LINKSYS®
A Division of Cisco Systems, Inc.

USER GUIDE

BUSINESS SERIES

4-Port Gigabit Security Router with VPN

Model: RVS4000

Cisco Systems

Copyright and Trademarks

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 Guide:

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

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

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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

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

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the 4-Port Gigabit Security Router with VPN. The Linksys 4-Port Gigabit Security Router with VPN is an advanced Internet-sharing network solution for your small business needs. Like any router, it lets multiple computers in your office share an Internet connection.

The 4-Port Gigabit Security Router with VPN also features a built-in 4-Port full-duplex 10/100/1000 Ethernet switch to connect four PCs directly, or you can connect more hubs and switches to create as big a network as you need.

The Virtual Private Network (VPN) capability creates encrypted "tunnels" through the Internet, allowing up to 5 remote offices and 5 traveling users to securely connect into your office network from off-site. Users connecting through a VPN tunnel are attached to your company's network — with secure access to files, e-mail, and your intranet — just as if they were in the building. You can also use the VPN capability to allow users on your small office network to securely connect out to a corporate network. The QoS features provide consistent voice and video quality throughout your business.

Ethernet: *a network protocol that specifies how data is placed on and retrieved from a common transmission medium.*

The 4-Port Gigabit Security Router with VPN can serve as a DHCP Server, and has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks. It can be configured to filter internal users' access to the Internet, and has IP and MAC address filtering so you can specify exactly who has access to your network. Configuration is a snap with the web browser-based configuration utility.

This user guide will give you all the information you need to connect, set up, and configure your Router.

What's in this Guide?

This user guide covers the steps for setting up and using the 10/100 4-Port VPN Router.

- Chapter 1: Introduction
  This chapter describes the 4-Port Gigabit Security Router with VPN applications and this User Guide.
- Chapter 2: Networking Basics
  This chapter describes the basics of networking.
- Chapter 3: Planning Your Virtual Private Network (VPN)
  This chapter describes a VPN and its various applications.
- Chapter 4: Getting to Know the Router
  This chapter describes the physical features of the Router.
- Chapter 5: Connecting the Router
  This chapter instructs you on how to connect the Router to your network.
- Chapter 6: Setting Up and Configuring the Router
  This chapter explains how to use the Web-based Utility to set up the Router and configure its settings.
- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the 4-Port Gigabit Security Router with VPN.
- Appendix B: 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 C: 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 pre-shared keys to join a private network inside the VPN Router and a Windows 2000 or XP PC.
- Appendix D: Configuring a Gateway-to-Gateway IPSec Tunnel
  This appendix describes how to configure an IPSec VPN Tunnel between two VPN Routers.
- Appendix E: 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 F: Physical Setup of the Router
  This appendix describes the physical setup of the Router.
- Appendix G: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- Appendix H Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix I: Specifications
  This appendix provides the technical specifications for the Router.
- Appendix J: Warranty Information
  This appendix supplies the warranty information for the Router.
- Appendix K: Regulatory Information
  This appendix supplies the regulatory information regarding the Router.
- Appendix L: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Networking Basics

An Introduction to LANs

A Router is a network device that connects two networks together.

The Router connects your local area network (LAN), or the group of PCs in your home or office, to the Internet. The Router processes and regulates the data that travels between these two networks.

The Router's Network Address Translation (NAT) technology protects your network of PCs so users on the Internet cannot "see" your PCs. This is how your LAN remains private. The Router protects your network by inspecting the first packet coming in through the Internet port before delivery to the final destination on one of the Ethernet ports. The Router inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

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

The Use of IP Addresses

IP stands for Internet Protocol. Every device in an IP-based network, including PCs, print servers, and routers, requires an IP address to identify its location, or address, on the network. This applies to both the Internet and LAN connections.

There are two ways of assigning IP addresses to your network devices.

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

***Static IP address**: a fixed address assigned to a computer or device that is connected to a network.*

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

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

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

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

A DHCP server can either be a designated PC on the network or another network device, such as the Router. By default, the Router's Internet Connection Type is **Obtain an IP automatically** (DHCP).

The PC or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

For DSL users, many ISPs may require you to log on with a user name and password to gain access to the Internet. This is a dedicated, high-speed connection type called Point to Point Protocol over Ethernet (PPPoE). PPPoE is similar to a dial-up connection, but PPPoE does not dial a phone number when establishing a connection. It also will provide the Router with a dynamic IP address to establish a connection to the Internet.

By default, a DHCP server (on the LAN side) is enabled on the Router. If you already have a DHCP server running on your network, you MUST disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Router, see the Basic Setup section in "Chapter 6: Setting Up and Configuring the Router."

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

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

Since the Router uses NAT technology, the only IP address that can be seen from the Internet for your network is the Router's Internet IP address. However, even this Internet IP address can be blocked, so that the Router and network seem invisible to the Internet.

Chapter 3: Planning Your Virtual Private Network (VPN)

Why do I need a VPN?

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

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

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

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

2) Data Sniffing

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

3) Man in the middle attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a “man in the middle” attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the

data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

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

What is a 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.)

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

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

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

There are two basic ways to create a VPN connection:

- VPN Router to VPN Router
- Computer (using 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

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 C: Configuring IPSec between a Windows 2000 or XP PC 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 D: Configuring a Gateway-to-Gateway IPSec Tunnel."

Figure 3-1: VPN Router to VPN Router

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 B: Using the Linksys QuickVPN Software for Windows 2000 or XP", "Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the Router," and "Appendix D: Configuring a Gateway-to-Gateway IPSec Tunnel."

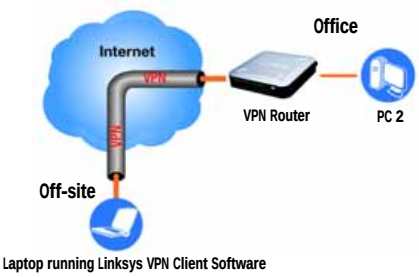


Figure 3-2: Computer to VPN Router

Chapter 4: Getting to Know the Router

The Front Panel

The Router's LEDs are located on the front panel of the Router.

Figure 4-1: Front Panel

LEDs

Power	Green. The **Power** LED lights up when the Router is powered on. If the LED is flashing, the Router is running a diagnostic test.
Diag	Red. The **Diag** LED lights up when the system is not ready. The LED goes off when the system is ready. The Diag LED blinks during Firmware upgrades.
IPS	Green. The **IPS** LED lights up when the IPS function is enabled. If the LED is off, then IPS functions are disabled. If the IPS LED is flashing green, then an external attack has been detected. If the IPS LED is flashing red, an internal attack has been detected.
Internet	Green. The **Internet** LED lights up the appropriate LED depending upon the speed of the device attached to the Internet port. If the Router is connected to a cable or DSL modem, typically the 10 LED will be the only LED lit up. Flashing indicates activity.
1-4 (Ethernet)	Green. For each port, there are three LEDs. If the corresponding LED is continuously lit, the Router is connected to a device at the speed indicated through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.

The Back and Side Panels

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

Figure 4-2: Back Panel

Reset Button

Reset Button	The Reset button can be used in one of two ways: If the Router is having problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the Reset button on your PC to reboot it. If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for 10 seconds. This will restore the factory defaults and clear all of the Router's settings, such as port forwarding or a new password.

Ports

1-4 (Ethernet)	The four **Ethernet** ports connect to network devices, such as PCs, print servers, or additional switches.
Internet	The **Internet** port connects to a cable or DSL modem.
Power	The **Power** port is where you will connect the included AC power cable.

Chapter 5: Connecting the Router

Overview

To set up your network, you will do the following:

- Connect the Router to one of your PCs according to the instructions in this chapter.
- By default, Windows 98, 2000, Millennium, and XP computers are set to obtain an IP address automatically, so unless you have changed the default setting, then you will not need to configure your PCs. (If you do need to configure your PCs, refer to Windows Help for more information.)
- Set up and configure the Router with the setting(s) provided by your Internet Service Provider (ISP) according to "Chapter 6: Setting Up and Configuring the Router."

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

Figure 5-1: Example of a Typical Network

Connection Instructions

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

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

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

Proceed to "Chapter 6: Setting Up and Configuring the Router."

Figure 5-2: Connect a PC

Figure 5-3: Connect the Internet

Figure 5-4: Connect the Power

Chapter 6: Setting Up and Configuring the Router

Overview

For your convenience, use the Router's Web-based Utility to set it up and configure it. This chapter will explain all of the functions in this Utility.

There are eight main tabs in the Utility: Setup, Firewall, VPN, QoS, Administration, IPS, L2 Switch, and Status. Additional tabs will be available after you click one of the main tabs. The tabs are described below:

Setup

- IP Mode. Provides options for IPv4 NAT Router mode or Dual-Stack Router mode.
- WAN. The Internet connection settings are entered and displayed on this screen.
- LAN. The Local Area Network (LAN) settings are entered and displayed on this screen.
- DMZ. The DMZ (Demilitarized Zone) Host feature allows one local user to be exposed to the Internet to use a special-purpose service such as Internet gaming or video conferencing.
- MAC Address Clone. Some ISPs require that you register a MAC address. This feature "clones" your network adapter's MAC address onto the Router, and prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address.
- Advanced Routing. The Router's dynamic routing feature can be used to automatically adjust to physical changes in the network's layout.
- Time. Change the time on this screen.

