LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 802.11g Wireless-G

WIRELESS

VPN Router with RangeBooster

User Guide

Model No. **WRV210**

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 User Guide:

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

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

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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

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

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

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

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

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

But what does all of this mean?

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

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

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

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

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

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

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

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

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

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

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

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

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

What's in this Guide?

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

- Chapter 1: Introduction
  This chapter describes the Wireless-G VPN Router applications and this User Guide.

- Chapter 2: Planning Your Wireless Network
  This chapter describes the basics of wireless networking.

- Chapter 3: Planning Your Virtual Private Network (VPN)
  This chapter describes a VPN and its various applications.

- Chapter 4: Getting to Know the Wireless-G VPN Router
  This chapter describes the physical features of the Router.

- Chapter 5: Connecting the Wireless-G VPN Router
  This chapter instructs you on how to connect the Router to your network.

- Chapter 6: Configuring the Wireless-G VPN Router
  This chapter explains how to use the Web-Based Utility to configure the settings on the Router.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G VPN Router with RangeBooster.

- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.

- Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP
  This appendix instructs you on how to use the Linksys QuickVPN software if you are using a Windows 2000 or XP PC.

- Appendix D: Configuring IPSec between a Windows 2000 or XP PC and the Router
  This appendix instructs you on how to establish a secure IPSec tunnel using preshared keys to join a private network inside the VPN Router and a Windows 2000 or XP PC.

- Appendix E: Configuring VPN Tunnels
  This appendix describes how to configure VPN IPSec tunnels using the VPN Routers and a VPN client.

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

- Appendix G: SNMP Functions
  This appendix explains SNMP (Simple Network Management Protocol).

- Appendix H: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on your Router should you need to do so.

- Appendix I: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

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

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

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

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

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

Chapter 2: Planning Your Wireless Network

Network Topology

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

Ad-Hoc versus Infrastructure Mode

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

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

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

Network Layout

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

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

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

***ssid**: your wireless network's name*

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

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

***adapter**: a device that adds network functionality to your PC*

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

***access point**: a device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network*

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

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

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

Figure 2-1: Network Diagram

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 software.

The VPN Router creates a "tunnel" or channel between two endpoints, so that data transmissions between them are secure. A computer with the Linksys VPN client software can be one of the two endpoints (refer to "Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP"). If you choose not to run the VPN client software, any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Router to create a VPN tunnel using IPSec (refer to "Appendix D: Configuring IPSec between a Windows 2000 or XP PC

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

VPN Router to VPN Router

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

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

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

For additional information and instructions about creating your own VPN, please visit Linksys's website at www.linksys.com. You can also refer to "Appendix C: Using the Linksys QuickVPN Software for Windows 2000 or XP", "Appendix D: Configuring IPSec between a Windows 2000 or XP PC and the Router," and "Appendix E: Configuring VPN Tunnels."

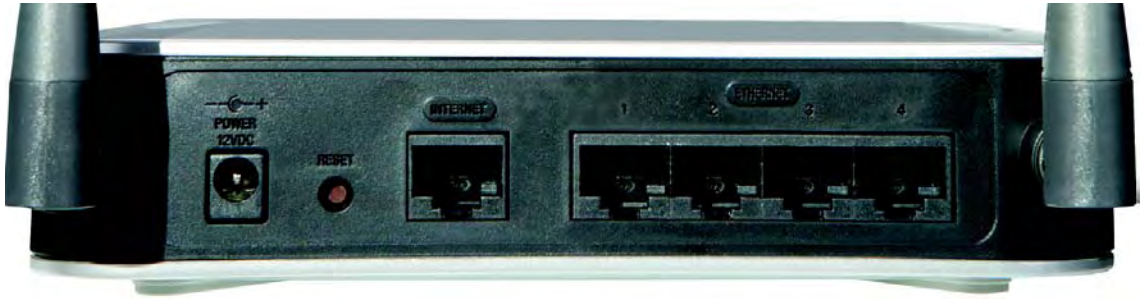
Figure 3-1: VPN Router to VPN Router

Figure 3-2: Computer to VPN Router

Chapter 4: Getting to Know the Wireless-G VPN Router

The Back Panel

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



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

Figure 4-1: Back Panel

Reset Button There are two ways to reset the Router's factory defaults. Either press the **Reset Button**, for approximately five seconds, or restore the defaults from the Administration tab - Factory Defaults in the Router's Web-based Utility.

Ethernet (1-4) The **Ethernet** ports connect to your PCs and other network devices.

Internet The **Internet** port connects to your cable or DSL modem.

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

The Front Panel

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

Figure 4-2: Front Panel

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

DMZ Red. The **DMZ** LED lights up when the Router has an available DMZ port. If the LED is flashing, the Router is sending or receiving data over the DMZ port.

Internet Green. The **Internet** LED lights up when the Router is connected to your cable or DSL modem. If the LED is flashing, the Router is sending or receiving data over the Internet port.

Wireless Green. The **Wireless-G** LED lights whenever there is a successful wireless connection. If the LED is flashing, the Router is actively sending or receiving data over the wireless network.

Ethernet (1-4) Green. The **LAN** LED serves two purposes. If the LED is solidly lit, the Router is connected to a device through the corresponding port (LAN 1, 2, or 3). If the LED is flashing, the Router is sending or receiving data over that port.

Chapter 5: Connecting the Wireless-G VPN Router

Overview

To begin installation of the Router, you will connect the Router to your PCs, other network devices, and cable or DSL modem. If you want to use a PC with an Ethernet adapter to configure the Router, go to "Wired Connection to a PC." If you want to use a PC with a wireless adapter to configure the Router, go to "Wireless Connection to a PC."

Wired Connection to a PC

1. Make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
2. Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router. Then connect the other end to an Ethernet port on a PC.
3. Repeat step 2 to connect additional PCs or other network devices to the Router.
4. Connect a different Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel.
5. Power on the cable or DSL modem.

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

6. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet.
   The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, and then it will be solidly lit when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."
7. Power on one of your PCs that is connected to the Router.

The Router's hardware installation is now complete.

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

Figure 5-1: Connect to LAN Ports

Figure 5-2: Connect to Internet Port

Figure 5-3: Connect to Power Port

Wireless Connection to a PC

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

1. Make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
2. Connect an Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel.
3. Power on the cable or DSL modem.
4. Connect the power adapter to the Router's Power port, and then plug the power adapter into a power outlet.

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

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

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

The Router's hardware installation is now complete.

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

Figure 5-4: Connect to Internet Port

Figure 5-5: Connect to Power Port

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

Chapter 6: Configuring the Wireless-G VPN Router

Overview

Linksys recommends using the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then follow the steps in this chapter and use the Router's Web-based Utility to configure the Router. For advanced users, you may configure the Router's advanced settings through the Web-based Utility.

This chapter will describe each web page in the Utility and each page's key functions. The Utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users only have to use the following screens of the Utility:

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

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

There are seven main tabs: Setup, Wireless, Firewall, VPN, QoS, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

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

HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix I: Windows Help" for more information on TCP/IP.

NOTE: For added security, you should change the password through the Administration screen of the Web-based Utility.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.
- VLAN. The Router provides a port-based VLAN feature.
- DDNS. On this screen, enable the Router's Dynamic Domain Name System (DDNS) feature.
- MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen.
- Advanced Routing. On this screen, configure the dynamic and static routing configuration.

Wireless

- Basic Wireless Settings. You can choose your wireless network settings on this screen.
- Wireless Security. You can choose your wireless security settings on this screen.

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

- Wireless Network Access. This screen displays your network access list.
- Advanced Wireless Settings. For advanced users, you can alter data transmission settings on this screen.
- WDS. This tab is used for Wireless Distribution System (WDS).

Firewall

- General. On this screen, you can configure a variety of filters to enhance the security of your network.
- Port Forwarding. To set up public services or other specialized Internet applications on your network, click this tab.
- Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- DMZ. Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services.
- Access Restriction. This tab allows you to block or allow specific kinds of Internet usage and traffic during specific days and times.
- URL Filtering. This tab allows you to create an URL Filtering policy.

VPN

- VPN Client Access. Use this screen to designate VPN clients and their passwords.
- VPN Passthrough. This tab is used to allow VPN tunnels to pass through the Router's firewall using IPSec, L2TP, or PPTP protocols.
- 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 Summary. This page summarizes the comprehensive details of IPSec VPN Tunnels.

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.
- Log. If you want to view or save activity logs, click this tab.
- Diagnostics. Use this screen to check the connection between the Router and a PC.
- Factory Defaults. If you want to restore the Router's factory defaults, then use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Router's firmware.
- Reboot. Use this to restart the Router.

Status

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

How to Access the Web-based Utility

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

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

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

The Setup Tab - Basic Setup

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

Figure 6-1: Login Screen

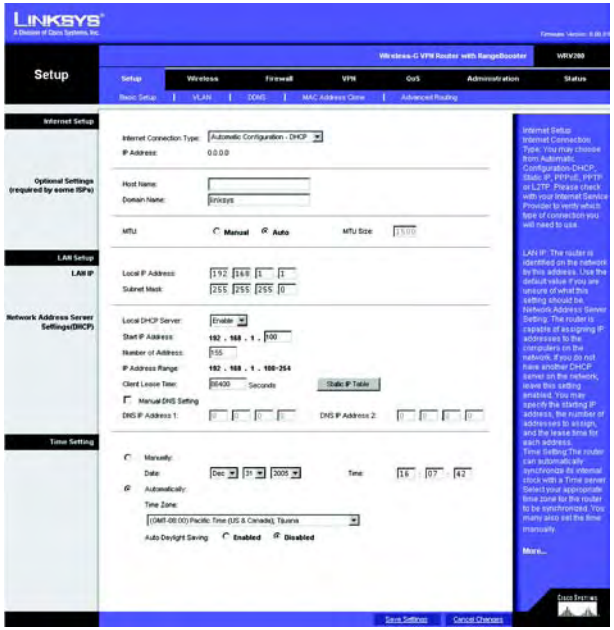


Figure 6-2: Setup Tab - Automatic Configuration - DHCP

Internet Setup

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

Internet Connection Type

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

Automatic Configuration - DHCP

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

Static IP

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

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

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

Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.

