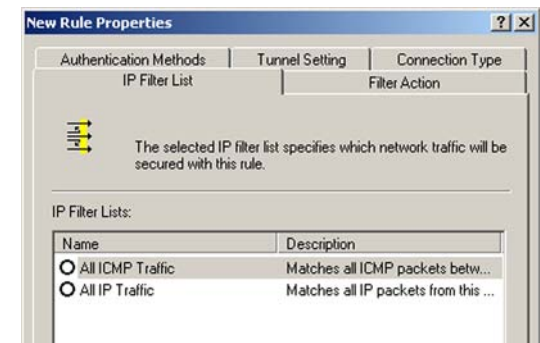


Figure D-3: IP Filter List Tab

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

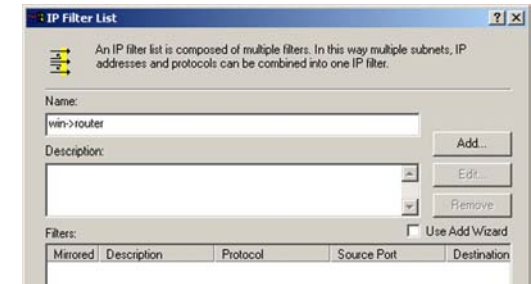


Figure D-4: IP Filter List

4. The *Filters Properties* screen will appear. 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.

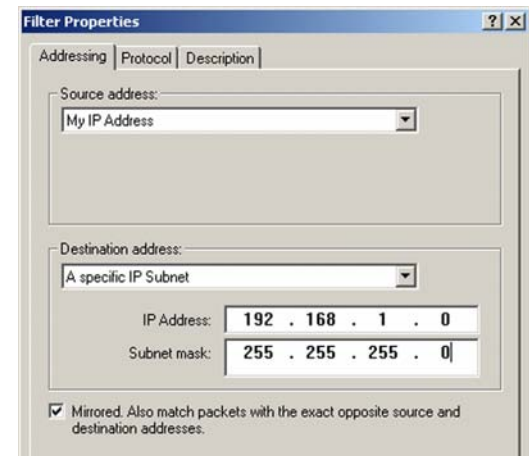


Figure D-5: Filters Properties

6. Click the **OK** button. Then, click the **OK** or **Close** button on the *IP Filter List* window.

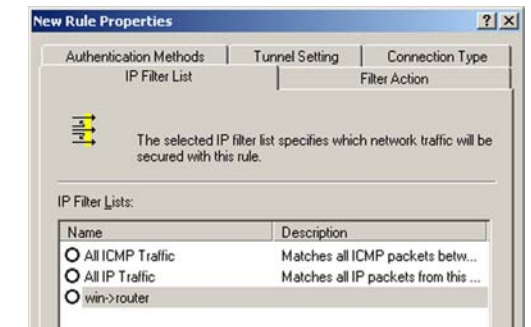


Figure D-6: New Rule Properties

Filter List 2: Router ->win

7. The *New Rule Properties* screen will appear. Select the **IP Filter List** tab, and make sure that **win -> Router** is highlighted. Then, click the **Add** button.
8. The *IP Filter List* screen should appear. Enter an appropriate name, such as Router->win for the filter list, and de-select the **Use Add Wizard** check box. Click the **Add** button.

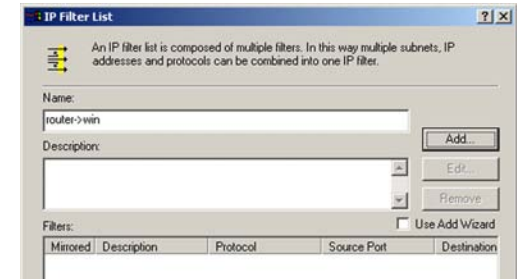


Figure D-7: IP Filter List

9. The *Filters Properties* screen will appear. 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.

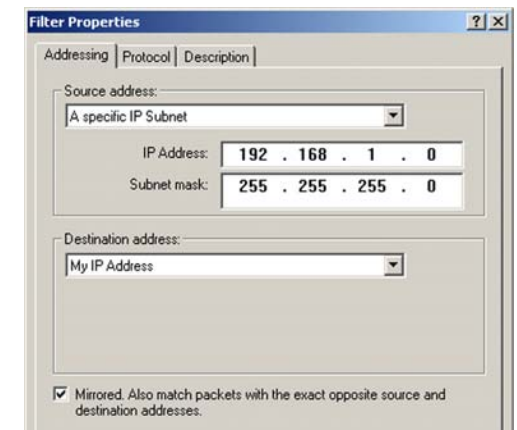


Figure D-8: Filters Properties

11. Click the **OK** or **Close** button and the *New Rule Properties* screen should appear with the IP Filer List tab selected. 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.