Firewall

- Basic. Basic Firewall settings are configured from here.
- Internet Access Policy. Network Access Rules evaluate the network traffic's Source IP address, Source MAC address, and IP protocol type to decide if the traffic is allowed to pass through the firewall.
- Single Port Forwarding. To set up public services or other specialized Internet applications with a single port on your network, click this tab.

- Port Range Forwarding. To set up public services or other specialized Internet applications on your network using a port range, click this tab.
- Port Range Triggering.To set up triggered ranges and forwarded ranges for Internet applications, click this tab.

VPN

- IPSec VPN. The VPN Router creates a tunnel or secure channel between two endpoints, so that the transmitted data or information between these endpoints is secure.
- VPN Client Accounts. Use this screen to designate VPN clients and their passwords.
- VPN Pass Through. This tab allows you to disable IPSec Pass Through, PPTP Pass Through, and L2TP Pass Through.

QoS

- Application-based QoS. This involves Internet traffic, which may involve demanding, real-time applications, such as videoconferencing.
- Port-based QoS. This ensures better service to a specific LAN port.

Administration

- Management. Alter the Router's password, its access privileges, SNMP settings, and UPnP settings.
- Reporting. Allows configuration of Log settings.
- Diagnostics. Use this screen to check the connection between the Router and a PC on the LAN or Internet.
- Backup & Restore. Allows you to save and load router configuration settings.
- 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.

IPS

- Configure. Enable or disable IPS functions from this screen.
- P2P/IM. Allows or block specific Peer to Peer (P2P) networks and Instant Messaging (IM) applications.

- Report. Provides report of network traffic and malicious attacks.
- Information. Provides the Protection Scope of the router.

L2 Switch

- VLAN. Virtual Local Area Network (VLAN) categorization is done from this screen.
- RADIUS. Used for configuration of Remote Authorization Dial-In User Service (RADIUS) settings.
- Port Setting. Allows configuration of port speeds and duplex.
- Statistics. Displays transmit and receive statistics.
- Cable Diagnostics. Used for testing cabling connected to the LAN ports.

Status

- Gateway. This screen provides status information about the Router.
- Local Network. This provides status information about the local network.
- VPN Clients. This screen provides status information about the Router's VPN clients.

How to Access the Web-based Utility

The router is configured using the built-in Web-based utility. To access the Web-based Utility of the Router:

- Launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Press the **Enter** key.
- A screen will appear asking you for your User name and Password. Enter **admin** in the *User Name* field, and enter your password (default password is **admin**) in the *Password* field. Then click the **OK** button.

Figure 6-1: Router's IP Address

Figure 6-2: Password

Setup Tab

The Setup screen contains all of the Router's basic setup functions. The device can be used in most network settings without changing any of the default values. Some users may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL, cable modem) carrier.

Figure 6-3: Setup Tab

IP Mode

IPv4 Only: This option utilizes IPv4 on the Internet and local network.

Dual-Stack IP: This options utilizes IPv4 over the Internet and IPV4 and IPv6 on the local network.

Click the **Save Settings** button to save the network settings or click the **Cancel Changes** button to undo your changes.

Figure 6-4: Obtain an IP Automatically

WAN

Internet Connection Type

The Router supports six connection types. 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.

Static IP

If your connection uses a permanent IP address to connect to the Internet, then select **Static IP**.

Figure 6-5: Static IP

Internet 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 Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the *Max Idle Time* field.

Keep Alive 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 option 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.

Figure 6-6: PPPoE

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.

PPTP Server. Enter the IP address of the PPTP server.

Figure 6-7: PPTP

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 Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the *Max Idle Time* field.

Keep Alive 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.

Heart Beat Signal

Heart Beat Signal is a service used in Australia. Check with your ISP for the necessary setup information.

Figure 6-8: Heart Beat Signal

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

Heart Beat Server. Enter the IP address of the Heart Beat server.

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 Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the *Max Idle Time* field.

Keep Alive 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.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.

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.

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

L2TP Server. Enter the IP address of the L2TP server.

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

Connect on Demand and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific 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 Connect on Demand option and enter the number of minutes you want to have elapsed before your Internet connection terminates in the *Max Idle Time* field.

Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to *Keep Alive*. The default Redial Period is **30** seconds.

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

Figure 6-9: L2TP

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: Some ISPs, usually cable ISPs, require a host name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host name. In most cases, leaving this field blank will work.

Domain Name: Some ISPs, usually cable ISPs, require a domain name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a domain name. In most cases, leaving this field blank will work.

MTU: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that will be transmitted. To have the Router select the best MTU for your Internet connection, keep the default setting, Auto

Size: When Manual is selected in the MTU field, this option is enabled. It is recommended that you set this value within the 1200 to 1500 range, but the value can be defined between 128 and 1500.

DDNS Service: DDNS Service is disabled by default. To enable DDNS Service, follow these instructions:

1. Sign Up for DDNS Service
    - DynDNS - Sign up for DDNS service at www.dyndns.org, and write down your User Name, Password, and Host Name information.
    - TZO - Sign up for DDNS service at www.tzo.com, and write down your E-mail Address, Password and Domain Name information.
2. Select the DDNS service provider whose service you are using.
3. Configure the following fields:
    - User Name (DynDNS) or E-mail address (TZO).
    - Password
    - Host Name (DynDNS) or Domain name (TZO)
4. Click Save Settings.

The Router will now advise the DDNS Service of your current WAN (Internet) IP address whenever this address changes. If using TZO, you should NOT use the TZO software to perform this "IP address update".

Connect button: When DDNS is enabled, the Connect button is displayed. This button is used to contact the DDNS server to manually update your IP address information. The Status area on this screen is also updated.

LAN

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

Figure 6-10: LAN

IPv4

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

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

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

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.

DHCP Server. DHCP is already enabled by factory default.If you already have a DHCP server on your network, or you don't want a DHCP server, then select Disabled (no other DHCP features will be available). If you already have a DHCP server on your network, and you want this Router to act as a Relay for that DHCP Server, select DHCP Relay, then enter the DHCP Server IP Address. If you disable DHCP, assign a static IP address to the Router.

Starting IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, but smaller than 192.168.1.254, because the default IP address for the Router is 192.168.1.1, and 192.168.1.255 is the broadcast IP address.

Maximum Number of DHCP Users. 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.

Client Lease Time. This is the amount of time a DHCP client can keep the assigned IP address before it sends a renewal request to the DHCP server.

Static DNS 1-3. If applicable, enter the IP address(es) of your DNS server(s).

WINS. The Windows Internet Naming Service (WINS) provides name resolution service (similar to DNS) in Windows networks. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

IPv6

IPv6 Address. If your network has implemented IPv6, enter the proper IPv6 address in this field.

Prefix Length. Enter the appropriate IPv6 prefix length.

Router Advertisement. Enabling this option allows IPv6 hosts to configure their IP addresses automatically using the IPv6 prefix broadcast by the router.

Primary DNS. Enter the Primary IPv6 DNS server address.

Secondary DNS. Enter the Secondary IPv6 DNS server address.

DMZ

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

Figure 6-11: DMZ Host

DMZ Hosting. This feature allows one local PC 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 DMZ feature, select **Disabled**.

DMZ Host IP Address. To expose one PC, enter the computer's IP address.

Click the **Save Settings** button to save the network settings or click the **Cancel Changes** button to undo your changes.

MAC Address Clone

Some ISPs require that you register a MAC address. This feature "clones" your network adapter's MAC address onto the Router, and prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address. The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification.

Figure 6-12: Mac Clone

Mac Address Clone. Enabled or Disabled.

Mac Address. Enter the MAC Address registered with your ISP in this field.

Clone My PC's MAC button. When Mac Address clone is enabled, click this to copy the MAC address of the network adapter in the computer that you are using to connect to the Web interface.

Click **Save Settings** to save the MAC Cloning settings or click the **Cancel Changes** button to undo your changes.

Advanced Routing

Operating Mode

Select the Operating mode in which this Router will function.

Gateway. This is the normal mode of operation. This allows all devices on your LAN to share the same WAN (Internet) IP address. In Gateway mode, the NAT (Network Address Translation) mechanism is enabled.

Router. You either need another Router to act as the Internet Gateway, or all PCs on your LAN must be assigned (fixed) Internet IP addresses. In Router mode, the NAT mechanism is disabled.

Dynamic Routing

The Router's dynamic routing feature can be used to automatically adjust to physical changes in the network's layout. The Router uses the dynamic RIP protocol. It determines the route that the network packets take 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 (Routing Information Protocol): The Router, using the RIP protocol, calculates the most efficient route for the network's data packets to travel between the source and the destination, based upon the shortest paths.