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

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

PPPoE

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

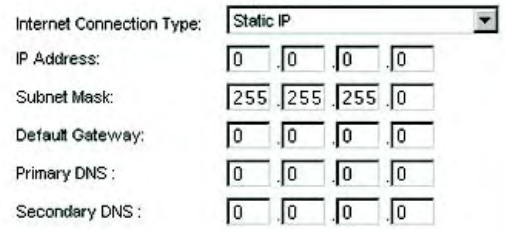


Figure 6-3: Internet Connection Type - Static IP

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

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

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

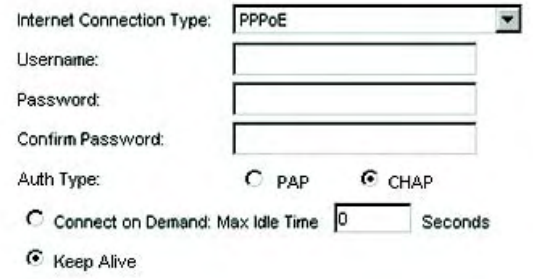


Figure 6-4: Internet Connection Type - PPPoE

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

User Name and Password. Enter the User Name and Password provided by your ISP. Then, enter the Password again to confirm it.

Auth Type: Select from two authentication protocols as required by your ISP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

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

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.

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

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

Auth Type: Select from two authentication protocols as required by your ISP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

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

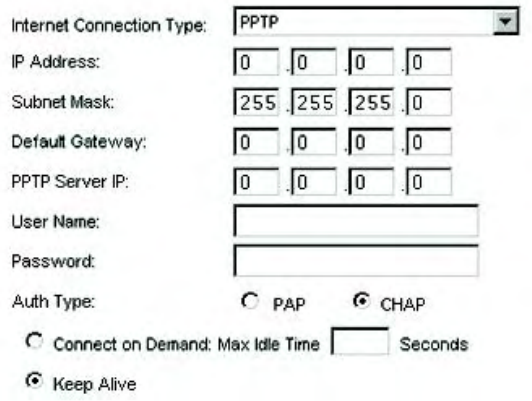


Figure 6-5: Internet Connection Type - PPTP

due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

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

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.

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

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

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

Auth Type: Select from two authentication protocols as required by your ISP: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

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. To use Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter **0** in the *Max Idle Time* field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

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

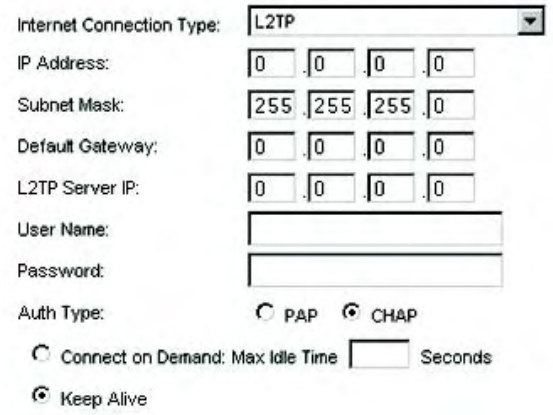


Figure 6-6: Internet Connection Type - L2TP

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.

Optional Settings (Required by some ISPs)

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

Host Name and Domain Name. These fields allow you to supply a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Enabled** and enter the value desired. It is recommended that you leave this value in the 1200 to 1500 range. For most DSL users, it is recommended to use the value 1492. By default, MTU is set at **1500** when disabled.

LAN Setup

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

LAN IP

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**.

Network Address Server Settings (DHCP)

The Router can be used as your network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each PC on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disabled**. If you disable DHCP, assign a static IP address to the Router.

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

Number of Address. Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users.

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

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.

The Static Table shows the mapping of MAC addresses to IP addresses. To use this feature, enter the Static IP Address and MAC address in the fields, then click **Add**. To edit an entry, highlight the entry in the table, click the **Edit** button, make your changes in the fields, then click **Add**. To remove an entry, highlight the entry, then click **Remove**.

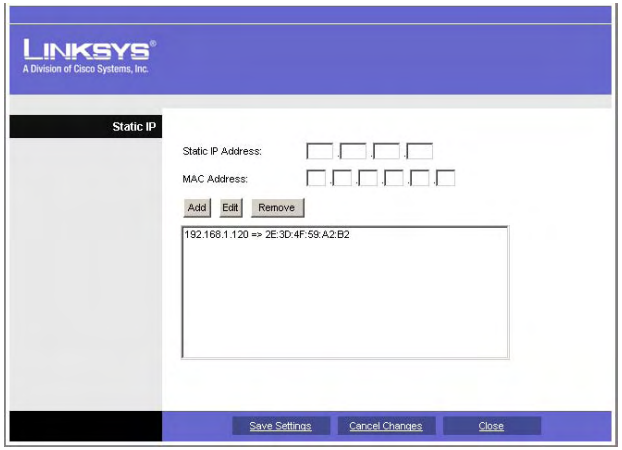


Figure 6-7: Static Table

Manual DNS Setting. To enter the DNS IP addresses manually, enter up to two in the fields provided.

Time Setting

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

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

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

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

The Setup Tab - VLAN

The Router provides a port-based VLAN feature.

Figure 6-8: The Setup Tab - VLAN

Port-based VLAN. Select **Enabled** to enable the feature. When enabled, and a VLAN is selected, VLAN1 will be enabled as a default VLAN, so you will have two VLANs. Select **Disabled** to disable the feature. When this feature is disabled, all LAN ports are on the same LAN.

Number of VLAN. Select the number of the VLAN from the drop-down menu.

VLAN No. Select the VLAN number to associate with the desired port.

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

The Setup Tab - DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router and your ISP does not give you a fixed IP address.

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

DDNS

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

DynDNS.org

User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.

Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, it will change.

Status. The status of the DDNS service connection is displayed here.

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

TZO.com

Email, TZO Password Key, and Domain Name. Enter the Email Address, TZO Password Key, and Domain Name of the service you set up with TZO.

Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.

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

Figure 6-9: The Setup Tab - DDNS - DynDNS.org

Figure 6-10: The Setup Tab - DDNS - TZO.com

Status. The status of the DDNS service connection is displayed here.

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

The Setup Tab - MAC Address Clone

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

MAC Address Clone

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

MAC Clone Address. Enter the MAC Address registered with your ISP. Then click the **Save Settings** button.

Clone My MAC Address. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click the **Clone My MAC Address** button. The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone tab.

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

Figure 6-11: Setup Tab - MAC Address Clone

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

The Setup Tab - Advanced Routing

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

Figure 6-12: The Setup Tab - Advanced Routing

Advanced Routing

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

Dynamic Routing

With Dynamic Routing you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

Dynamic Routing (RIP). To use dynamic routing, click the **Enabled** radio button.

Receive RIP Versions. To use dynamic routing for reception of network data, select the protocol you want: **RIPv1** or **RIPv2**.

Transmit RIP Versions. To use dynamic routing for transmission of network data, select the protocol you want: **RIPv1** or **RIPv2**.

Static Routing

If the Router is connected to more than one network, you can configure static routes to direct packets to the destination network (A static route is a pre-determined pathway that a packet must travel to reach a specific host or network.) To create a static route, change the following settings:

Route Entries. Select the **number** of the static route from the drop-down menu. The Router supports up to 5 static route entries.

Delete This Entry. If you need to delete a route, select its number from the drop-down menu, and click the **Delete This Entry** button.

Enter Router Name. Enter the name of your Router.

LAN IP Address. The LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are

building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router.

Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the Subnet Mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.

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

Interface. Select **LAN & Wireless** or **Internet**, depending on the location of the static route's final destination.

Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how packets are routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to exit this screen.

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

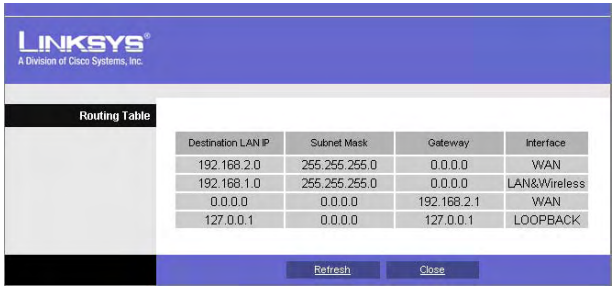


Figure 6-13: Routing Table Entry List

The Wireless Tab - Basic Wireless Settings

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

Wireless Network

Figure 6-14: The Wireless Tab - Basic Wireless Settings

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

Wireless Network Name (SSID). The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (linksys-g) to a unique name.

TX Rate Limitation. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds and the Router will negotiate the connection speed between the Router and a wireless client by this rate.

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

WMM. WMM (Wi-Fi Multimedia) is a component of the IEEE 802.11e wireless LAN standard for quality of service (OoS). It specifically supports priority tagging and queuing. Click the **WMM** check box to enable WMM.

Wireless Channel. Select the appropriate channel from the drop-down menu. All devices in your wireless network must transmit using the same channel in order to function correctly. You may need to change the wireless channel to improve the communication quality.

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

The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are eight wireless security mode options supported by the Router: WPA-Personal, WPA2-Personal, WPA Enterprise, WPA2 Enterprise, WPA2-Personal-Mixed, WPA2-Enterprise Mixed, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) Select the appropriate security mode for your network; all devices on your network must use the same security mode and settings to work correctly. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

Select SSID. Select the SSID that you want to apply the wireless security settings to.

Allow PCs on the same wireless network name (SSID) to see each other. This feature is enabled by default. Wireless PCs that are associated to the same Network Name (SSID), can see and transfer files between each other. By disabling this feature, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location.

WPA-Personal. WPA gives you two encryption methods with dynamic encryption keys. Select **TKIP** or **AES** from the *Enryption* drop-down menu. Enter a Shared Secret (Pre-Shared Key) of 8-32 characters. Then enter the Key Renewal, which instructs the Router how often it should change the encryption keys.

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

Figure 6-15: Wireless Security - WPA-Personal

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

WPA2-Personal. WPA2 gives you the encryption method AES. Enter a Shared Secret of 8-32 characters. Then enter the Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys.