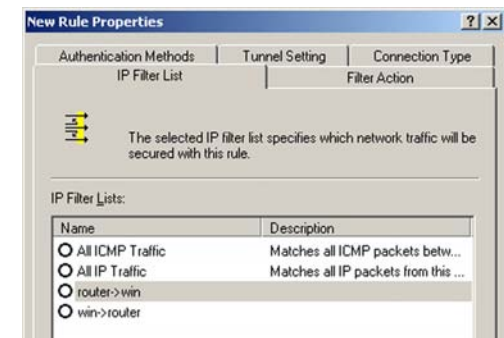


Figure D-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->Router

1. From the *IP Filter List* tab, click the filter list win->Router.

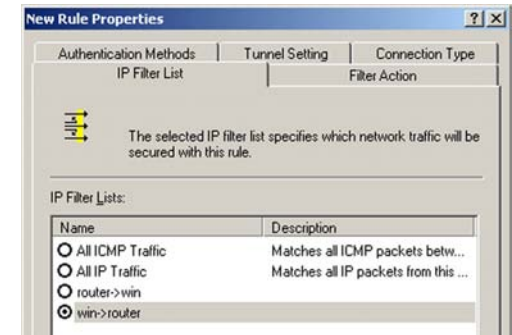


Figure D-10: IP Filter List Tab

2. Click the **Filter Action** tab, and click the filter action **Require Security** radio button. Then, click the **Edit** button.

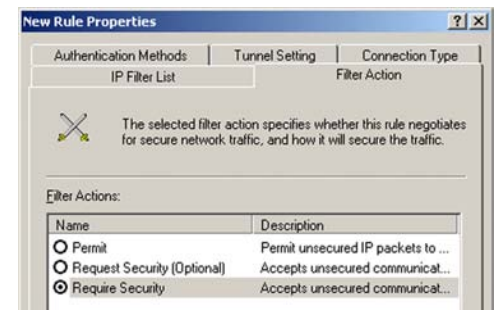


Figure D-11: Filter Action Tab

3. From the *Security Methods* tab, 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.

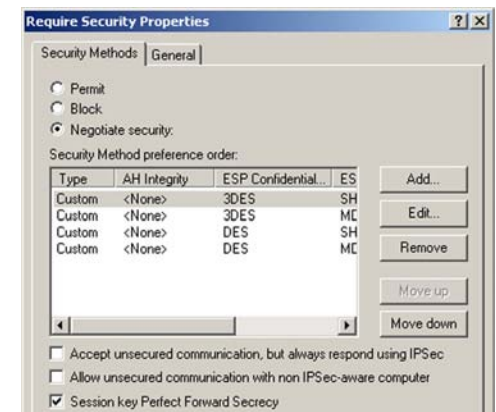


Figure D-12: Security Methods Tab

4. Select the **Authentication Methods** tab, and click the **Edit** button.

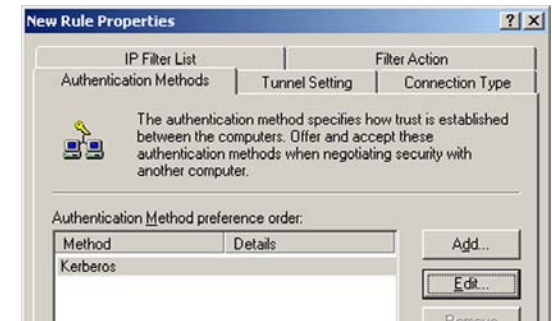


Figure D-13: Authentication Methods

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

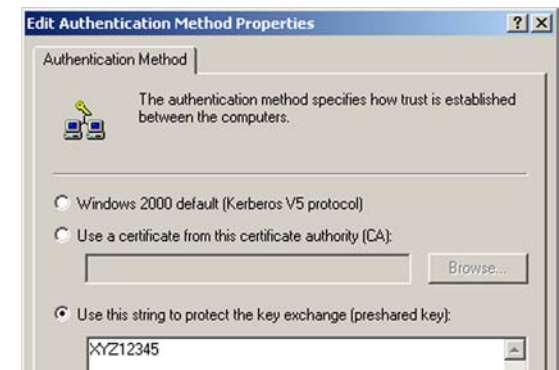


Figure D-14: Preshared Key

6. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen; otherwise, proceed to the next step.