RIP Send Packet Version: Choose the TX protocol you want for transmitting data on the network: None, RIPv1, RIPv2-Broadcast, or RIPv2-Multicast. This should match the version supported by other Routers on your LAN.

RIP Recv Packet Version: Choose the RX protocol you want for receiving data from the network: None, RIPv1, RIPv2, or Both RIPv1 and v2. This should match the version supported by other Routers on your LAN.

Static Routing

You will need to configure Static Routing if there are multiple routers installed on your network. The static routing function determines the path that data follows over your network before and after it passes through the Router. You can use static routing to allow different IP domain users to access the Internet through this device. This is an advanced feature. Please proceed with caution.

This Router is also capable of dynamic routing (see the Dynamic Routing tab). In many cases, it is better to use dynamic routing because the function will allow the Router to automatically adjust to physical changes in the network's layout. In order to use static routing, the Router's DHCP settings must be disabled.

Figure 6-13: Advanced Routing

Figure 6-14: Routing Table Entry List

To set up static routing, you should add routing entries in the Router's table that tell the device where to send all incoming packets. All of your network routers should direct the default route entry to the Linksys Router.

Enter the following data to create a static route entry:

1. **Select Set Number**: Select the set number (routing table entry number) that you wish to view or configure. If necessary, click Delete This Entry to clear the entry.
2. **Destination IP Address**: Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be zero.
3. **Subnet Mask**: Enter the Subnet Mask used on the destination LAN IP domain. For Class C IP domains, the Subnet Mask is 255.255.255.0.
4. **Gateway**: If this Router is used to connect your network to the Internet, then your gateway IP is the Router's IP Address. If you have another router handling your network's Internet connection, enter the IP Address of that router instead.
5. **Hop Count (max. 16)**: This value gives the number of nodes that a data packet passes through before reaching its destination. A node is any device on the network, such as switches, PCs, etc.

Click the **Save Settings** button to save the Routing settings, click the **Cancel Changes** button to undo your changes or click the **Show Routing Table** button to view the current routing table.

Time

Manually

If you wish to enter the time and date manually, select the **Date** from the drop-down fields and enter the hour, minutes, and seconds in the **Time** field using 24 hour format (example 10:00pm would be entered 22:0:0).

Automatically

Time Zone. Select the time zone for your location and your time setting is synchronized over the Internet.

Auto Daylight Saving. If your location observes daylight savings time, select the **Enable** option.

Figure 6-15: Time

Firewall Tab

From the Firewall Tab, you can configure the Router to deny or allow specific internal users from accessing the Internet. You can also configure the Router to deny or allow specific Internet users from accessing the internal servers. You can set up different packet filters for different users that are located on internal (LAN) side or external (WAN) side based on their IP addresses or their network Port number.

Figure 6-16: Firewall Basic

Basic

SPI Firewall Protection: SPI (Stateful Packet Inspection), when enabled this feature will block DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it.

Restrict WEB Features

Block. Place a checkmark next to the Web features that you wish to restrict.

- **Proxy**: If local users have access to WAN proxy servers, they may be able to circumvent the Router's content filters and access Internet sites blocked by the Router. Denying Proxy will block access to any WAN proxy servers.
- **Cookies**: A cookie is data stored on your PC and used by Internet sites when you interact with them, so you may not want to deny cookies.
- **Java Applets**: Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language.
- **ActiveX**: ActiveX is a Microsoft (Internet Explorer) programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites using this programming language. Also, Windows Update uses ActiveX, so if this is blocked, Windows update will not work.

Block WAN Request

Block Anonymous Internet Requests. Check this checkbox if you wish to have these filtered out.

Internet Access Policy

Access can be managed by a policy. Use the settings on this screen to establish an access policy. Selecting a policy from the drop-down menu will display that policy's settings. You can then perform the following operations:

Figure 6-17: Internet Access Policy

- Create a Policy - see instructions below.
- Delete the current policy - click the **Delete** button.
- View all policies - click the **Summary** button. On the Summary screen, the policies are listed with the following information: No., Policy Name, Days, Time, and a checkbox to delete (clear) the policy. To delete a policy, check the checkbox in the Delete column, and click the Delete button
- View or change the PCs covered by the current policy - click the **Edit List of PCs** button.

On the List of PCs screen, you can define PCs 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.

To create an Internet Access policy:

1. Select the desired policy number from the **Internet Access Policy** drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select the **Enable** option.
4. Click the **Edit List of PCs** button to select which PCs will be affected by the policy. The List of PCs screen will appear in a sub-window. 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 **Save Settings** button to apply your changes.
5. 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.
6. 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. Enter a range of hours and minutes during which the policy will be in effect, or select 24 Hours.
7. If you wish to block access to Web sites, use the **Website Blocking by URL Address** or **Website Blocking by Keyword** feature.
   - **Website Blocking by URL Address**. Enter the URL or Domain Name of the web sites you wish to block.
   - **Website Blocking by Keyword**. Enter the keywords you wish to block in the fields provided. If any of these Keywords appears in the URL of a web site, access to the site will be blocked. Note that only the URL is checked, not the content of each Web page.

Figure 6-18: List of PC's

Figure 6-19: Internet Policy Summary

8. You can filter access to various applications accessed over the Internet, such as FTP or telnet, by selecting up to two services to block in the **Blocked Services** section. The block services select list offers a choice of preset applications. If you select a preset application, its port numbers and protocol are displayed and can not be changed. If the application you want to block is not listed, select User-Defined, then you can enter the port range and protocol for the service you wish to block. To remove the blocking, select "None" in the service list.

9. Click the **Save Settings** button to save the policy settings.

Single Port Forwarding

Figure 6-20: Single Port Forwarding

Application Name. Enter the name of the application you wish to configure.

External Port. This is the port number used by the server or Internet application. Internet users must connect using this port number. Check with the software documentation of the Internet application for more information.

Internal Port. This is the port number used by the Router when forwarding Internet traffic to the PC or server on your LAN. Normally, this is the same as the External Port number. If it is different, the Router performs a "Port Translation", so that the port number used by Internet users is different to the port number used by the server or Internet application.

For example, you could configure your Web Server to accept connections on both port 80 (standard) and port 8080. Then enable Port Forwarding, and set the External Port to 80, and the Internal Port to 8080. Now, any traffic from the Internet to your Web server will be using port 8080, even though the Internet users used the standard port, 80. (Users on the local LAN can and should connect to your Web Server using the standard port 80.)

Protocol. Select the protocol used for this application, TCP and/or UDP.

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.

Port Range Forwarding

Figure 6-21: Port Range Forwarding

Application. Enter the name of the application you wish to configure.

Start. This is the beginning of the port range. Enter the beginning of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.

End. This is the end of the port range. Enter the end of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.

Protocol. Select the protocol(s) used for this application, TCP and/or UDP.

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

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

Port Range Triggering

Application Name. Enter the name of the application you wish to configure.

Triggered Range. For each application, list the triggered port number range. These are the ports used by outgoing traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number of the Triggered Range.

Forwarded Range. For each application, list the forwarded port number range. These are the ports used by incoming traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

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

Figure 6-22: Port Range Triggering

VPN Tab

IPSec VPN

Select Tunnel Entry. Select a tunnel to configure.

Delete Button. Click this button to delete all settings for the selected tunnel.

Summary Button. Clicking this button shows the settings and status of all enabled tunnels.

IPSec VPN Tunnel. Check the Enable option to enable this tunnel.

Tunnel Name. Enter a name for this tunnel, such as “Anaheim Office”.

Figure 6-23: VPN

Local Security Group

Local Security Group Type. Select the local LAN user(s) behind the router that can use this VPN tunnel. This may be a single IP address or Sub-network. Notice that the Local Security Group must match the other router's Remote Security Group.

IP Address. Enter the IP address on the local network.

Subnet Mask. If the "Subnet" option is selected, enter the mask to determine the IP addresses on the local network.

Remote Security Group

Remote Security Group. Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address, a Sub-network, or any addresses. If "Any" is set, the router acts as responder and accepts request from any remote user. Notice that the Remote Security Group must match the other router's Local Security Group.

IP Address. Enter the IP address on the remote network.

Subnet Mask. If the "Subnet" option is selected, enter the mask to determine the IP addresses on the remote network.

Remote Security Gateway

Remote Security Gateway Type. Select the desired option - IP address or "Any". If the remote gateway has a dynamic IP address, select "Any".

IP Address. The IP address in this field must match the public IP address (i.e. WAN IP Address) of the remote gateway at the other end of this tunnel.

Key Management

Key Exchange Method. The router supports both automatic and manual key management. When choosing automatic key management, IKE (Internet Key Exchange) protocols are used to negotiate key material for SA. If manual key management is selected, no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purpose. Notice that both sides must use the same Key Management method.

Auto IKE

Encryption. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Only 3DES is supported. Notice that both sides must use the same Encryption method.