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

Figure 6-16: Wireless Security - WPA2-Personal

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

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

Figure 6-17: Wireless Security - WPA Enterprise

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

WPA2 Enterprise. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Enter the RADIUS server's IP address. Enter the RADIUS server's port number, along with the Shared Secret key, which is the key shared between the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

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

Figure 6-18: Wireless Security - WPA2 Enterprise

WPA2 Personal Mixed. WPA2 Personal Mixed gives you either WPA-Personal (TKIP) or PSK2 (AES) encryption. Enter a Shared Secret of 8-63 characters. Then enter a Key Renewal period, which instructs the Router how often it should change the encryption keys.

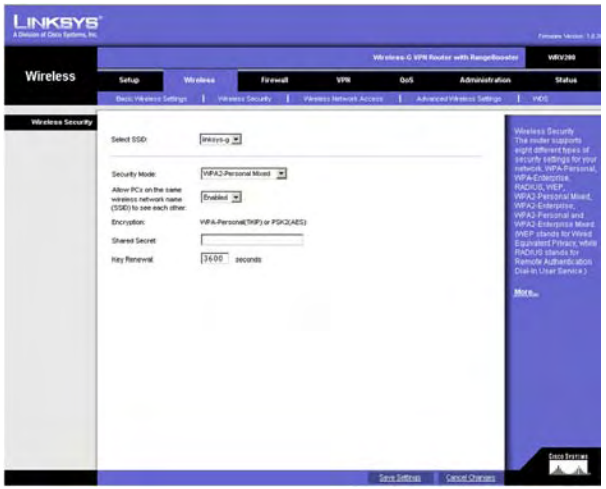


Figure 6-19: Wireless Security - WPA2 Personal Mixed

WPA2 Enterprise Mixed. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Enter the RADIUS server's IP address and port number, along with the shared secret (authentication key) shared by the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

Figure 6-20: Wireless Security - WPA2 Enterprise Mixed

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

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

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

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

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

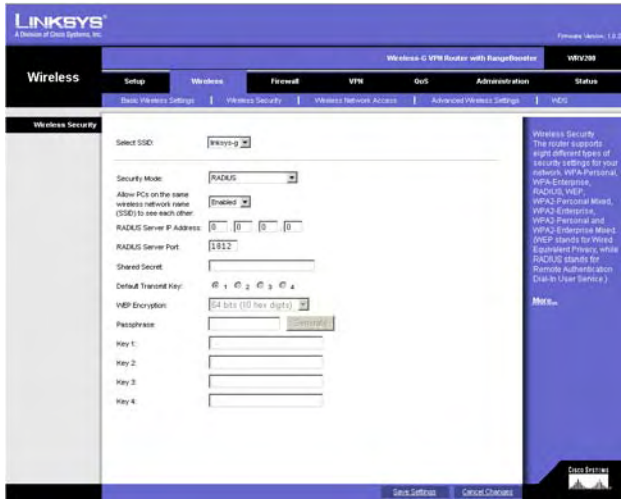


Figure 6-21: Wireless Security - RADIUS

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

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

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

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

Figure 6-22: Wireless Security - WEP

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

The Wireless Tab - Wireless Network Access

This screen allows you to control access to your wireless network for each SSID.

Wireless Network Access

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

MAC 1-16. Enter the MAC addresses of the designated computers. For a more convenient way to add MAC addresses, click the **Select MAC Address From Networked Computers** button. The *Networked Computers* screen will appear. Select the MAC Addresses you want. Then click the **Select** button. Click the **Refresh** button if you want to refresh the screen. Click the **Close** button to return to the previous screen.

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

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

Figure 6-23: Wireless Tab - Wireless Network Access

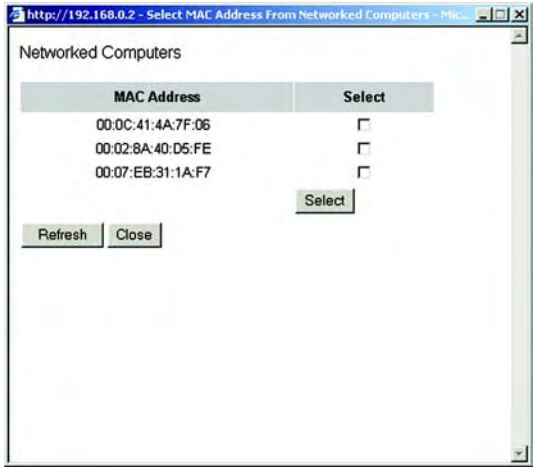


Figure 6-24: Networked Computers

The Wireless Tab - Advanced Wireless Settings

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

Advanced Wireless Settings

Figure 6-25: The Wireless Tab - Advanced Wireless Settings

AP Isolation. This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, click **Enabled**. AP Isolation is disabled by default.

Basic Rate. The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default setting is Auto.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode's default setting is **Auto**. The Router will automatically use CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance.

Beacon Interval. The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

DTIM Interval. The default value is **3**.This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

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

dtim *(delivery traffic indication message): A message included in data packets that can increase wireless efficiency*

Fragmentation Threshold. In most cases, this value should remain at its default value of **2346**. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended.

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

RTS Threshold. The RTS Threshold value should remain at its default value of **2347**. Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

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

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

The Wireless Tab - WDS

This tab is used for Wireless Distribution System (WDS). WDS will ONLY work with the SSID1. Make sure that the channel and security settings are the same for all WDS enabled devices.

WDS allows a wireless signal to be repeated by a repeater. This mode allows a wireless client to connect to the Router through a repeater, such as WAP54G, WAP54GP, WAP54GPE, when operating in the Repeater Mode. This mode allows you to extend the coverage of the Router by using up to three repeaters. Select **Auto** to enable the remote access point when operating in Repeater Mode or select Manual and enter the MAC address of the repeater.

Click the **Site Survey** button to view the available access points.

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

Figure 6-26: Wireless Tab - WDS

The Firewall Tab - General

When you click the Security tab, you will see the *General* screen. The Router's firewall enhances the security of your network. You can implement a Stateful Packet Inspection (SPI) firewall, block anonymous Internet requests, and enable block mechanisms.

Figure 6-27: The Firewall Tab - General

General

DoS Prevention. Denial of Service (DoS) Prevention checks incoming packets before allowing them to enter your network. To use this feature, select **Enabled** from the drop-down menu. If you do not want DoS Prevention, select **Disabled**.

Internet Block

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

Block Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enabled** to filter multicasting, or **Disabled** to disable this feature.

Web Block

Proxy. Use of WAN proxy servers may compromise the Router's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.

Java. Java is a programming language for websites. If you deny Java applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java applet filtering, click **Enabled**.

ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click **Enabled**.

Cookies. A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.

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

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

The Firewall Tab - Port Forwarding

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

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

Figure 6-28: The Firewall Tab - Port Forwarding

Port Forwarding

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

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

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

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

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

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

The Firewall Tab - Port Triggering

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

Figure 6-29: The Firewall Tab - Port Triggering

Port Triggering

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

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

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

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

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

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

The Firewall Tab - 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 through Software DMZ. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.

Software DMZ. This feature allows one local 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 Software DMZ feature, select **Disabled**.

DMZ Host IP Address. To expose one PC, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix F: Finding the MAC Address and IP Address for Your Ethernet Adapter."

Figure 6-30: The Firewall Tab - DMZ

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

The Firewall Tab - Access Restriction

The *Access Restriction* screen allows you to block or allow specific kinds of Internet usage and traffic during specific days and times.

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

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

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

Figure 6-31: The Firewall Tab - Access Restriction

To create an Internet Access Policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.
4. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PC with the given IP address.
5. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
6. You can block access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. (You can block up to 20 services.)
7. Then enter the range of ports you want to filter.

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

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

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

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

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

The Firewall Tab - URL Filtering

To create an URL Filtering policy:

1. Select a number from the URL Filtering Policy drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select Enabled from the Status menu.
4. Enter the Start IP Address and End IP Address what will be affected by the policy. After making your changes, click the Save Settings button to apply your changes.
5. The address entered to access Internet site, by entering the address in the URL String field.
6. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

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

Figure 6-32: The Firewall Tab - URL Filtering

The VPN Tab

Virtual Private Networking (VPN) is a security measure that creates a secure connection between two remote locations. The security is created by the very specific settings for the connection. The VPN Tab allows you to configure your VPN settings to make your network more secure.

The VPN Tab - VPN Client Access

The Router offers a QuickVPN Client utility for Windows 2000 or XP. If the Router has clients using this utility, then you can designate the QuickVPN clients and their passwords on this screen.

VPN Client Access

User Name. Enter a name for the VPN client.

Password. Enter a password for the VPN client.

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

Allow user to change password? If you want to let the user change his or her password from the user's QuickVPN client, select **Yes**.

When you have finished entering the user name and password of the VPN client, click the **Add/Save** button to add the VPN client to your list. A warning message will appear the first time you add a VPN client. After all VPN clients are added to the VPN Client List Table, click **Save Settings**.

VPN Client List Table

No. This is the number assigned to this VPN client. The Router supports up to 10 QuickVPN clients.

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

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

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

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

Figure 6-33: The VPN Tab - VPN Client Access

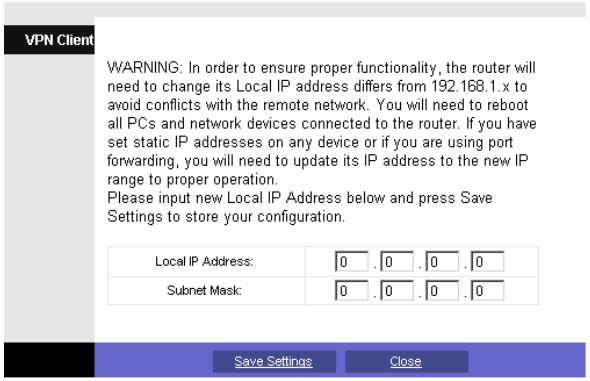


Figure 6-34: The VPN Tab - VPN Client Access Warning

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

The VPN Tab - VPN Passthrough

This tab is used to allow VPN tunnels to pass through the Router's firewall using IPSec, L2TP, or PPTP protocols.

Figure 6-35: The VPN Tab - VPN Passthrough

VPN PassThrough

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

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

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

The VPN Tab - 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.