Figure D-15: New Preshared Key

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

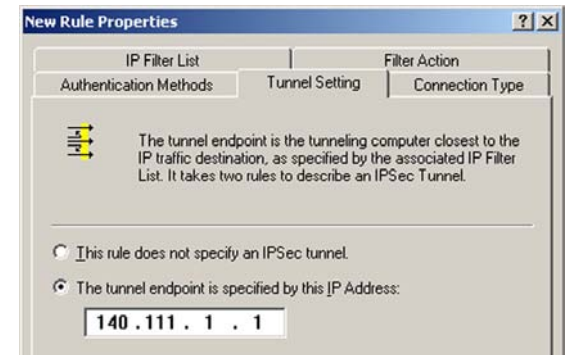


Figure D-16: Tunnel Setting Tab

8. Select the **Connection Type** tab, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

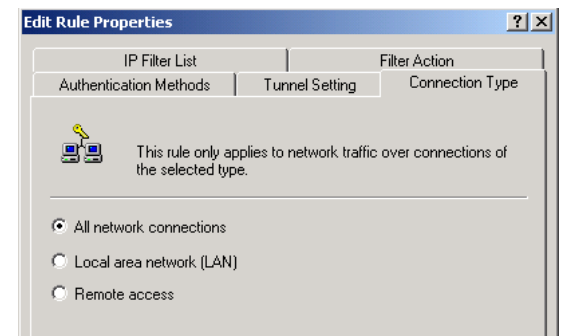


Figure D-17: Connection Type Tab

Tunnel 2: Router->win

9. In the new policy's properties screen, 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.

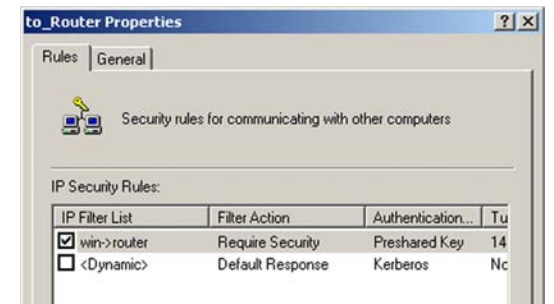


Figure D-18: Properties Screen

10. Go to the **IP Filter List** tab, and click the filter list **Router->win**.

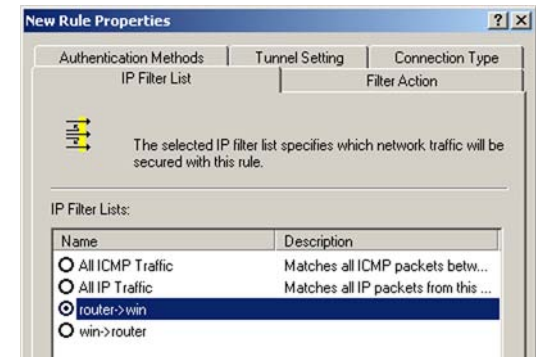


Figure D-19: IP Filter List Tab

11. Click the **Filter Action** tab, and select the filter action **Require Security**. Then, click the **Edit** button. From the *Security Methods* tab, 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.

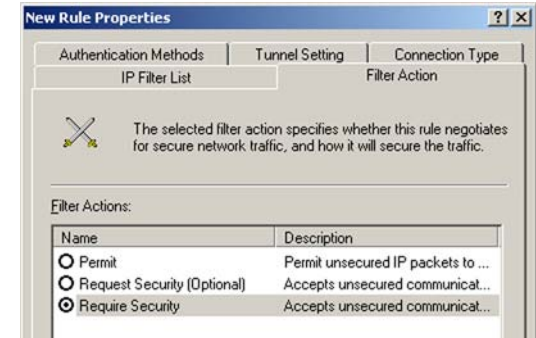


Figure D-20: Filter Action Tab

12. Click the **Authentication Methods** tab, and verify that the authentication method **Kerberos** is selected. Then, click the **Edit** button.

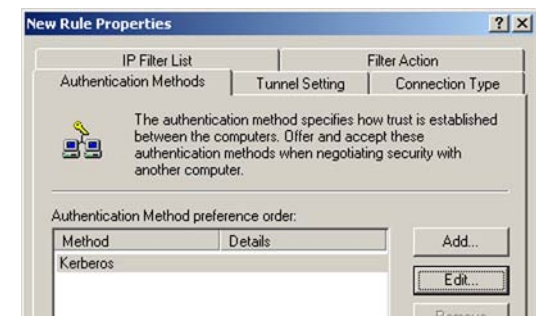


Figure D-21: Authentication Methods Tab

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. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.



Figure D-22: Preshared Key

14. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen; otherwise, proceed to the next step.

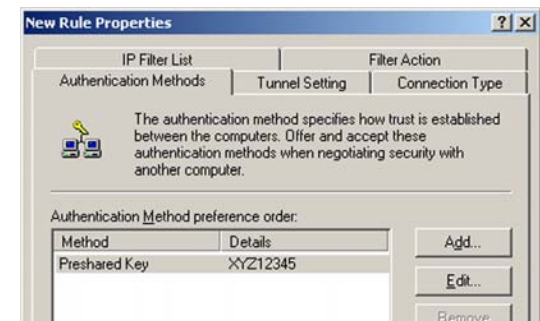


Figure D-23: New Preshared Key

15. Click the **Tunnel Setting** tab. Click the radio button for **The tunnel endpoint is specified by this IP Address**, and enter the Windows 2000/XP computer's IP Address.

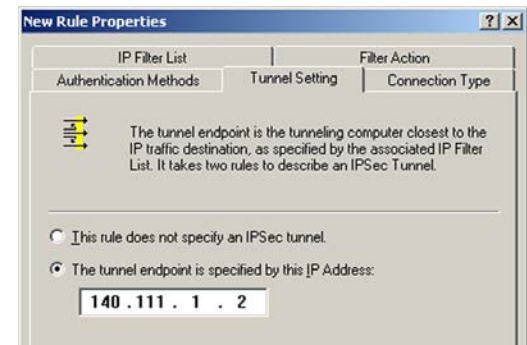


Figure D-24: Tunnel Setting Tab

16. Click the **Connection Type** tab, and select **All network connections**. Then click the **OK** or **Close** button to finish.



Figure D-25: Connection Type

17. From the *Rules* tab, click the **OK** or **Close** button to return to the screen showing the security policies.

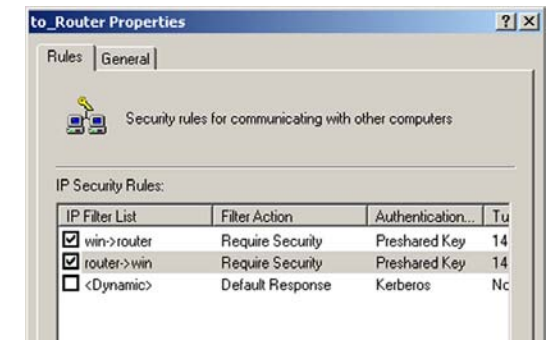


Figure D-26: Rules

Step 4: Assign New IPSec Policy

In the *IP Security Policies on Local Machine* window, right-click the policy named *to_Router*, and click **Assign**. A green arrow appears in the folder icon.