Authentication. Authentication determines a method to authenticate the ESP packets. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.

- MD5: A one way hashing algorithm that produces a 128-bit digest.
- SHA1: A one way hashing algorithm that produces a 160-bit digest.

PFS. If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. Note: that both sides must have this selected.

Pre-Shared Key. IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field. e.g. “My_@123” or “0x4d795f40313233” Note: that both sides must use the same Pre-shared Key.

Key Life Time. This field specifies the lifetime of the IKE generated key. If the time expires, a new key will be renegotiated automatically. The Key Life Time may range from 300 to 100,000,000 seconds. The default Life Time is 3600 seconds.

Manual

Encryption Algorithm. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Only 3DES is supported. Notice that both sides must use the same Encryption method.

Encryption Key. This field specifies a key used to encrypt and decrypt IP traffic. Both character and hexadecimal value are acceptable in this field. Note: that both sides must use the same Encryption Key.

Authentication Algorithm. Authentication determines a method to authenticate the ESP packets. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.

- MD5: A one way hashing algorithm that produces a 128-bit digest.
- SHA1: A one way hashing algorithm that produces a 160-bit digest.

Authentication Key. This field specifies a key used to authenticate IP traffic. Both character and hexadecimal values are acceptable in this field. Note: that both sides must use the same Authentication Key.

Inbound SPI/Outbound SPI. The SPI (Security Parameter Index) is carried in the ESP header. This enables the receiver to select the SA, under which a packet should be processed. The SPI is a 32-bit value. Both decimal and hexadecimal values are acceptable. e.g. “987654321” or “0x3ade68b1”. Each tunnel must have

unique an Inbound SPI and Outbound SPI. No two tunnels share the same SPI. Notice that Inbound SPI must match the other router's Outbound SPI, and vice versa.

Status

Status. This field shows the connection status for the selected tunnel. The state is either connected or disconnected.

Connect button. Use this to establish a connection for the current VPN tunnel. If you have made any changes, click Save Settings to first apply your changes.

Disconnect button. Use this to break a connection for the current VPN tunnel.

View Log button. Click this to view the VPN log, which shows details of each tunnel established.

Advanced Settings button. If the Key Exchange Method is Auto (IKE), this button provides access to some additional settings relating to IKE. Use this if this router is unable to establish a VPN tunnel to the remote VPN Gateway; ensure the Advanced Settings match those on the remote VPN Gateway.

Advanced Settings

Phase 1

Operation Mode. Select the method to match the remote VPN endpoint.

- Main: Main Mode is slower but more secure.
- Aggressive: Aggressive mode is faster but less secure.

Local Identity. Select the desired option to match the “Remote Identity” setting at the other end of this tunnel.

- Local IP address: Your WAN IP Address.
- Name: Your domain name.

Remote Identity. Select the desired option to match the “Local Identity” setting at the other end of this tunnel.

- Local IP address: WAN IP Address of the remote VPN endpoint.
- Name: Domain name of the remote VPN endpoint.

Encryption. Encryption Algorithm used for the IKE SA. This setting must match the setting used at the other end of this tunnel.

Authentication. Authentication Algorithm used for the IKE SA. This setting must match the setting used at the other end of this tunnel.

- MD5: A one way hashing algorithm that produces a 128-bit digest.
- SHA1: A one way hashing algorithm that produces a 160-bit digest.

Group. The Group setting determines the bit size used in the IKE exchange. This value must match the value used at the other end of this tunnel.

Key Life Time. This determines the time interval before the IKE SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time period increases security, it also degrades performance. While this unit is in seconds, it is common to use periods over an hour (3600 seconds) for the SA Life Time.

VPN Client Accounts

Use this page to administer your VPN Client users. Enter the information at the top of the screen and the users you've entered will appear in the list at the bottom, showing their status. This will work with the Linksys QuickVPN client only. (The Router supports up to five Linksys QuickVPN Clients by default. Additional QuickVPN Client licenses can be purchased separately. See www.linksys.com for more information.)

Figure 6-24: VPN Client Accounts

Username. Enter the username using any combination of keyboard characters.

Password. Enter the password you would like to assign to this user.

Re-enter to Confirm. Retype the password to ensure it has been entered correctly.

Allow User to Change Password. This option determines whether the user is allowed to change their password.

VPN Client List Table

No. Displays the user number.

Active. When checked, the designated user can connect, otherwise the VPN client account is disabled.

Username. Displays the username.

Edit button. This button is used to modify the username, password or toggle whether the user is allowed to change their password.

Remove button. This button is used to delete a user account.

Click the **Save Settings** button to save the settings or the **Cancel Changes** button to undo your changes.

VPN Passthrough

Ipsec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default to allow IPSec tunnels to pass through the Router. To disable IPSec Passthrough, select Disabled.

PPTP Passthrough. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Passthrough is enabled by default. To disable PPTP Passthrough, select Disabled.

L2TP Passthrough. Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select Disabled.

Click the **Save Settings** button when you finish the VPN Passthrough settings, or click the **Cancel Changes** button to undo the changes.

Figure 6-25: VPN Passthrough

QoS Tab

QoS (Quality of Service) allows you to prioritize network traffic using either **Application-based** priority (such as Web browsing applications, FTP applications, etc...) or **Port-based** priority which allows you to assign priority to the four physical network ports.

Application-based

Application-based QoS. QoS (Quality of Service) is disabled by default. When enabled, this option allows you to assign priority based on the application type.

Table 1: Application-based QoS

Application Name	Port(s)	Primary Use
FTP	TCP Port 20	FTP (File Transfer Protocol) is used for transferring files over the Internet.
HTTP	TCP Port 80	HTTP (HyperText Transfer Protocol) is used for browsing the Internet.
Telnet	TCP Port 23	Telnet is a client-server protocol used to communicate over a network or the Internet.
SMTP	TCP Port 25	SMTP (Simple Mail Transfer Protocol) is used for sending e-mail.
POP3	TCP Port 110	POP3 (Post Office Protocol version 3) is used for retrieving e-mail.
Specific Port	User Defined	User Defined (0-65535)

Figure 6-26: Application-based QoS

Select the desired option:

- High priority
- Medium priority
- Low priority

Port-based

Physical ports 1-4 can be assigned High, Medium, Normal, or Low priority. Lower priority traffic will be slowed down to allow greater throughput for higher priority traffic.

Figure 6-27: Port-based QoS

Administration Tab

Management

Local Gateway Access

Gateway Userlist. Select the desired Gateway User List.

Gateway Username. Enter the user name here.

Gateway Password. Enter the password.

Re-enter to Confirm. Retype the password in this field.

Remote Gateway Access

Remote Management. To access the Gateway remotely, from outside the local network, select Enable. Otherwise, keeps the default setting, Disable.

Management Port. Enter the port number that will be open to outside access. The default setting is 8080. This port must be used when you establish a remote connection.

SNMP

Device Name. Enter a suitable name. This name will be used to identify this device, and will be displayed by your SNMP software.

SNMP. Select Enable if you wish to use SNMP. To use SNMP, you need SNMP software on your PC.

Read Community. Enter the SNMP community name for SNMP "Get" commands.

Write Community. Enter the SNMP community name for SNMP "Set" commands.

Trap To. Enter the IP Address of the SNMP Manager to which traps will be sent. If desired, this may be left blank.

UPnP. If you want to use UPnP, keep the default setting, Enable. Otherwise, select Disable.

IGMP Proxy. IGMP (Internet Group Membership Protocol) Proxy can facilitate the communication between IGMP clients and IGMP routers. Enable this feature if you are using IGMP-based multicast services in your network.

Log

Email Alerts. If enabled, an e-mail will be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, the E-mail address information (below) must be provided.

Denial of Service Thresholds. Enter the number of DoS (Denial of Service) attacks which need to be blocked by the built-in Firewall before an e-mail alert is sent. The minimum value is 20, the maximum value is 100.

SMTP Mail Server. Enter the address (domain name) or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing e-mail.

Figure 6-28: Administration

Email Address for Alert Logs. Enter the e-mail address the Log is to be sent to.

Return Email Address. The e-mail will show this address as the Sender's address.

Enable Syslog. Enable the checkbox if you want to this feature.

Syslog Server. Enter the IP Address in the Syslog Server field when Enable Syslog is checked.

Local Log. Enable this if you want to see a log of all incoming and outgoing URLs or IP addresses.

View Log button. When you wish to view the logs, click View Log. A new window will appear with the log data.

Figure 6-29: Log

Diagnostics

Ping Test Parameters

Ping Target IP. Enter the IP address or URL that you want to ping.

Ping Size. Enter the size of the packet you want to use.

Number of Pings. Enter the number of times you wish to ping the target device.

Ping Interval. Enter the time period (Milliseconds) between each ping.

Ping Timeout. Enter the desired time period (Milliseconds). If a response is not received within the defined ping period, the ping is considered to have failed.

Start Test. Click this button to begin the test. A new screen will appear and display the test results. A summary of the results will be shown on this screen.