Tunnel Entry. To establish this tunnel, select the tunnel you wish to create from the drop-down box. It is possible to create up to 5 gateway-to-gateway tunnels.

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

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

NAT-Traversal. You can select this option to enable NAT-Traversal to make IPSec tunnels with remote peers. NAT-Traversal is developed for the IPSec peer behind the NAT device to avoid error identification of IKE phase and ESP packet fallacious authentication which are caused by NAT IP translation. It will help to establish IPSec tunnels and encapsulate the ESP packet into UDP packet. While the IP address and port number of such UDP packet being modified by NAT, the encapsulated ESP can still be integrity for remote IPSec peer verification. Because we do not know where the NAT server of the remote peer is located exactly, the Remote Secure Group and Remote Secure Gateway must be set to Any when NAT-Traversal is enabled.

Select **Enabled** to enable NAT-Traversal support for this tunnel, and **Disabled** to disable it.

Figure 6-36: The VPN Tab - IPSec VPN

Local Secure Group

The Local Secure Group is the computer(s) on your LAN that can access the tunnel. From the drop-down menu, select **Subnet**, to include the entire network for the tunnel; select **IP Address** if you want a specific computer; **IP Range**, if you want to include a range of IP addresses; or select **Host**, which is used with Port Forwarding to direct the traffic to the correct computer. The screen will change depending on the selected option. The options are described below.

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

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

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

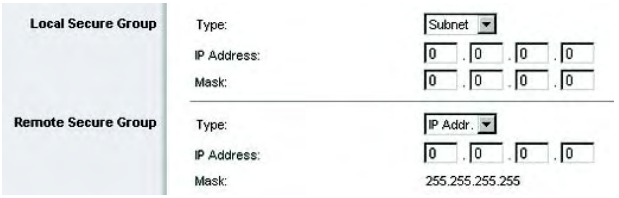


Figure 6-37: Local Secure Group - Subnet and Remote Secure Group - IP Addr.

Remote Secure Group

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

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

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

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

Any. Allows any computer to access the tunnel.

Remote Secure Gateway

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

If the IP Address is static, select **IP Addr.** and enter the IP address. Make sure that you have entered the IP address correctly, or the connection cannot be made. Remember, this is NOT the IP address of the local VPN Router; it is the IP address of the remote VPN router or device with which you wish to communicate. If the IP address is dynamic, select **FQDN** for DDNS or **Any**. If FQDN is selected, enter the domain name of the remote router, so the Router can locate a current IP address using DDNS. If Any is selected, then the Router will accept requests from any IP address.

Key Management

Key Exchange Method. IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Pre-shared Key to authenticate the remote IDE peer. Select **Auto (IKE)** for the Key Exchange Method. Both ends of a VPN tunnel must use the same mode of key management. The settings available on this screen may change, depending on the selection you have made.

Encryption. Using encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but

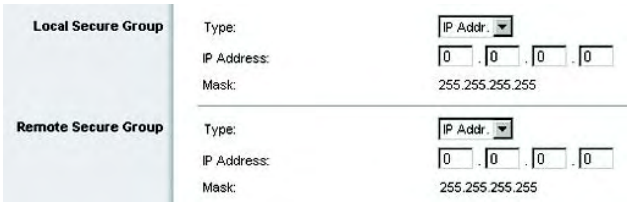


Figure 6-38: Local Secure Group - IP Address and Remote Secure Group - IP Address

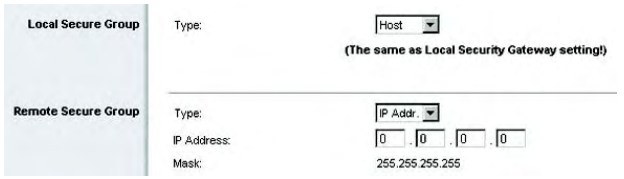


Figure 6-39: Local Secure Group - Host and Remote Secure Group - IP Addr.

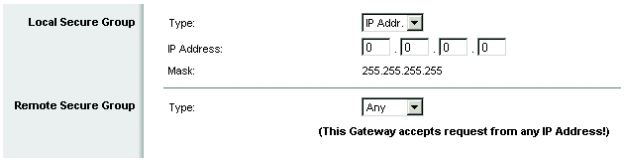


Figure 6-40: Local Secure Group - IP Addr. and Remote Secure Group - Any

it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose to disable this feature.

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

Pre-shared Key. You can choose to use a Pre-shared Key or RSA Signature. To use the Pre-shared Key, click its radio button. enter a series of numbers or letters in the *Pre-shared Key* field. Based on this word, which MUST be entered at both ends of the tunnel, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed.

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

ISAKMP Key Lifetime(s).The Field specifies how long an ISAKMP key channel should been kept, before being renegotiated.

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

Key Lifetime. You may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.

Advanced Settings Button. Advanced Settings provide the administrator more detailed options to control the whole IPSec tunnel construction procedure. Advanced Settings devides the original IPSec tunnel construction procedure into 2 phases, Phase 1 is for ISAKMP SA establishment, and Phase 2 is for, after ISAKMP SA established, IPSec Data Connection Encryption and Authentication Method.

Phase1

Tunnel Entry. The configurating tunnel.

Operation Mode. We support Main Mode operation in ISAKMP SA establishment.

Encryption Method. You can select **3 ISAKMP** encryption method including 3DES to indicate 3DES encryption with a key length of 192 bits, AES to indicate AES encryption with key length 256 bits.

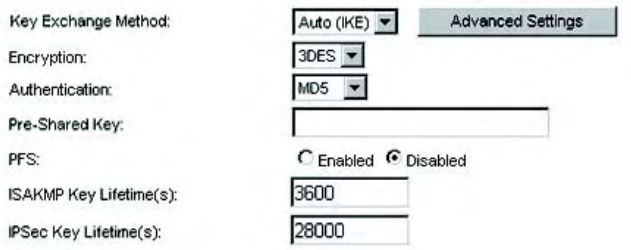


Figure 6-41: Key Exchange Method - Auto(IKE)

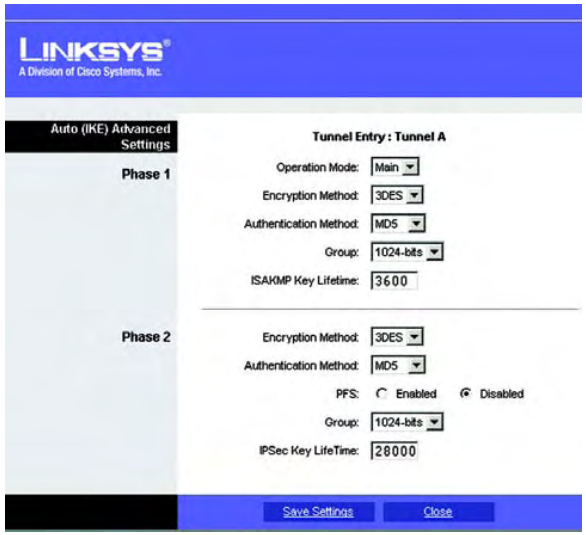


Figure 6-42: Advanced Settings

Authentication Method. You can select **MD5** or **SHA1** authentication method to generate IPSec Authentication Header (AH) during ISAKMP.

Group. This is for Diffie-Hellman key negotiation. There are 7 groups available for ISAKMP SA establishment. Group 1024, 1536, 2048, 3072, 4096, 6144, and 8192 represent different bits used in Diffie-Hellman mode operation. The default value is 1024.

ISAKMP Key Lifetime(s).The field specifies how long an ISAKMP key channel should been kept before being renegotiated.

Phase 2:

Encryption Method. You can select 3 IPSec data connection encryption method including 3DES to indicate 3DES encryption with key length 192 bits, AES to indicate AES encryption with key length 256 bits.

Authentication Method. You can select **MD5** or **SHA1** authentication method to generate IPSec Authentication Header (AH) of IPSec data connection.

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

Group. The value is the same as Phase 1 Group

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

Tunnel Options

Dead Peer Detection. You can select **Dead Peer Detection** (DPD) to detect the status of a remote Peer. DPD will issue DPD packets (ISAKMP format) to query aremote peer, and wait for a reply to recognize that it is still alive. There are 3 auxiliary options: Detection Delay(s), Detection Timeout(s), and DPD Action for DPD.

Detection Delay(s). You can indicate the interval between DPD query packets. The default value is 30 seconds.

Detection Timeout(s). You can indicate the length of timeout when DPD cannot hear any DPD reply. The default value is 120 seconds.

DPD Action. When DPD Timeout expires, the DPD will take DPD Action to deal with the connection. You can select **Wait for Respons**e to still wait for remote peer response, or select **Suspend Connection** to stop passively recovering the connection or select **Auto Recover.**

If IKE failed more than _times, block this unauthorized IP for _ seconds. This feature is enabled by default. It enables the Router to block unauthorized IP addresses. Specify the number of times IKE must fail before the Router blocks that unauthorized IP address.

IPComp Compression. You can click the **IPComp Compression** checkbox to enable IP compression to be done before encryption.

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

Global Options

Global NAT-Traversal. This feature is enabled by default. You can select Global NAT-Traversal to support the remote peers behind NAT workaround for *all* IPSec tunnels. NAT-Traversal is a technology that is developed for the IPSec peer behind NAT to ward off error identification of IKE phase and ESP packet fallacious authentication, such two error situation are caused by regular NAT IP translation. NAT-Traversal will help to establish IPSec Tunnels and encapsulate the original ESP packet with a UDP header and a trailer. Such UDP packet will be regularly translated private/public IP and port number by NAT, but the internal encapsulated ESP packet can keep the original integrity and secrecy for remote IPSec peer verification. You can indicate certain accepted private networks, click **Advanced Setting**.

Select **Enabled** to enable Global NAT-Traversal support, and Disabled will disable it.

Global NAT-Traversal Advanced Settings

Allowable Remote Private Networks. You can select **Allow All** to allow the peer to sit in any private network that is behind a NAT, or **By Manual Setting** to indicate designated private networks manually.

Manual Setting. Enter the IP Address and Mask of what you want to accept that remote peer sat behind NAT. Click the Checkbox and Save Setting to save and enable your new configuration.