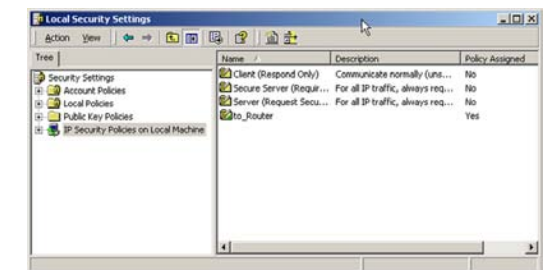


Figure D-27: Local Computer

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* fields appear, enter the default user name and password, **admin**. Press the **Enter** key.
3. From the *Setup* tab, click the **VPN** tab.
4. From the *VPN* tab, 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 Router* fields.
7. Select from 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**.
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 you designate. 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.

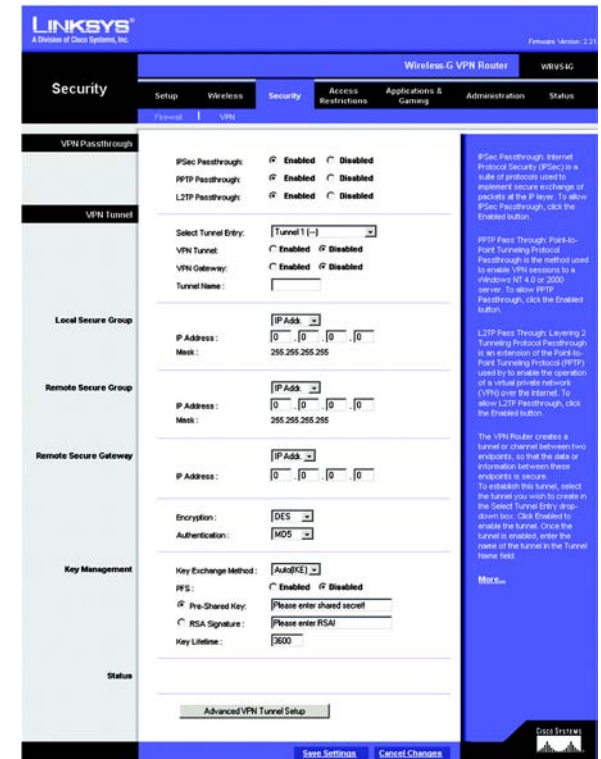


Figure D-28: VPN Tab

Appendix E: Configuring VPN Tunnels

Overview

This appendix has two sections. The first explains how to configure a VPN IPsec tunnel between two VPN Routers. The second explains how to connect a QuickVPN client to the VPN Router.

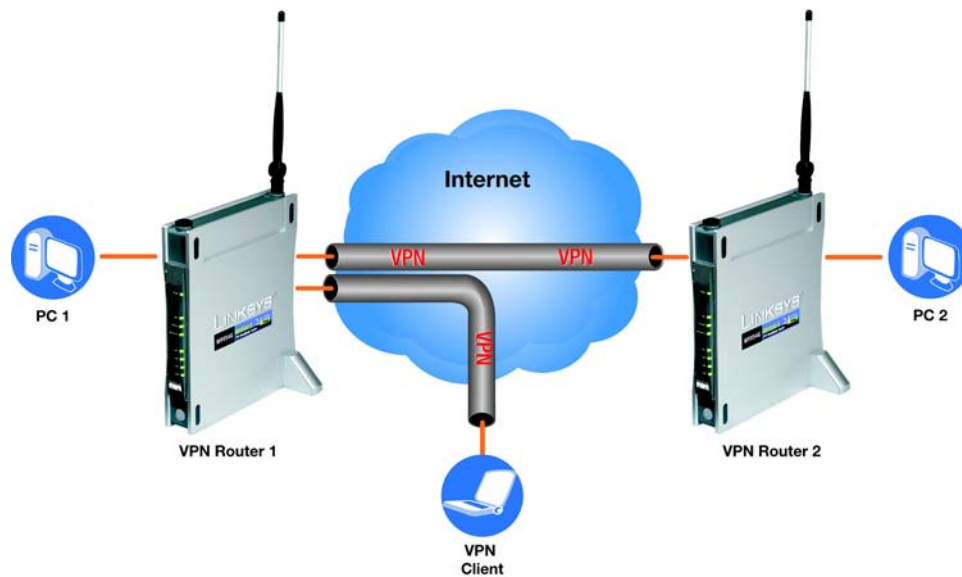


Figure E-1: Diagram of All VPN Tunnels

Before You Begin

The following is a list of equipment you need:

- Two Windows desktop PCs (each PC will be connected to a VPN Router)
- One QuickVPN client (a Windows notebook or desktop PC with QuickVPN software installed)
- Two VPN Routers



NOTE: Each computer must have a network adapter installed.

Configuring the VPN Settings for the VPN Routers

Configuring VPN Router 1

Follow these instructions for the first VPN Router, designated VPN Router 1. The other VPN Router is designated VPN Router 2.