Ping Result. It displays the Ping status.

Figure 6-30: Diagnostics

Backup & Restore

Backup & Restore. Use this to download a copy of the current configuration, and store the file on your PC. Click **Backup** button to start the download.

Restore configuration. This allows you to restore a previously saved config file back to the Router. Click the **Browse** button to select the config file, then click **Restore** button to upload the config file.

Factory Defaults

Restore Factory Defaults. Click this button to reset all configuration settings to their default values. Any settings that have been saved will be lost when the default settings are restored. After clicking the button, another screen will appear. Click **OK** to continue. Another screen will appear while the system reboots.

Firmware Upgrade

WARNING: Uploading a configuration file will destroy (overwrite) ALL of the existing settings.

To upgrade firmware, download the latest firmware for the product from Linksys.com, extract it to your computer, and perform the steps below:

1. **File**. Type in the name of the extracted firmware upgrade file or click **Browse** to locate the file.
2. **Start to Upgrade**. Once you have selected the appropriate file, click the **Start to Upgrade** button and follow the on-screen instructions to upgrade your firmware.

IPS Tab

Configure

IPS Function. Enable or Disable IPS Function.

Abnormally Detection

- **HTTP**. Web attack signature is matched. HTTP request decoder will decode UTF-8 (1,2, and 3 byte) code and normalize URI (according to those evasion methods mentioned in whisker) before pattern match.
- **FTP**. FTP Bounce Detection and Inserting telnet opcodes into FTP command stream Detection.
- **TELNET**. Normalization of Telnet negotiation strings.
- **RPC**. RPC record fragging detection.

Signature Update. Before upgrading the firmware, download the Router firmware upgrade file from the Linksys website, www.linksys.com.

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

Figure 6-31: Backup & Restore

Figure 6-32: Factory Defaults

Figure 6-33: Firmware Upgrade

Figure 6-34: IPS Configure

Update button. After you have selected the appropriate file, click this button, and follow the on-screen instructions.

P2P/IM

Peer to Peer

Peer to peer file sharing applications can be blocked or allowed. The preconfigured file sharing networks are GNUTELLA(EZPEER), FASTTRACK, KURO, EDONKEY2000, BITTORRECT, DIRECTCONNECT, PIGO, and WINMX.

Instant Messenger

Instant messaging applications can be blocked from use or allowed. The preconfigured instant messaging applications are MSN, ICQ, YAHOO MESSEGER, SKYPE, IRC, ODIGO, REDIFF, GOOGLE TALK, and QQ.

Figure 6-35: P2P/IM

Report

Twenty four hour diagram displaying network traffic and attacks.

Attacker

Displays the IP Address of attackers and the frequency (number of times) of the attacks.

Attacked Category

Displays the category (type) of attack and the frequency (number of times) of the attacks.

Figure 6-36: Report

Information

Signature Version. The Signature Version displays the version of the signature patterns in the router that protects against malicious threats.

Last Time Upload. This displays when the signature patterns in the router were last updated.

Protect Scope. Displays a list of the categories of attacks that the IPS feature in the router protects against.

L2 Switch Tab

VLAN

VLAN Configuration

Port/VLAN VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduce the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

VLANs function at layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router functioning router is needed to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs.

VLANs are broadcast and multicast domains. Broadcast and multicast traffic is transmitted only in the VLAN in which the traffic is generated.

Figure 6-37: VLAN

RADIUS

Mode. Choose the function to Enable or Disable RADIUS.

RADIUS IP. Enter the Server IP address.

RADIUS UDP Port. Identifies the UDP port. The UDP port is used to verify the RADIUS server authentication.

RADIUS Secret. Indicates the Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS server encryption key. If no host-specific value is specified, the global value applies to each host.

Administration State. Specifies the port authorization state. The possible field values are:

- **Auto**. The controlled port state is set by the Authentication method.
- **Force Authorized**. The controlled port state is set to Force-Authorized (forward traffic).
- **Force Unauthorized**. The controlled port state is set to Force-Unauthorized (discard traffic).

Port State. It displays the state of the selected port.

Port Setting

Port. Displays the physical port number.

Link. Displays the port duplex mode and speed. Full indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. Half indicates that the interface supports transmission between the device and the client in only one direction at a time.

Mode. Specify port duplex mode and speed. Auto Speed is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

Flow Control. Displays the flow control status on the port. Operates when port is in Full duplex mode.

MaxFrame. Displays the Max frame size the port can receive and send.

Statistics

Statistics Overview

Tx Bytes. Displays the number of Bytes transmitted from the selected port.

Tx Frames. Displays the number of Frames transmitted from the selected port.

Rx Bytes. Displays the number of Bytes received on the selected port.

Rx Frames. Displays the number of Frames received on the selected port.

Tx Errors. Displays the number of error packets transmitted from the selected port.

Rx Errors. Displays the number of error packets received from the selected port.

Cable Diagnostics

Port. Select the port number.

Pair. Each cable consists of 8 pins (4 pairs).

Cable Length. The length of the cable.

Status. The status of the pair.

Figure 6-38: RADIUS

Figure 6-39: Port Setting

Figure 6-40: Statistics

Status Tab

Gateway

Firmware Version. This is the Gateway current firmware.

MAC Address. This is the Gateway MAC Address, as seen by your ISP.

Current Time. This shows the time, based on the time zone you selected on the Setup tab.

Internet Connection

Connection Mode. This shows the mode of the connection.

Login Type. This indicates the type of Internet connection you are using.

Interface. The Gateway Internet Interface is displayed here.

IP Address. The Gateway Internet IP Address is displayed here.

Subnet Mask. This Subnet Mask is associated with the IP address above.

Default Gateway. This is your ISP's Gateway.

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

IPv6 DNS. This displays the IPv6 DNS IP Primary and Second Address.

Figure 6-41: Cable Diagnostics

Figure 6-42: Status

Local Network

Current IP address System. This shows the current system.

MAC Address. This is the Router MAC Address, as seen on your local, Ethernet network.

IP Address. The Internet IP Address is displayed here.

Subnet Mask. This Subnet Mask is associated with the IP address above.

IPv6 Address. This shows the IPv6 IP address, if applicable.

DHCP Server. The status of the Router's DHCP server function is displayed here.

Start IP Address. This shows the beginning of the range of IP addresses used by the DHCP Server.

End IP Address. This shows the end of the range of IP addresses used by the DHCP Server.

DHCP Client Table. Clicking this button will open a screen showing you which PCs are utilizing the Router as a DHCP server. On the DHCP Client Table screen, you will see a list of DHCP clients (PCs and other network devices) with the following information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the length of time before their assigned IP addresses expire.

ARP/RARP Table. Clicking this button will open a screen showing you which PCs are utilizing the Router as a ARP/RARP server. On the ARP/RARP Table screen, you will see a list of ARP/RARPs (PCs and other network devices) with the following information: IP Addresses and MAC Addresses.

Figure 6-43: Local Network

VPN Clients

Username. Displays the username of the VPN Client.

Status. Displays the connection status of the VPN Client.

Start Time. Displays the start time of the most recent VPN session for the specified VPN Client.

End Time. Displays the end time of a VPN session if the VPN Client has disconnected.

Duration. Displays the total connection time of the latest VPN session.

Refresh button. Updates the screen with the latest VPN Client information.

Disconnect button. Check the Disconnect box and click the **Disconnect** button to disconnect a VPN Client.

Figure 6-44: VPN Clients

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. ***I need to set a static IP address on a PC.***
   The Router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.149 using the DHCP server on the Router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.150 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

   For Windows 98 and Millennium:

   A. Click **Start**, **Setting**, and **Control Panel**. Double-click **Network**.
   B. In *The following network components are installed* box, select the **TCP/IP**-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.
   C. In the *TCP/IP properties* window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Make sure that each IP address is unique for each PC or network device.
   D. Click the **Gateway** tab, and in the *New Gateway* prompt, enter **192.168.1.1**, which is the default IP address of the Router. Click the **Add** button to accept the entry.
   E. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
   F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the *Network* window.
   G. Restart the computer when asked.

For Windows 2000:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
C. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
D. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
I. Restart the computer if asked.

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.

A. Click **Start** and **Control Panel**.
B. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
C. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
D. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
E. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
F. Enter the Subnet Mask, **255.255.255.0**.
G. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
H. 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.
I. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window. Click the **OK** button in the *Local Area Connection Properties* window.

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98 and Millennium:

Refer to Windows Help for details. Make sure **Obtain IP address automatically** is selected in the settings.

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. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
4. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
5. Restart the computer if asked.
6. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
7. 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)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

B. Open a command prompt.

- For Windows 98 and Millennium, click **Start** and **Run**. In the *Open* field, type **command**. Press the **Enter** key or click the **OK** button.