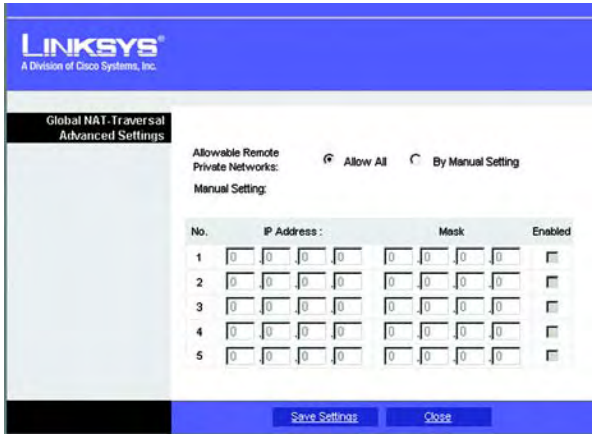


Figure 6-43: Global NAT Traversal Advanced Settings

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

The VPN Tab - VPN Summary

This page summarizes the comprehensive details of IPSec VPN Tunnels that include Tunnel Name, Remote Gateway, Remote Group, Local Group, Key Methods, Tunnel Status, and Start/Stop/Detail Connection. Each field displays information according to a pre-configured value of IPSec tunnel separately, and each IPSec tunnel can be easily commanded to start/stop connection here. VPN Summary can help an administrator to manage and examine all IPSec tunnels status.

Figure 6-44: The VPN Tab - VPN Summary

VPN Summary

Tunnel Name. The field displays the name of the tunnel.

Remote Gateway. The field displays the remote gateway. If the pre-configured type is IP Addr., the field displays the IP address of remote gateway. If the pre-configured type of remote gateway is Any, the field displays ANY. If the pre-configured type is FQDN, the filed displays the FQDN string directly.

Remote Group. The field displays the remote peer that is designated for VPN communication after a IPSec VPN tunnel is established. If the pre-configured type of the remote group is IP Addr., the field displays the IP address of the remote peer. If the pre-configured type of the remote group is Subnet, the field displays the subnet type "IP Address/Mask". If the pre-configured type of remote group is Host or Any, the field displays the "Host" or "Any" directly.

Local Group. The field displays the local peer that is designated for VPN communication after an IPSec VPN tunnel is established. If the pre-configured type of local group is IP Addr., the field displays the IP address of the local peer. If the pre-configured type of local group is Subnet, the field displays the subnet type "IP Address/Mask". If the pre-configured type of local group is Host, the field displays the "Host" directly.

Key Methods. The field displays the IPSec authentication and encryption key methods of the Key exchange Method that is followed with the setting value of the Password Forward Secrecy.

Tunnel Status. The field displays the status of IPSec Tunnel as follows.

C: The Tunnel Connected.

T: Try to Connect to Remote Peer.

Stop: The Tunnel is stopped.

D: The Tunnel Disabled.

Any : The Tunnel always waits for the connection from the remote initiator.

NAT-T : The Tunnel enables the NAT-Traversal to allow the remote initiator that is behind the NAT to construct this IPSec Tunnel.

Start/Stop/Restart Connection. You can manually start/stop IPSec connection according to pre-configured tunnel settings. If the pre-configured type of remote gateway or remote group is either Any or NAT-Traversal, Detail button can also examine Remote Security Gateway information.

Detail. Each Tunnel has a Detail button. This button will become available when a Tunnel Status reveals a "C", "T", "Any", and " NAT-T". When you press the Detail button, a "VPN Advanced Tunnel Information" screen appears. This feature provides more detailed information for advanced configuration and management. VPN Advanced Tunnel Information will show Advanced Tunnel Information and Remote Security Gateway.

VPN Log Button. Use to check the overall related VPN behaviors and contact messages of a VPN Tunnel and VPN Client. Press the button to view the VPN operation situation. If you want to clear this log information, just press the button Clear Log Now.

Click the Refresh button to update the on-screen information.

The QoS Tab - Application-based QoS

Quality of Service (QoS) ensures better service to high-priority service.

Application-based QoS involves Internet traffic, which may involve demanding, real-time applications, such as videoconferencing. To enable Application-based QoS, you can select either **Priority Queue** or **Bandwidth Allocation**.

Priority Queue. Application-based QoS manages information as it is transmitted from LAN to WAN. Depending on the settings of the Priority Queue, this feature will assign infromation a high or low priority for the five preset applications and three additional applications that you specify. For each application, select **High Priority** or **Low Priority**. The packets will be put into High or Low Priority Queue for the egress port of WAN according to your settings. Specific Port #. You can add three additional applications by entering their respective application port numbers in the Specific Port # field.

Bandwidth Allocation. For each of the three Application Level Gateways (ALGs), you can choose a Bandwidth Allocation Policy from Guaranteed and Spare with a specified percentage value to control the bandwidth utilization from LAN to WAN. It depends on specified policy to let the bandwidth to be reserved or shared with the applications. Guaranteed wil reserve specific bandwidth for the applications and Spare will use the remaining bandwidth for other applications.

User Define Button. You can define the policies regarding source or destination IP, protocol and port number. You also can mark the DSCP field with specific value to egress packets. The bandwidth utiliazation could be controlled from LAN to WAN.

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

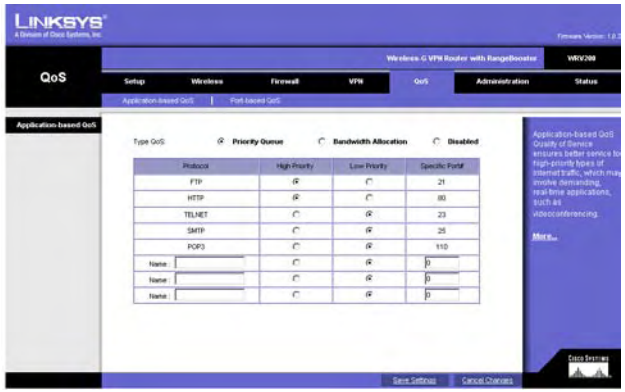


Figure 6-45: The QoS Tab - Application-based QoS - Priority Queue

Figure 6-46: The QoS Tab - Application-based QoS - Bandwidth Allocation

The QoS Tab - Port-based QoS

Port-based QoS ensures better service to a specific LAN port.

Priority. Select the QoS priority for each LAN port. High/Low setting will queue all egress packets from this port according to its priority value. If you select High for the specific port, the packets received from this port would be put into High Priority Queue.

Flow Control. When this feature is enabled, the wired LAN ports will exchange control packets with the connected port before sending packets. If the other end is not able to process more packets, it will send a pause frame and a sending port will hold the packets.

Ingress Rate. This setting lets the user choose the input data rate for a port. Packets exceeding this rate will be dropped. The rates can be 128kbps, 256kbps, 512kbps, 1Mbps, 2Mbps, 4Mbps, 8Mbps, 16Mbps, 32Mbps or no rate control.

Egress Rate. This setting lets the user choose the output data rate for a port. Packets exceeding this rate will be dropped. The rates can be 128kbps, 256kbps, 512kbps, 1Mbps, 2Mbps, 4Mbps, 8Mbps 16Mbps, 32Mbps or no rate control.

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

Figure 6-47: The QoS Tab - Port-based QoS

The Administration Tab - Management

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

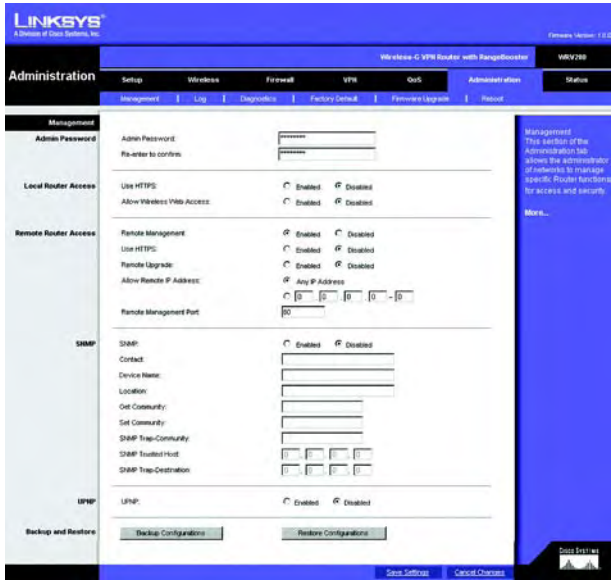


Figure 6-48: The Administration Tab - Management

Admin Password

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

User Name. You should change the default user name to one of your choice.

Router Password. You should change the default password to one of your choice.

Re-enter to confirm. Re-enter the Router's new Password to confirm it.

Local Router Access

This feature allows you to manage your Router from a local location, via the Wireless. To enable this feature, select **Enabled** in *Allow Wireless Web Access* option. To use the SSL encryption, select **Enabled** in *Use HTTPS* option. After HTTPS is enabled, http requests to the Router's LAN IP will be redirected to HTTPS.

Remote Router Access

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

Remote Management. This feature allows you to manage the Router from a remote location, via the Internet. To enable Remote Management, click the **Enabled** radio button.

Use HTTPS. To use the SSL encryption, select Enabled.

Remote Upgrade. If you want to be able to upgrade the Router remotely from outside the local network, select **Enabled**. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default setting, **Disabled**.

Allow Remote IP Address. If you want to be able to access the Router from any external IP address, select **Any** IP Address. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

Remote Management Port. Enter the port number that will be open to outside access. Otherwise, keep the default setting, **8080**.

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

SNMP

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

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

Identification

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

Device Name. Enter the name of the Router.

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

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

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

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

SNMP Trusted Host. You can restrict access to the Router's SNMP information by IP address. Enter the IP address in the *SNMP Trusted Host* field. If this field is left blank, then access is permitted from any IP address.

SNMP Trap-Destination. Enter the IP address of the remote host computer that will receive the trap messages.

UPnP

Universal Plug and Play (UPnP) allows Windows XP, Windows 2000, and Windows Me to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, check the **Enabled** box.

Backup and Restore

Backup Configurations. To back up the Routers configuration, click this button and follow the on-screen instructions.

Restore Configurations. To restore the Routers configuration, click this button and follow the on-screen instructions. (You must have previously backed-up the Router's configuration.)