1. Launch the web browser for a networked PC, designated PC 1.
2. Enter the VPN Router's local IP address in the *Address* field (default is **192.168.1.1**). Then press **Enter**.
3. A password request page will appear. (Non-Windows XP users will see a similar screen.) Complete the *User Name* and *Password* fields (**admin** is the default user name and password). Then click the **OK** button.
4. The first screen that appears will be the *Basic Setup* screen. For the Internet Connection Type, select **Automatic Configuration - DHCP**.
5. Click the **Security** tab.
6. Click the **VPN** tab.
7. For the VPN Tunnel setting, select **Enabled**.
8. Enter a name in the *Tunnel Name* field.
9. For the Local Secure Group, select **Subnet**. Enter VPN Router 1's local network settings in the *IP Address* and *Mask* fields.
10. For the Remote Secure Group, select **Subnet**. Enter VPN Router 2's local network settings in the *IP Address* and *Mask* fields.
11. For the Remote Secure Gateway, select **IP Addr**. Enter VPN Router 2's WAN IP address in the *IP Address* field.
12. Click the **Save Settings** button.



Figure E-2: Login Screen



Figure E-3: Setup - Basic Setup (Internet Setup)

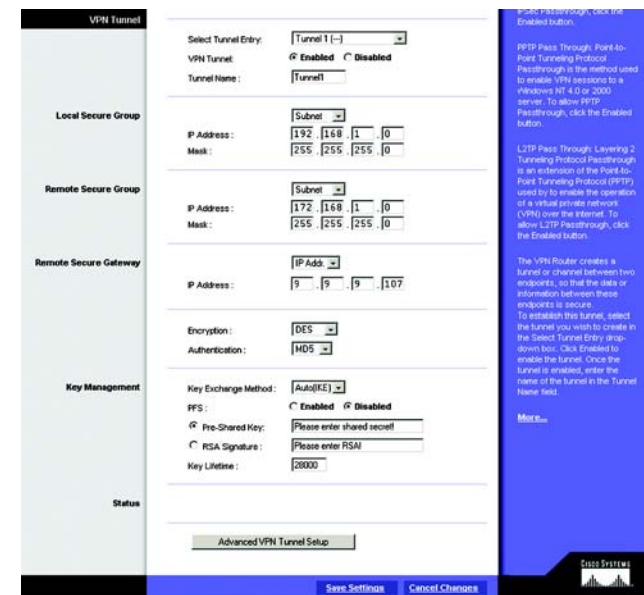


Figure E-4: Security - VPN Screen (VPN Tunnel)

Configuring VPN Router 2

Follow similar instructions for VPN Router 2.

1. Launch the web browser for a networked PC, designated PC 2.
2. Enter the VPN Router's local IP address in the *Address* field (default is **192.168.1.1**). Then press **Enter**.
3. A password request page will appear. (Non-Windows XP users will see a similar screen.) Complete the *User Name* and *Password* fields (**admin** is the default user name and password). Then click the **OK** button.
4. The first screen that appears will be the *Basic Setup* screen. For the Internet Connection Type, select **Automatic Configuration - DHCP**.
5. Click the **Security** tab.
6. Click the **VPN** tab.
7. For the VPN Tunnel setting, select **Enabled**.
8. Enter a name in the *Tunnel Name* field.
9. For the Local Secure Group, select **Subnet**. Enter VPN Router 2's local network settings in the *IP Address* and *Mask* fields.
10. For the Remote Secure Group, select **Subnet**. Enter VPN Router 1's local network settings in the *IP Address* and *Mask* fields.
11. For the Remote Secure Gateway, select IP Addr. Enter VPN Router 1's WAN IP address in the *IP Address* field.
12. Click the **Save Settings** button.



Figure E-5: Setup - Basic Setup (Internet Setup)

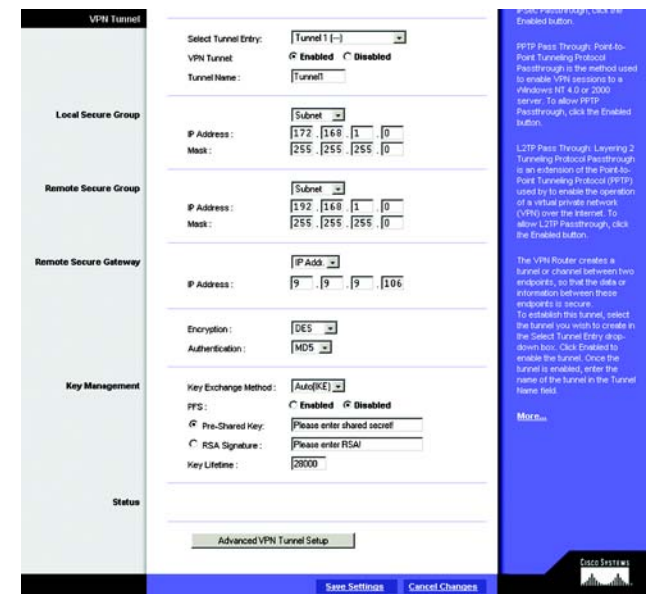


Figure E-6: Security - VPN Screen (VPN Tunnel)