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

C. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
   - If you get a reply, the computer is communicating with the Router.
   - If you do NOT get a reply, check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

D. In the command prompt, type **ping** followed by your Internet IP address and press the **Enter** key. The Internet IP Address can be found in the web interface of the Router. For example, if your Internet IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.
   - If you get a reply, the computer is connected to the Router.
   - If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E. In the command prompt, type **ping www.linksys.com** and press the **Enter** key.
   - If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
   - If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

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

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

4. I am not able to access the Router's Web-based Utility Setup page.

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

5. I can't get my Virtual Private Network (VPN) to work 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 **VPN => VPN Pass Through** tab. Make sure you have IPsec passthrough and/or PPTP passthrough 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 Basic Setup tab of the Web-based Utility. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

Check the Linksys website at *www.linksys.com* for more information.

6. I need to set up a server behind my Router.

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

documentation provided with the server you installed. Follow these steps to set up port forwarding through the Router's Web-based Utility. We will be setting up web, ftp, and mail servers.

A. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Setup** => **Forwarding** tab.
B. Select the Service from the pull-down menu. If the Service you need is not listed in the menu, click the **Service Management** button to add the new Service Name, and enter the Protocol and Port Range. Click the **Add to List** button. Then click the **Save Setting** button. Click the **Exit** button.
C. Enter the IP Address of the server that you want the Internet users to access. 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 E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address. Then check the **Enable** checkbox for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
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

D. Click the **Add to List** button, and configure as many entries as you like.

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

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

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

A. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Setup** => **Forwarding** tab.
B. Select the Service from the pull-down menu. If the Service you need is not listed in the menu, click the **Service Management** button to add the new Service Name, and enter the Protocol and Port Range. For

example, if you have a web server, you would enter the range 80 to 80. Click the **Add to List** button. Then click the **Save Setting** button. Click the **Exit** button.

C. Enter the IP Address of the server that you want the Internet users to access. 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 E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address. Then check the **Enable** checkbox for the entry. Consider the examples 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

D. Click the **Add to List** button, and configure as many entries as you like.

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

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

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

A. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Setup** => **Forwarding** tab.
B. Disable or remove the entries you have entered for forwarding. To delete an entry, select it and then click the **Delete selected application** button. Keep this information in case you want to use it at a later time.
C. Click the **DMZ Host** tab.
D. Enter the Ethernet adapter's IP address of the computer you want exposed to the Internet. This will bypass the NAT security for that computer. Please refer to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Once completed with the configuration, click the **Save Settings** button.

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

Reset the Router to factory defaults by pressing the Reset button for ten seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

A. Access the Router's web interface by going to **http://192.168.1.1** or the IP address of the Router. Enter the default password admin, and click the **Setup** => **Password** tab.
B. Enter the old password in the *Old Password* field.
C. Enter a different password in the *New Password* field, and enter the new password in the *Confirm New Password* field to confirm the password.
D. Click the **Save Settings** button.

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

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

For Microsoft Internet Explorer 5.0 or higher:

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

For Netscape 4.7 or higher:

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

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

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

12. I need to upgrade the firmware.

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

A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware, or use the Web-based Utility to be automatically redirected to the download webpage. Go to System Management - Firmware Upgrade, and click the **Firmware Download from Linksys Web Site** button. Select the Router from the pull-down menu and choose the firmware from the options.
B. Extract the firmware file on your computer.
C. To upgrade the firmware, follow the steps in the Upgrade section found in "Chapter 6: Setting Up and Configuring the Router".

13. The firmware upgrade failed.

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

A. Use the Linksys TFTD program to upgrade the firmware. Go to the Linksys website at **http://www.linksys.com** and download the TFTP program, which will be listed with the firmware.
B. Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

   IP Address: 192.168.1.50
   Subnet Mask: 255.255.255.0
   Gateway: 192.168.1.1

C. Perform the upgrade using the TFTP utility.

If the firmware upgrade failed, the Router will still work using its current firmware.

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

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

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

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

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

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Go to Firewall => General tab.
D. Look for the MTU option, and select **Enable**. In the *Size* field, enter 1492.
E. Click the **Save Settings** button to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
1462
1400
1362
1300

16. I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the Router to open a specific port, depending on which port an Internet application uses. Follow these steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Setup** => **Forwarding** tab.
D. Enter any name you want to use for the Application Name.
E. Enter the Start and End Ports of the Triggered Port Range. Check with your Internet application provider for more information on which outgoing port services it is using.
F. Enter the Start and End Ports of the Forwarded Port Range. Check with your Internet application provider for more information on which incoming port services are required by the Internet application.

Once completed with the configuration, click the **Save Settings** button.

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

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.

- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.
- Manually configure the TCP/IP 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**.

18. 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):

A. Click **File**. Make sure *Work Offline* is NOT checked.
B. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
C. 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.

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 Passthrough supported by the Router?
Yes, enable or disable IPSec Passthrough on the VPN => VPN Pass Through tab.

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 the LAN.

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 98, Millennium, 2000, or 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 to 27900. If you want to use the UT Server Admin, forward another port (8080 usually works well but is used for remote admin. You may have to disable this.), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the 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 for ten seconds. 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 can I be notified of new Router firmware upgrades?
All Linksys firmware upgrades are posted on the Linksys website at *www.linksys.com*, where they can be downloaded for free. The Router's firmware can be upgraded using the 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 5.0 or Netscape Navigator 5.0 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 E: 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 4,000 sessions at the same time, but you can only forward 30 ranges of ports.

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

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

What 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?
Ask your ISP to find out.

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

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

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

Overview

The Linksys 4-Port Gigabit Security Router with VPN 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.

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.*

Before You Begin

The QuickVPN software program only works with a 4-Port Gigabit Security Router with VPN that is properly configured to accept a QuickVPN connection. Follow these instructions for configuring the VPN client settings for the Router:

1. Click the **VPN** tab.
2. Click the **VPN Client Accounts** tab.
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.

Click the **Save Settings** button.

Figure B-1: VPN Client Accounts Screen

Installing the Linksys QuickVPN Software

Installing from the CD-ROM

1. Insert the RVS4000 CD-ROM into your CD-ROM drive. Go to the **Start** menu and then click **Run**. In the field provided, enter **D:\VPN_Client.exe** (if "D" is the letter of your CD-ROM drive).
2. The License Agreement screen appears, click **Yes** to accept the agreement and the appropriate files are copied to the computer.
3. Click **Finished** to complete the installation. Proceed to the section, "Using the Linksys QuickVPN Software".

Downloading and Installing from the Internet

1. Go to *www.linksys.com* and select **Products**.
2. Click **Business Solutions**.
3. Click **Router/VPN Solutions**.
4. Click **RVS4000**.
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. Proceed to the next section, "Using the Linksys QuickVPN Software".

Figure B-2: License Agreement

Figure B-3: Copying Files

Figure B-4: Finished Installing Files

Using the Linksys QuickVPN Software

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

1. Double-click the Linksys QuickVPN software icon on your desktop or in the system tray.

Figure B-5: QuickVPN Desktop Icon

Figure B-6: QuickVPN Tray Icon - No Connection

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 Linksys 4-Port Gigabit Security Router with VPN. To save this profile, click the **Save** button. Multiple profiles can be set up if you want to establish a tunnel to multiple sites. Note that only one tunnel can be active at a time. To delete this profile, click the **Delete** button. For information, click the **Help** button.

Figure B-7: QuickVPN Software - Profile

3. To begin your QuickVPN connection, click the **Connect** button and the Connecting, Activating Policy, and Verifying Network screens appear.

Figure B-8: Connecting

Figure B-9: Activating Policy

Figure B-10: Verifying Network

4. When your QuickVPN connection is established, 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.

Figure B-11: QuickVPN Software - Status

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.

Figure B-12: QuickVPN Tray Icon - Connection

Figure B-13: QuickVPN Tray Icon - No Connection

Figure B-14: QuickVPN Software - Change Password

Appendix C: 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

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.

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

RVS4000

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

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the *Open* field. The *Local Security Setting* screen will appear.
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.

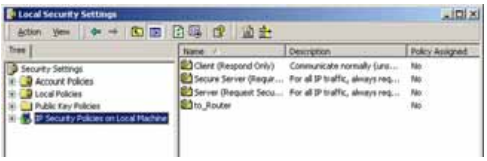


Figure C-1: Local Security Screen

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.

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.

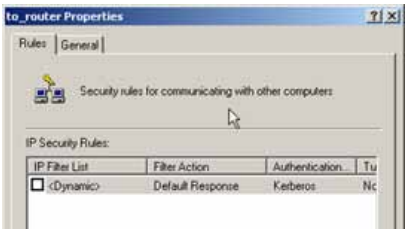


Figure C-2: Rules Tab

2. Make sure the **IP Filter List** tab is selected, and click the **Add** button.

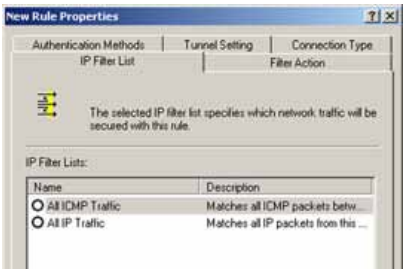


Figure C-3: IP Filter List Tab

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.