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

The Administration Tab - Log

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

Figure 6-49: The Administration Tab - Log

Log

Email Alert. To enable the Router to send email alerts in the event of Denial of Service attacks and the like, select **Enabled**. If you do not wish to have email alerts, select **Disabled**. The router will send out e-mail logs to a specific e-mail address.

Mail From. Enter the e-mail address so that the receiver can know where the mail is from.

Recipient To. Enter the e-mail address where you want the alerts to be sent.

Event Types. There are ACL, DoS, URL Detect and New Connection event types for E-Mail Alert. You can select some of them to enable those event alerts.

System Log. You may keep a log of the router's activities. This requires the installation of an external log viewer. To enable System Log, click **Enabled**.

Logviewer IP Address. Enter the address where you want the system log to be send.

Event Types. There are System, ACL, DoS, URL Detect and New Connection event types for System Log. You can select some of them to enable those event logs.

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

The Administration Tab - Diagnostics

The Diagnostcs allow you to check the connections of your network components.

Figure 6-50: The Administration Tab - Diagnostics

Ping Test

Ping Test Parameters

IP or URL Address. Enter the IP or URL address of the network device whose connection status you wish to test.

Packet Size. Enter the size of the ping packets.

Times to Ping. Enter the number of times that you want to ping the device: **5**, **10**, **15**. or **Unlimited**.

Click the **Start to Ping** button to start the test. The results of the test will be displayed in the window. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

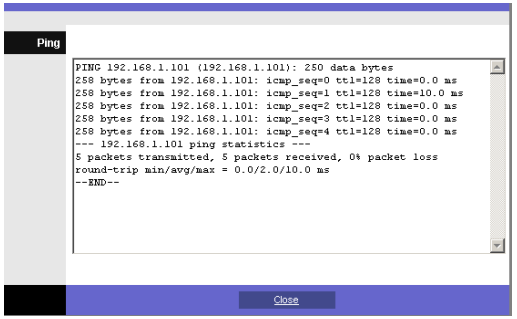


Figure 6-51: Ping Test

Traceroute Test

IP or URL Address. Enter the IP or URL address of the network device whose performance you wish to test.

Click the **Start to Traceroute** button to start the test. The results of the test will be displayed in the window. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

For help information, click **More**.

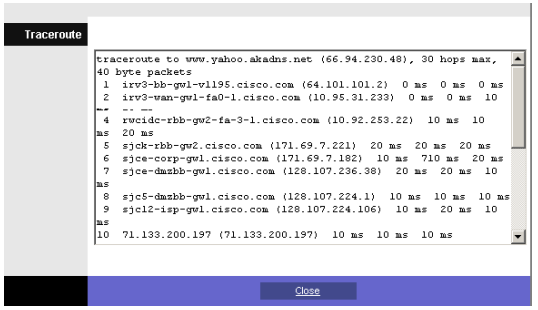


Figure 6-52: Traceroute Test

The Administration Tab - Factory Defaults

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

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

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

Figure 6-53: The Administration Tab - Factory Default

The Administration Tab - Firmware Upgrade

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

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

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

Figure 6-54: The Administration Tab - Firmware Upgrade

Upgrade Firmware

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

For help information, click **More**.

The Administration Tab - Reboot

To restart the Router, select **Yes**, then click the **Save Settings** button.

Figure 6-55: The Administration Tab - Reboot

The Status Tab - Router

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

Figure 6-56: The Status Tab - Router

Information

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

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

Current Time. The current time is displayed here.

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

Host Name. If entered on the Setup Tab, the host name is displayed here.

Domain Name. If entered on the Setup Tab, the domain name is displayed here.

Internet Connection

Configuration Type. This shows the information required by your ISP for connection to the Internet. This information was entered on the Setup Tab.

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

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

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

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

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

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

The Status Tab - Local Network

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

Figure 6-57: The Status Tab - Local Network

Local Network

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

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

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

DHCP Server

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

Start IP. The start of the IP address range used by the device on you local network is displayed here.

End IP. The end of the IP address range used by the device on you local network is displayed here.

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

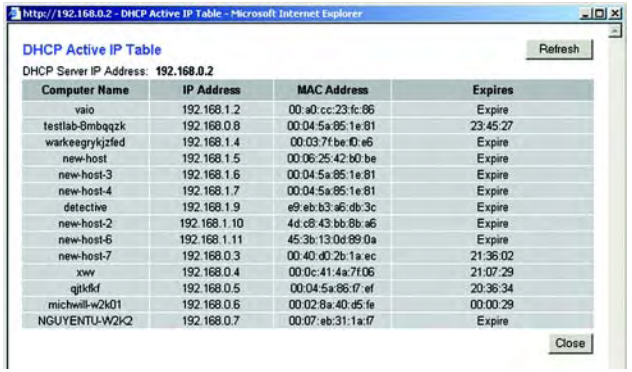


Figure 6-58: DHCP Active IP Table

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

The Status Tab - Wireless

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

Figure 6-59: The Status Tab - Wireless

Wireless

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

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

SSID MAC Address. As entered on the Wireless tab, this will display the MAC Address of the SSID listed in the table and on your network.

Wireless Network Name (SSID). As entered on the Wireless tab, This displays the SSID of your network.

Security Mode. As selected on the Wireless tab, this will display what type of wireless security the Router uses.

WMM. As entered on the Wireless tab, this displays the status of the Router's WMM feature.

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

The Status Tab - System Performance

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

Figure 6-60: The Status Tab - System Performance

System Performance

Internet/Wireless

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

Connection. The status of the connection is shown here.

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

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

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

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

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

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

LAN

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

Connection. The status of the connection is shown here.

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

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

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

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

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

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

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

The Status Tab - VPN Clients

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

VPN Summary

Figure 6-61: The Status Tab - VPN Clients

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

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

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

Status. This is the status of the VPN connection.

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

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

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

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

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

Appendix A: Troubleshooting

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

Common Problems and Solutions

1. ***I'm trying to access the Router's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."***
   If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):
   1. Click **File**. Make sure *Work Offline* is NOT checked.
   2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
   3. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

2. ***I need to set a static IP address on a PC.***
   You can assign a static IP address to a PC by performing the following steps:
   - For Windows 98 and Me:
     1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
     2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
     3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Router. Make sure that each IP address is unique for each PC or network device.
     4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Router. Click the Add button to accept the entry.
     5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
     6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
     7. Restart the computer when asked.

- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
  7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
  9. Restart the computer if asked.
- For Windows XP:

  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
  4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  6. Enter the Subnet Mask, 255.255.255.0.
  7. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
  8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

3. I want to test my Internet connection.

A Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

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

For Windows NT 4.0:

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

B Open a command prompt.

For Windows 98 and Me:

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

For Windows NT, 2000, and XP:

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

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

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

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

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

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

- Refer to "Problem #3, I want to test my Internet connection" to verify that you have connectivity.
  1. If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix F: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of "Chapter 6: Configuring the Wireless-G VPN Router" for details.
  2. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: Configuring the Wireless-G VPN Router" for details on Internet connection settings.
  3. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.

4. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's web-based utility shows a valid IP address from your ISP.
5. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's web-based utility to see if you get an IP address.

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

- Refer to "Problem #3, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
  1. Refer to "Appendix F: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
  2. Set a static IP address on your system; refer to "Problem #2: I need to set a static IP address."
  3. Refer to "Problem #11: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

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

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

- VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab
- of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #8, I need to set up online game hosting or use other Internet applications" for details.
- Check the Linksys website for more information at www.linksys.com.

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

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

- Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.
  1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications and Gaming => Port Forwarding tab.
  2. Enter any name you want to use for the Customized Application.
  3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
  4. Check the protocol you will be using, TCP and/or UDP.
  5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix F: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
  6. Check the Enable option for the port services you want to use. Consider the example below:

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

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

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

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

1. Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications and Gaming => Port Forwarding tab.

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

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

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

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

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

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

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

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

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

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

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

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

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

13. I need to upgrade the firmware.

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

- Follow these steps:
  1. Go to the Linksys website at http://www.linksys.com and download the latest firmware.
  2. To upgrade the firmware, follow the steps in the System section found in "Chapter 6: Configuring the Wireless-G VPN Router with RangeBooster."

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

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

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the PC; refer to "Problem #2, I need to set a static IP address." Use the following IP address settings for the computer you are using:
  IP Address: 192.168.1.50
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Router's web-based utility through its Administration tab.

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

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

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.
  1. To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
  4. Click the **Save Settings** button.
  5. Click the **Status** tab, and click the **Connect** button.
  6. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
- Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

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

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

- If you are having some difficulties, perform the following steps:
  1. To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
  4. Click the **Save Settings** button to continue.

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

17. The Power LED flashes continuously.

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

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

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

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support?

The Router will support up to 253 IP addresses.

Is IPSec Pass-Through supported by the Router?

Yes, it is a built-in feature that the Router automatically enables.

Where is the Router installed on the network?

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

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

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

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

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

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

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

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

How do I get Half-Life: Team Fortress to work with the Router?

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

How can I block corrupted FTP downloads?

If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

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

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

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

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

How will I be notified of new Router firmware upgrades?

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

Will the Router function in a Macintosh environment?

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

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

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and

then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

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

If DMZ Hosting is used, does the exposed user share the public IP with the Router?
No.

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

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

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

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

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

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

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

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

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

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

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

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

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

- CSMA/CA plus Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

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

What is infrastructure mode?

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

What is roaming?

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

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

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

What is ISM band?

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

What is Spread Spectrum?

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

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

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

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

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

What is WEP?

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

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Router?

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

How do I resolve issues with signal loss?

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

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

I have excellent signal strength, but I cannot see my network.

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

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

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

Appendix B: Wireless Security

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

Security Precautions

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

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

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

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

Security Threats Facing Wireless Networks

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

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

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

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

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

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

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

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

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

There are several ways that WEP can be maximized:

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

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

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

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

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

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

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

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

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

Overview

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

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 Wireless-G VPN Router 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 Access** 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 C-1: Access Restrictions - VPN Client Access Screen

Installing the LInksys QuickVPN Software

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

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

1. Go to *www.linksys.com* and select **Products**.
2. Click **Business Solutions**.
3. Click **Router/VPN Solutions**.
4. Click **WRV**.
5. Click **Linksys QuickVPN Utility** in the More Information section.
6. Save the zip file to your PC, and extract the .exe file.
7. Double-click the .exe file, and follow the on-screen instructions. Then proceed to the next section, "Using the Linksys QuickVPN Software."