Configuring the Key Management Settings

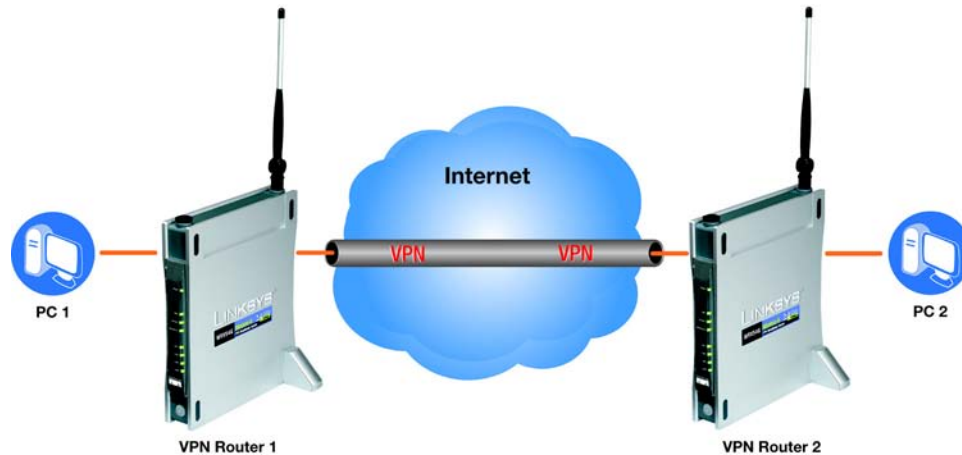


Figure E-7: Diagram of VPN Tunnel between VPN Routers

Configuring VPN Router 1

Following these instructions for VPN Router 1.

1. On the *VPN* screen, select **3DES** from the *Encryption* drop-down menu.
2. Select **SHA1** from the *Authentication* drop-down menu.
3. Keep the default Key Exchange Method, **Auto(IKE)**.
4. For the PFS setting, select **Enabled**.
5. Select **Pre-Shared Key**, and enter a string for this key.
6. If you need more detailed settings, click the **Advanced VPN Tunnel Setup** button. Otherwise, click the **Save Settings** button and proceed to the next section, "Configuring VPN Router 2."
7. On the *Advanced VPN Tunnel Setup* screen, keep the default Operation Mode, **Main**.
8. For Phase 1, select **DES** from the *Encryption* drop-down menu.
9. Select **MD5** from the *Authentication* drop-down menu.

The screenshot shows the 'Security - VPN Screen (Key Management)' configuration interface. The interface is divided into three main sections: 'Remote Secure Gateway', 'Key Management', and 'Status'.
 - **Remote Secure Gateway**: Includes an 'IP Addr.' dropdown and an 'IP Address' field with a dotted decimal input (9 . 9 . 9 . 107).
 - **Key Management**: Includes an 'Encryption' dropdown set to '3DES', an 'Authentication' dropdown set to 'SHA1', a 'Key Exchange Method' dropdown set to 'Auto(IKE)', a 'PFS' section with 'Enabled' selected, a 'Pre-Shared Key' field containing '1234567890', an 'RSA Signature' field with the placeholder 'Please enter RSA!', and a 'Key Lifetime' field set to '28000'.
 - **Status**: Contains an 'Advanced VPN Tunnel Setup' button.
 At the bottom right, there are 'Save Settings' and 'Cancel Changes' buttons.

Figure E-8: Security - VPN Screen (Key Management)

10. Select **768-bit** from the *Group* drop-down menu.
11. Enter **3600** in the *Key Life Time* field.
12. For Phase 2, the Encryption, Authentication, and PFS settings were set on the *VPN* screen.

Select **1024-bit** from the *Group* drop-down menu.

13. Keep the default Key Life Time value, **28000**.
14. Click the **Save Settings** button on the *Advanced VPN Tunnel Setup* screen.
15. Click the **Save Settings** button on the *VPN* screen.

Configuring VPN Router 2

For VPN Router 2, follow the same instructions in the previous section, “Configuring VPN Router 1.”

Configuring PC 1 and PC 2

1. Set PC 1 and PC 2 to be DHCP clients (refer to Windows Help for more information).
2. Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information).

If the computers can ping each other, then you know the VPN tunnel is configured correctly. You can select different algorithms for the encryption, authentication, and other key management settings for VPN Routers 1 and

2. Refer to the previous section, “Configuring the Key Management Settings,” for details.

Congratulations! You have successfully configured a VPN tunnel between two VPN Routers.

Proceed to the next section if you want to connect a QuickVPN client to a VPN Router.

Connecting a VPN Client

Configuring the VPN Client Settings for VPN Router 1

Follow these instructions for VPN Router 1.

1. Click the **Access Restrictions** tab.
2. Click the **VPN Client Access** tab.

The screenshot shows the 'Advanced VPN Tunnel Setup' interface. The title bar is blue with the text 'Advanced VPN Tunnel Setup'. The main content area is white. At the top, it says 'Tunnel 1'. Below this, there are two sections: 'Phase 1' and 'Phase 2'. Phase 1 settings include: Operation Mode (Main), Proposal (Main), Encryption (DES), Authentication (MD5), Group (768-bit), and Key Life Time (3600). A note below Phase 1 states: '(Note: Following three additional proposals are also proposed in Main mode: DES/MD5/768, 3DES/SHA/1024 and 3DES/MD5/1024.)'. Phase 2 settings include: Proposal (Main), Encryption (3DES), Authentication (SHA1), PFS (Enabled), Group (1024-bit), and Key Life Time (28000). At the bottom, there are three buttons: 'Save Settings', 'Cancel Changes', and 'Help'. Below the buttons, there are checkboxes for 'NetBIOS broadcast', 'Anti-replay', 'Keep Alive', and 'If IKE failed more than 5 times, block this unauthorized IP for 60 seconds'.