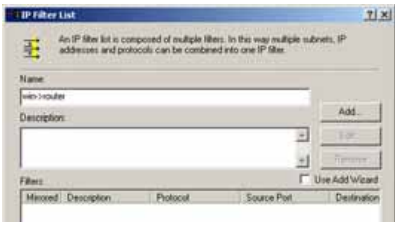


Figure C-4: IP Filter LIst

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.

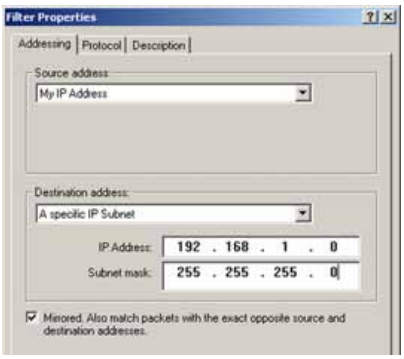


Figure C-5: Filters Properties

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

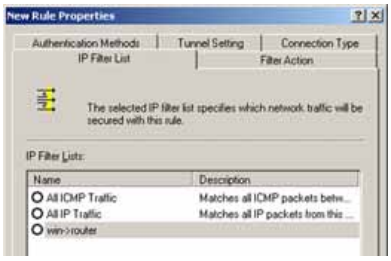


Figure C-6: New Rule Properties

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.

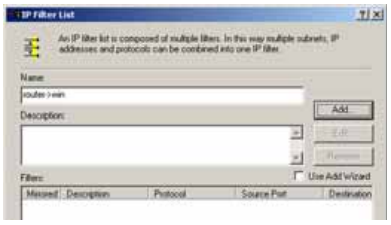


Figure C-7: IP Filter List

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 C-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 C-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.

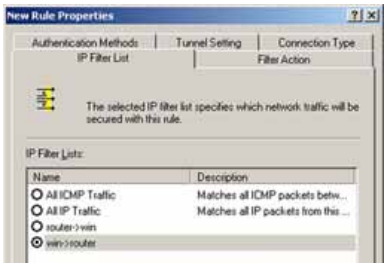


Figure C-10: IP Filter List Tab

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

Figure C-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.

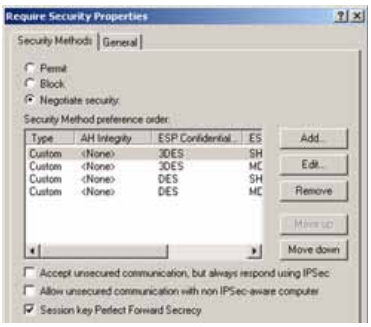


Figure C-12: Security Methods Tab

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

Figure C-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.

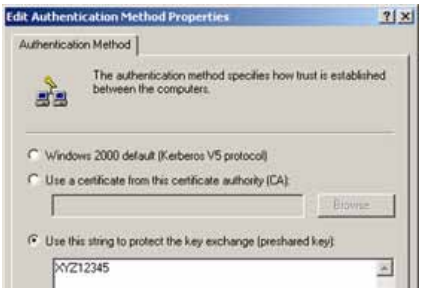


Figure C-14: Preshared Key

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 C-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.

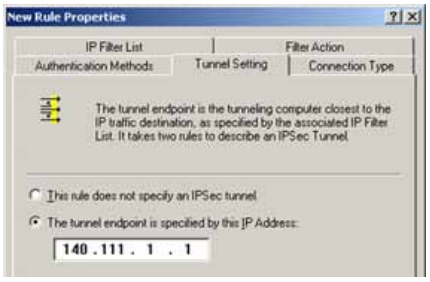


Figure C-16: Tunnel Setting Tab

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

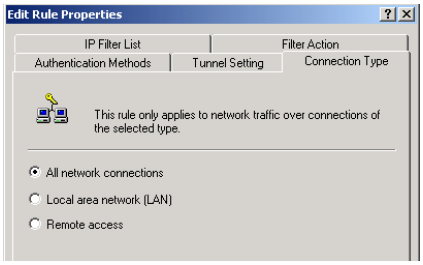


Figure C-17: Connection Type Tab

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.

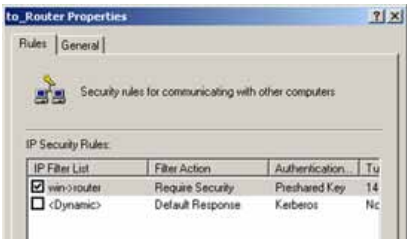


Figure C-18: Properties Screen

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

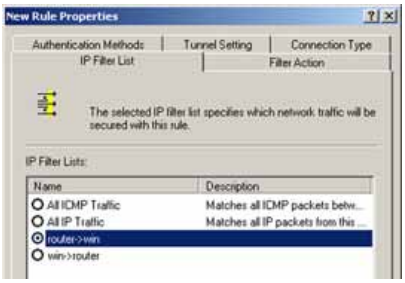


Figure C-19: IP Filter List Tab

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.

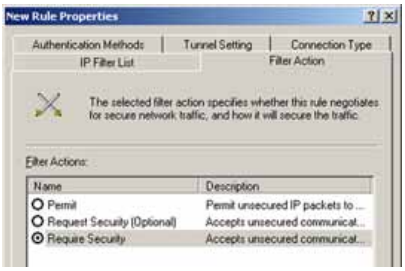


Figure C-20: Filter Action Tab

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

Figure C-21: Authentication Methods Tab

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

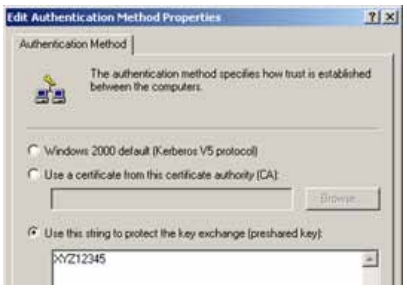


Figure C-22: Preshared Key

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.

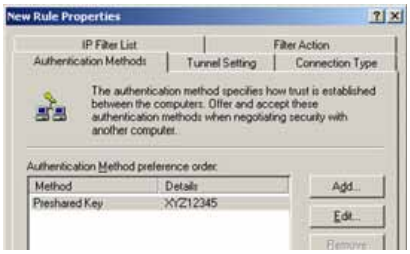


Figure C-23: New Preshared Key

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.

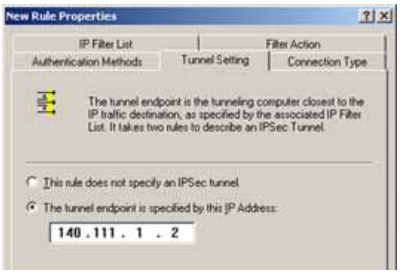


Figure C-24: Tunnel Setting Tab

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

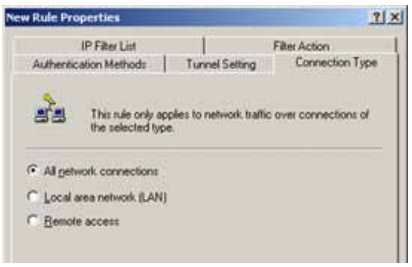


Figure C-25: Connection Type

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

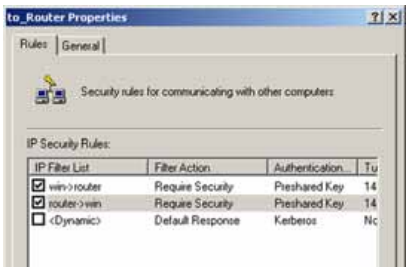


Figure C-26: Rules

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.

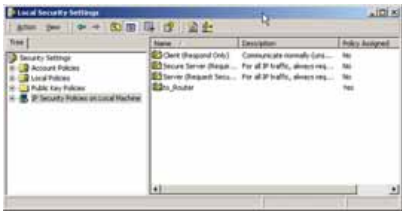


Figure C-27: Local Computer

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

1. Open your web browser, and enter **192.168.1.1** in the *Address* field. Press the **Enter** key.
2. When the *User name* and *Password* 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 types of authentication: **MD5** and **SHA1** (SHA1 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.
8. Select the Key Management. Select **Auto (IKE)** and enter a series of numbers or letters in the *Pre-shared Key* field. Select **PFS** (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. You may use any combination of up to 128 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.
9. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

Figure C-28: VPN Tab

Appendix D: Configuring a Gateway-to-Gateway IPSec Tunnel

Overview

This appendix explains how to configure an IPSec VPN tunnel between two VPN Routers by example. Two PCs are used to test the liveliness of the tunnel.

Figure D-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)
- Two VPN Routers that are both connected to the Internet

Configuring the VPN Settings for the VPN Routers

NOTE: Each computer must have a network adapter installed.