Figure C-2: Setup Wizard - Welcome Screen

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.

2. The login screen will appear. Enter a name for your profile.

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

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

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

Figure C-3: QuickVPN Desktop Icon

Figure C-4: QuickVPN Tray Icon - No Connection

Figure C-5: QuickVPN Software - Profile

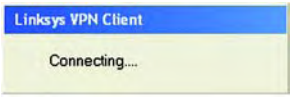


Figure C-6: Connecting

Figure C-7: Activating Policy

Figure C-8: 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 C-9: QuickVPN 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 C-10: QuickVPN Tray Icon - Connection

Figure C-11: QuickVPN Tray Icon - No Connection

Figure C-12: QuickVPN QuickVPN Software - Change Password

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

Introduction

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

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

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

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

WRV54G

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

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

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.

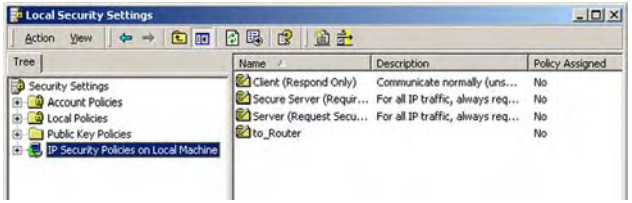


Figure D-1: Local Security Screen

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

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

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.

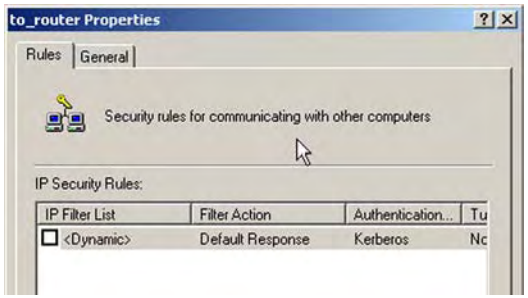


Figure D-2: Rules Tab

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

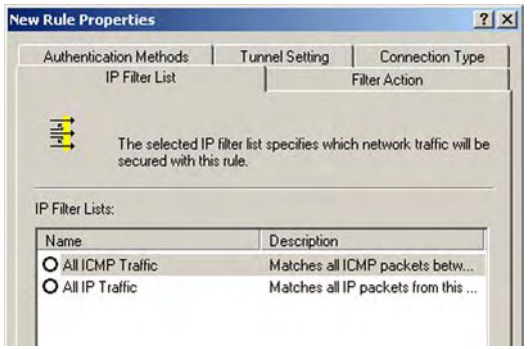


Figure D-3: IP Filter List Tab

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

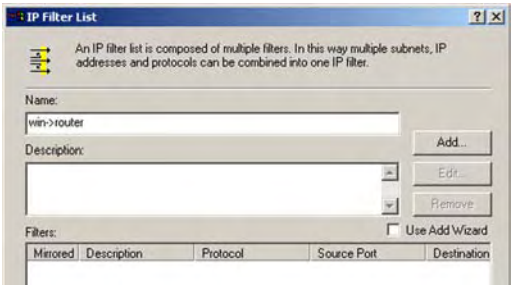


Figure D-4: IP Filter LIst

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

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

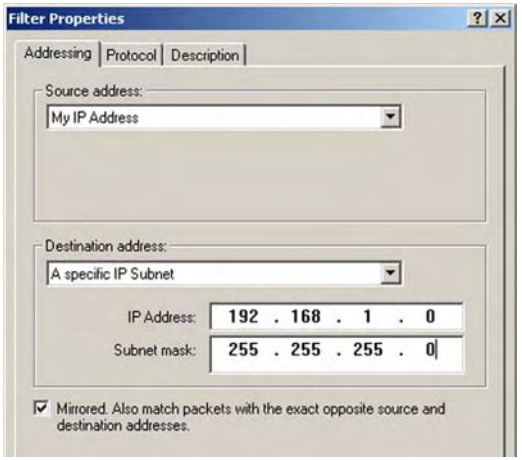


Figure D-5: Filters Properties

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

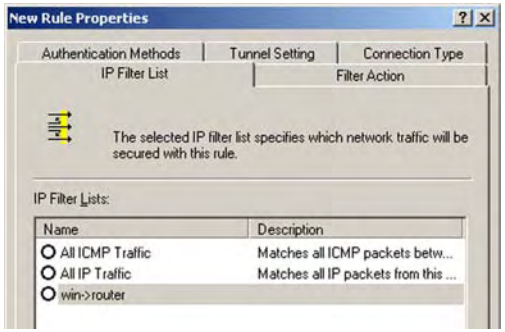


Figure D-6: New Rule Properties

Filter List 2: Router ->win

7. The *New Rule Properties* screen will appear. Select the **IP Filter List** tab, and make sure that **win -> Router** is highlighted. Then, click the **Add** button.

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

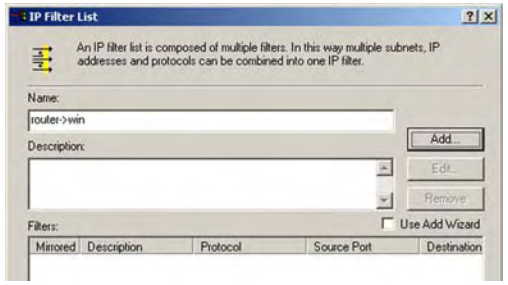


Figure D-7: IP Filter List

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

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

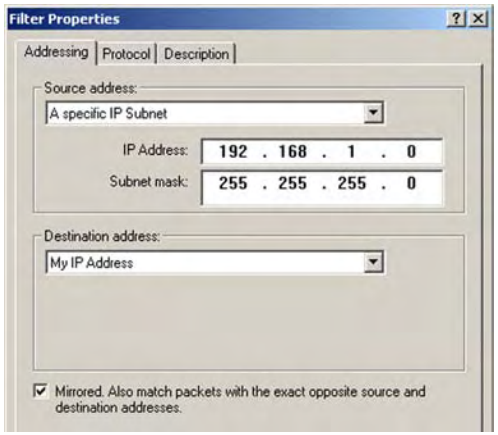


Figure D-8: Filters Properties

11. Click the **OK** or **Close** button and the *New Rule Properties* screen should appear with the IP Filer List tab selected. There should now be a listing for “Router -> win” and “win -> Router”. Click the **OK** (for WinXP) or **Close** (for Win2000) button on the *IP Filter List* window.