Figure E-9: Advanced Tunnel Setup Screen

Wireless-G VPN Broadband Router

3. Enter the username in the *Username* field.
4. Enter the password in the *Password* field, and enter it again in the *Re-enter to confirm* field.
5. Click the **Add/Save** button.
6. Click the **Active** checkbox for VPN Client No. 1.
7. Click the **Save Settings** button.

Configuring the QuickVPN Settings for the VPN Client

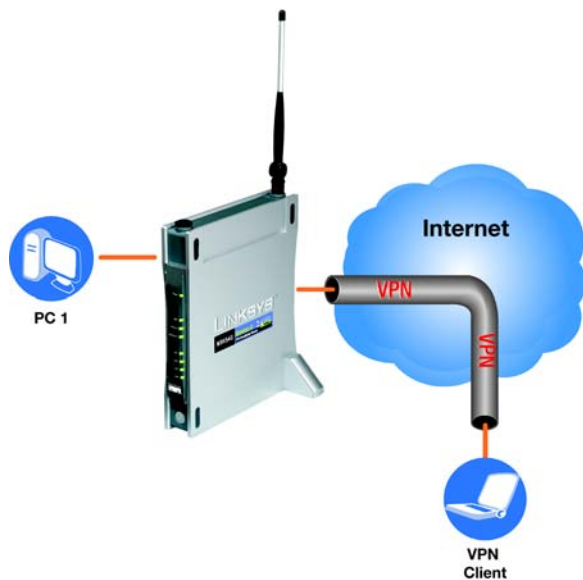


Figure E-11: Diagram of VPN Tunnel between VPN Router 1 and VPN Client

1. Activate the high-speed Internet connection on the VPN client.
2. Double-click the Linksys QuickVPN software icon on your desktop or in the system tray.
3. The login screen will appear. Enter a name for your profile.
4. Enter the user name in the *User Name* field.

The screenshot shows the 'Access Restrictions' configuration page for a Linksys Wireless-G VPN Router. The 'VPN Client Access' tab is selected. The 'VPN Client Status' section shows a table with columns: No., Active, Username, Password, and Edit/Remove. The first row is for 'user' and is checked as 'Active'. The 'Add/Save' button is visible. The 'VPN Client List Table' section shows a table with columns: No., Active, Username, Password, and Edit/Remove. The first row is for 'user' and is checked as 'Active'. The 'Add/Save' button is visible. The 'VPN Client List Table' section shows a table with columns: No., Active, Username, Password, and Edit/Remove. The first row is for 'user' and is checked as 'Active'. The 'Add/Save' button is visible.

Figure E-10: Access Restrictions - VPN Client Access Screen



NOTE: The VPN client is a Windows desktop PC or notebook with QuickVPN installed.



Figure E-12: QuickVPN Desktop Icon

The screenshot shows the 'Linksys VPN Client' window. The 'QuickVPN' logo is prominent. Below it, the 'Profile Name' is set to 'ipsec-vpn'. The 'User Name' is 'user' and the 'Password' is 'password'. The 'Server Address' is '12.1.1.2'. The 'Connect', 'Save', 'Delete', and 'Help' buttons are at the bottom.

Figure E-13: QuickVPN Software - Profile

5. Enter the password in the *Password* field.
6. Enter the WAN IP address of VPN Router 1 in the *Server Address* field.
7. Click the **Connect** button.
8. When your QuickVPN connection is active, the status screen will appear, and the QuickVPN tray icon will turn green. It will display the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.
9. Verify that the VPN client and PC 1 can ping each other.
10. To terminate the VPN tunnel, click the **Disconnect** button. The QuickVPN tray icon will turn gray.

Congratulations! You have successfully created a QuickVPN connection.

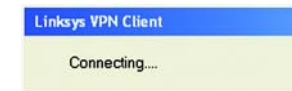


Figure E-14: Connecting

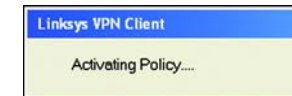


Figure E-15: Activating Policy



Figure E-16: Verifying Network



Figure E-17: QuickVPN Software - Status



**Figure E-18: QuickVPN Tray
Icon - Connection**



**Figure E-19: QuickVPN Tray
Icon - No Connection**

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

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

Windows 98 or Me Instructions

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

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

On the *MAC Address/Adapter Address* screen, the example shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.



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

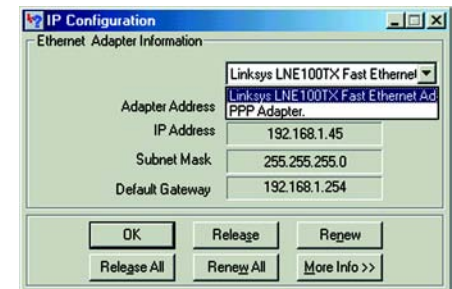


Figure F-1: IP Configuration Screen

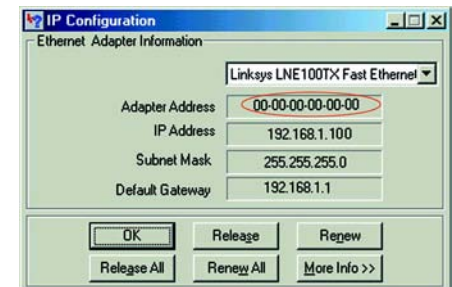


Figure F-2: MAC Address/Adapter Address

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; 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.