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. Click the **VPN** tab.
5. Click the **IPSec VPN** tab.
6. For the VPN Tunnel setting, select **Enabled**.
7. Enter a name in the *Tunnel Name* field.
8. For the Local Secure Group, select **Subnet**. Enter VPN Router 1's local network settings in the *IP Address* and *Mask* fields.
9. For the Remote Secure Group, select **Subnet**. Enter VPN Router 2's local network settings in the *IP Address* and *Mask* fields. Note that the subnet of Router 2 must be different than the subnet of Router 1.
10. For the Remote Secure Gateway, select **IP Addr**. Enter VPN Router 2's WAN IP address in the *IP Address* field.
11. Click the **Save Settings** button.

Figure D-2: Login Screen

Figure D-3: 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. If the LAN IP address is still the default one, change it to 172.168.1.1 and save the setting.
5. Click the **VPN** tab.
6. Click the **IPSec 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 D-4: Security - VPN Screen (VPN Tunnel)

Configuring the Key Management Settings

Configuring VPN Router 1

Following these instructions for VPN Router 1.

1. On the *IPSec VPN* screen, select **3DES** from the *Encryption* drop-down menu.
2. Select **MD5** from the *Authentication* drop-down menu.
3. Keep the default Key Exchange Method, **Auto(IKE)**.
4. Select **Pre-Shared Key**, and enter a string for this key., e.g. 13572468.
5. For the PFS setting, select **Enabled**.
6. If you need more detailed settings, click the **Advanced Settings** button. Otherwise, click the **Save Settings** button and proceed to the next section, "Configuring VPN Router 2."
7. On the *Auto (IKE) Advanced Settings* screen, keep the default Operation Mode, **Main**.
8. For Phase 1, select 3**DES** from the *Encryption* drop-down menu.
9. Select **MD5** from the *Authentication* drop-down menu.
10. Select **1024-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, **28800**.
14. Click the **Save Settings** button on the *Auto (IKE) Advanced Settings* screen.
15. Click the **Save Settings** button on the *IPSec VPN* screen.

Figure D-5: Auto (IKE) Advanced Settings 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.

Appendix E: 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 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. See Figure C-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure C-2). This is the MAC address for your Ethernet adapter and is shown as a series of numbers and letters.

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

   The example in Figure C-2 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.

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

Figure E-1: IP Configuration Screen

Figure E-2: MAC Address/Adapter Address

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

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

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

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

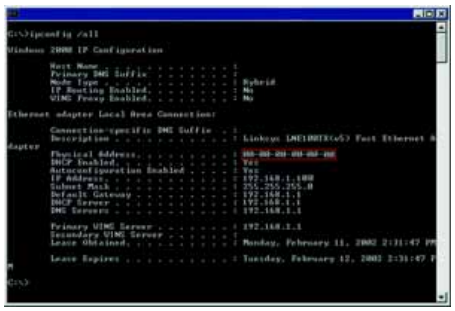


Figure E-3: MAC Address/Physical Address

For the Router's Web-based Utility

For MAC address cloning, enter the MAC Address in the MAC Address field or select **Clone My PCs MAC**. See Figure C-4.

Click **Save Settings** to save the MAC Cloning settings or click the **Cancel Changes** button to undo your changes.

Figure E-4: MAC Address Clone

Appendix F: Physical Setup of the Router

This section describes the physical setup of the Router, including the installation of the mounting brackets.

Setting up the Router

You can set the Router on a desktop or mount it on the wall.

Placement of the Router

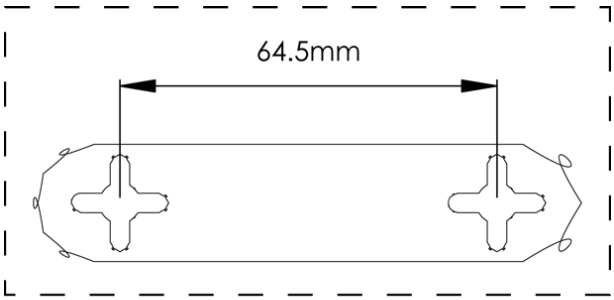
Set the Router on a desktop or other flat, secure surface. Do not place excessive weight on top of the Router.

Wall-Mount Option

You will need 2 suitable screws (See Figure F-1) to mount the Router.

1. Determine where you want to mount the Router. Ensure that the wall you use is smooth, flat, dry and sturdy and make sure the location is within reach of the power outlet.
2. Drill two holes into the wall. Make sure the holes are 64.5mm apart.
3. Insert a screw into each hole, and leave 3 mm of its head exposed.
4. Maneuver the Router so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots. Congratulations! The Wall-Mount installation of the Router is complete.

Figure F-1: Suggested Mounting Hardware



Print this page at 100% size, cut along the dotted line and place on the wall to drill precise spacing.

Figure F-2: Wall-Mounting Template

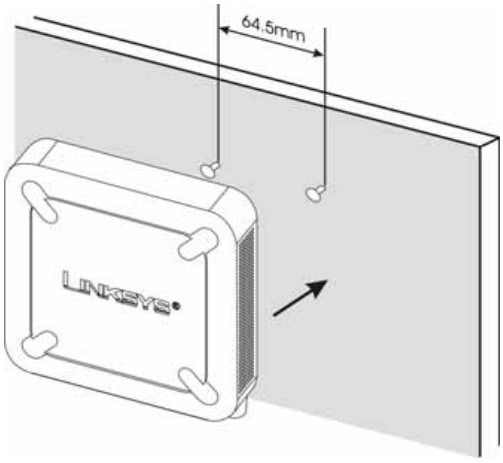


Figure F-3: Wall-Mounting the Router

Appendix G: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

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

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

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

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

EAP (**E**xtensible **A**uthentication **P**rotocol) - 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 (**F**ile **T**ransfer **P**rotocol) - 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 (**H**yper**T**ext **T**ransport **P**rotocol) - 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 (**I**nternet **P**rotocol) - A protocol used to send data over a network.

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

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

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

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

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

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

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

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

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

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

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

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

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

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

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

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**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 (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

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

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

SSID (**S**ervice **S**et **ID**entifier) - 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 (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

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

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

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

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

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - 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 (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

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

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

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix I: Specifications

Model	RVS4000
Standards	IEEE802.3, 802.3u, 802.1x, RFC791 (IP Protocol)
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, Diag, IPS (Blinks RED - Internal attack, Blinks Green - external attack), LAN 1-4, Internet
Operating System	Linux
Performance	
NAT Throughput	800 Mb/s
Setup/Config	
WebUI	Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
Management	
SNMP Version	SNMP Version 1, 2c
Event Logging	Event Logging: Local, Syslog, E-mail Alerts
Web F/W upgrade	Firmware Upgradable Through Web-Browser
Diagnostics	DIAG LED for Flash and RAM failure; Ping Test for network diagnostics

Security

Access Control	Access Control List (ACL) Capability: MAC-based, IP-based
Firewall	SPI stateful packet inspection firewall
Content Filtering	URL blocking, keyword blocking
IPS (Intrusion Prevention System)	IP Sweep Detection, Application Anomaly Detection (HTTP, FTP, Telnet, RCP), P2P Control, Instant Messenger Control, L3-L4 Protocol (IP, TCP, UDP, ICMP) Normalization, L7 Signature Matching
Signature Update	Manual download from the web (Free download for 1 year)
Secure Management	HTTPS, Username/Password
802.1x	Port-based Radius Authentication (EAP-MD5, EAP-PEAP)

QoS

Prioritization types	Port-based and Application-based Priority
Queues	4 queues

Network

VLAN Support	Port-based VLAN
DHCP	DHCP Server, DHCP Client, DHCP Relay Agent
DNS	DNS Relay, Dynamic DNS (DynDNS, TZO)
NAT	PAT, NAPT, ALG support, NAT Traversal
DMZ	Software configurable on any LAN port

VPN	5 QuickVPN Tunnels for remote client access 5 IPSec Gateway-to-Gateway Tunnels for branch office connectivity 3DES Encryption MD5/SHA1 Authentication IPSec NAT-T VPN Passthrough of PPTP, L2TP, IPSec
Routing	Static and RIP v1,v2

Environmental

Device Dimensions (W x H x D)	6.69 x 1.61 x 6.69 inches 170 x 41 x 170 mm
Weight	0.84 lbs (0.38kg)
Power	12V 1A
Certification	FCC class B, CE, ICES-003
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix J: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix K: Regulatory Information

FCC Statement

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

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

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 Industry Canada ICES-003 rule.
Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

IC Statement

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

Règlement d'Industry Canada

Le fonctionnement est soumis aux conditions suivantes :
1. Ce périphérique ne doit pas causer d'interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

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 Haushaltmüll 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 tootel 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.

Ξλληνικά/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 κοινοτικά 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/EC 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 nešķirotā 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 mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša 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 perdirbant 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 Klijenti 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 muniċipali li ma ġiex 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 ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin 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-ħanut 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, amelyeken, 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 gyűjtőredszereken 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 Państwu 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 dos 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 domácností. Je vašou povinnosťou 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 gospodinjskih 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, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

Appendix L: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-823-3002
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000