On the *MAC Address/Physical Address* screen, the example shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

```

C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . : 
Primary DNS Suffix . . . . . : 
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  : 
   Description . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
   dapter
   Physical Address. . . . . : 00-00-00-00-00-00
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . : 192.168.1.100
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
   DHCP Server . . . . . : 192.168.1.1
   DNS Servers . . . . . : 192.168.1.1

   Primary WINS Server . . . . . : 192.168.1.1
   Secondary WINS Server . . . . . : 
   Lease Obtained. . . . . : Monday, February 11, 2002 2:31:47 PM
   Lease Expires . . . . . : Tuesday, February 12, 2002 2:31:47 PM
  
```

Figure F-3: MAC Address/Physical Address

Appendix G: SNMP Functions

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

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

Appendix H: Upgrading Firmware

You can use the Router's Web-based Utility to upgrade the firmware; however, if you do so, you will lose the settings you have configured on the Router. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.

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

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

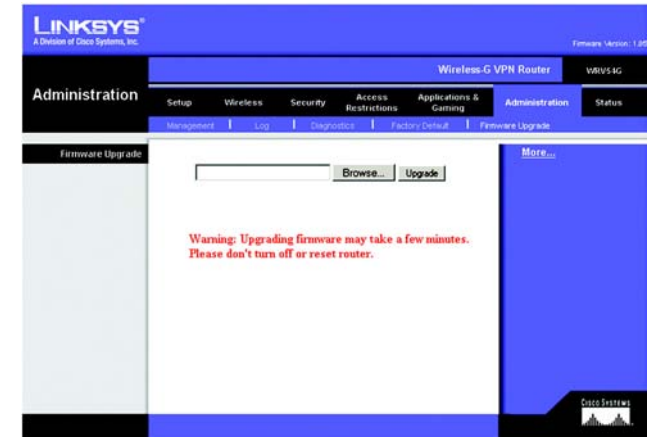


Figure H-1: Upgrade Firmware

Appendix I: Windows Help

Almost 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 J: Glossary

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at <http://www.linksys.com/glossary>.

Access Point - A 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.

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

AES (Advanced Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

Byte - A unit of data that is usually eight bits long.

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

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

DDNS (Dynamic Domain Name System) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

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

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

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.

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

EAP (Extensible Authentication Protocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

Encryption - Encoding data transmitted in a network.

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

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

Firmware - The programming code that runs a networking device.

FTP (File Transfer Protocol) - A protocol used to transfer files over a TCP/IP network.

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

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

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

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

Infrastructure - A wireless network that 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.

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

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

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.

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.

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 mail server commonly used on the Internet.

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

Power over Ethernet (PoE) - A technology enabling an Ethernet network cable to deliver both data and power.

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.

RADIUS (Remote Authentication Dial-In User Service) - A protocol that uses an authentication server to control network access.

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.

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.

SPI (Stateful Packet Inspection) Firewall - A technology that inspects incoming packets of information before allowing them to enter the network.

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

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

TCP/IP (Transmission Control Protocol/Internet Protocol) - A set of instructions PCs use to communicate over a network.

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

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

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

TKIP (Temporal Key Integrity Protocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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 network data transmitted on a wireless network for greater security.

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

WPA (Wi-Fi Protected Access) - A wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix K: Specifications

Standards	802.11b, 802.11g, 802.3
Ports	Internet, Ethernet (1-4), Power
Buttons	Power, Reset
Cabling Type	UTP CAT 5 or better
LEDs	Power, Internet, Ethernet (1, 2, 3, 4), Wireless-G, DMZ
Transmit Power	19 dBm
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	5 V, 2.5 A
Certifications	FCC, IC-03
Operating Temp.	32° ~ 104° F (0° ~ 40° C)
Storage Temp.	-4° ~ 158° F (-20° ~ 70° C)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix L: Warranty Information

LIMITED WARRANTY

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

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. **BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING.** If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. **RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.** You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

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

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

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

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

Appendix M: Regulatory Information

FCC Statement

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

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

FCC Radiation Exposure Statement

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

Safety Notices

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

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

Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Industry Canada (Canada)

This device complies with Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:



English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk/Danish**Miljøinformation for kunder i EU**

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German**Umweltinformation für Kunden innerhalb der Europäischen Union**

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian**Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele**

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootet või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish**Información medioambiental para clientes de la Unión Europea**

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Ελληνικά/Greek**Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης**

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός, ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινотικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/CE richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķīrotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājāsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskās un elektroniskās ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmestā atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākās ziņas par novecojušu aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdurbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart municipli li ma għex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir iehor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklaġġ jghin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyek, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszeren keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwie spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácnosti. Je vaša povinnosť likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshantering eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

Appendix N: 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](ftp://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:
Or fax your request in to:

800-546-5797 (LINKSYS)
949-823-3002

If you experience problems with any Linksys product, you can call us at:

800-326-7114
support@linksys.com

Don't wish to call? You can e-mail us at:

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.)

949-823-3000