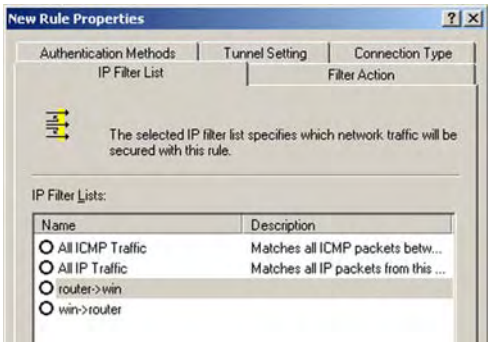


Figure D-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->Router

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

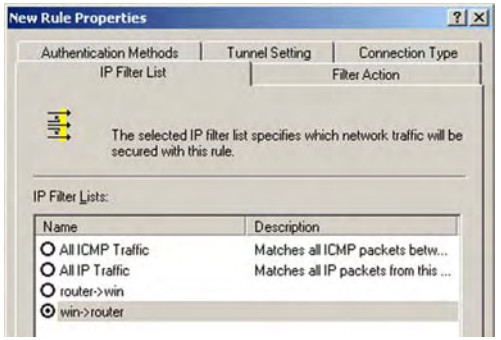


Figure D-10: IP Filter List Tab

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

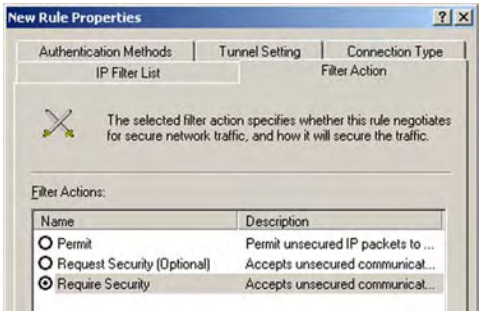


Figure D-11: Filter Action Tab

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

Figure D-12: Security Methods Tab

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

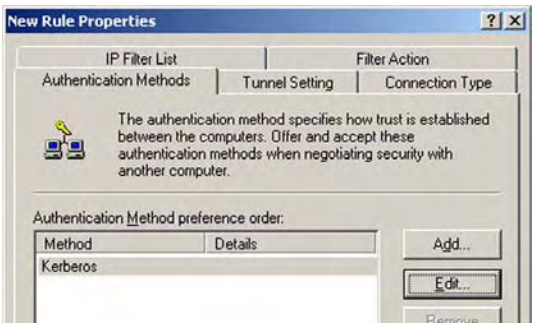


Figure D-13: Authentication Methods

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

Figure D-14: Preshared Key

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

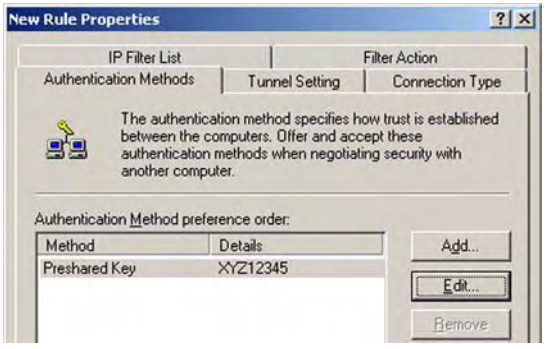


Figure D-15: New Preshared Key

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

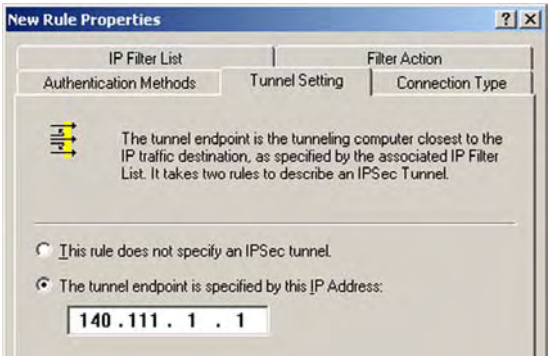


Figure D-16: Tunnel Setting Tab

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

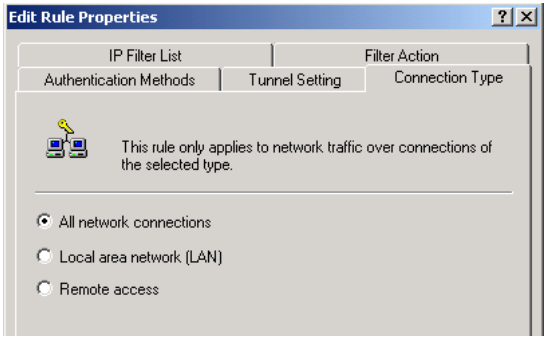


Figure D-17: Connection Type Tab

Tunnel 2: Router->win

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

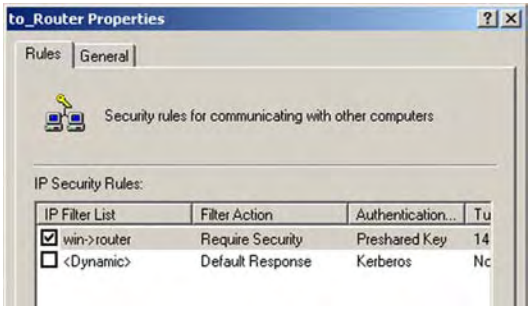


Figure D-18: Properties Screen

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

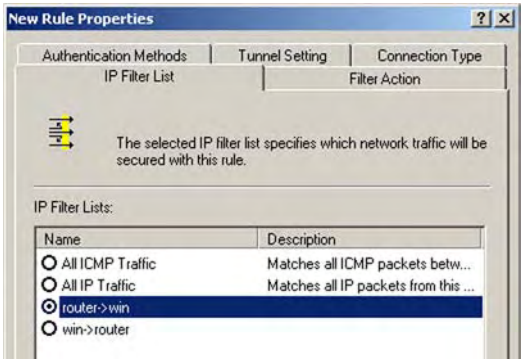


Figure D-19: IP Filter List Tab

11. Click the **Filter Action** tab, and select the filter action **Require Security**. Then, click the **Edit** button. From the *Security Methods* tab, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

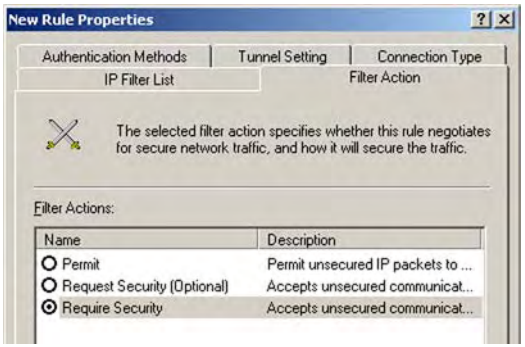


Figure D-20: Filter Action Tab

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

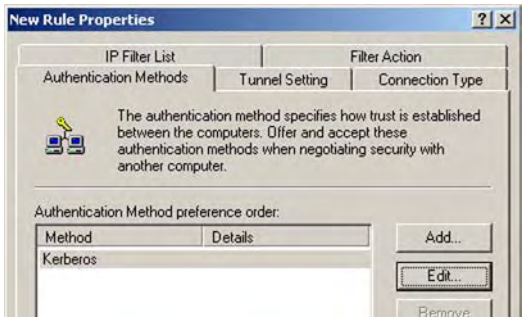


Figure D-21: Authentication Methods Tab

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

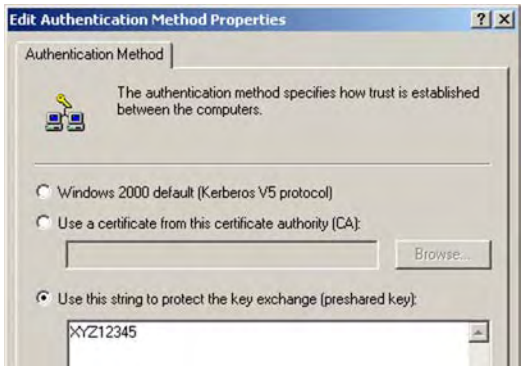


Figure D-22: Preshared Key

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

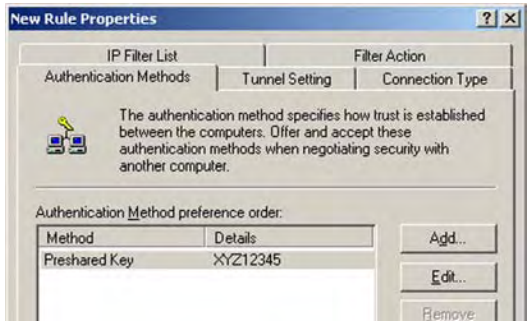


Figure D-23: New Preshared Key

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

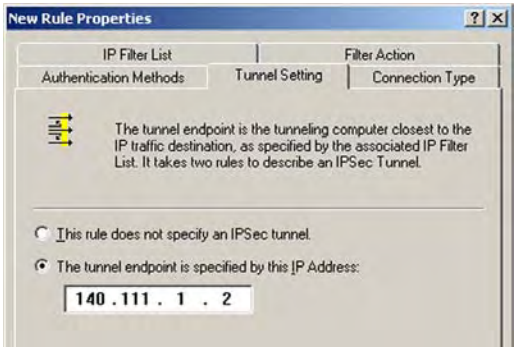


Figure D-24: Tunnel Setting Tab

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

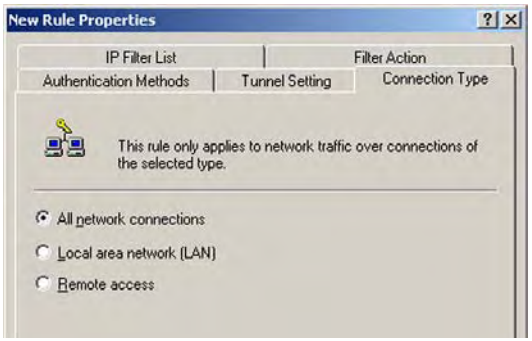


Figure D-25: Connection Type

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

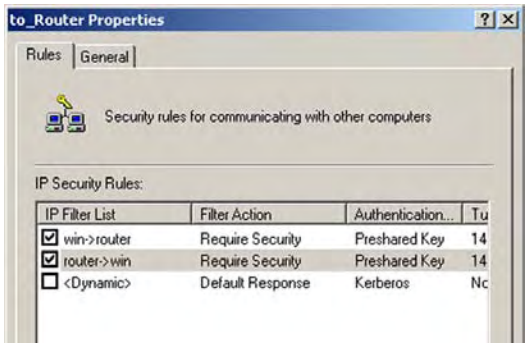


Figure D-26: Rules

Step 4: Assign New IPSec Policy

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

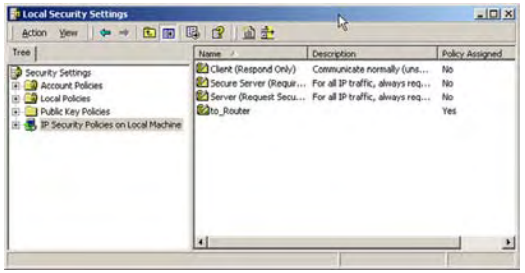


Figure D-27: Local Computer

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

1. Open your web browser, and enter **192.168.1.1** in the *Address* field. Press the **Enter** key.
2. When the *User name* and *Password* fields appear, enter the default user name and password, **admin**. Press the **Enter** key.
3. From the *Setup* tab, click the **VPN** tab.
4. From the *VPN* tab, select the tunnel you wish to create in the *Select Tunnel Entry* drop-down box. Then click **Enabled**. Enter the name of the tunnel in the *Tunnel Name* field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
5. Enter the IP Address and Subnet Mask of the local VPN Router in the *Local Secure Group* fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses (e.g. 192.168.1.0).
6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the *Remote Security Router* fields.
7. Select from two different types of encryption: **DES** or **3DES** (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable.
8. Select from two types of authentication: **MD5** and **SHA** (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication.
9. Select the Key Management. Select **Auto (IKE)** and enter a series of numbers or letters in the *Pre-shared Key* field. Check the box next to **PFS** (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the *Key Lifetime* field, you may optionally select to have the key expire at the end of a time period you designate. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.
10. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

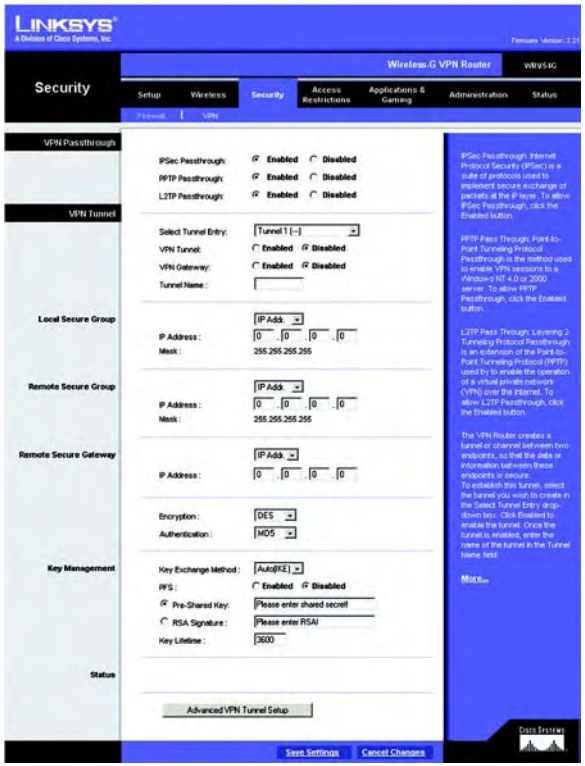


Figure D-28: VPN Tab

Appendix E: Configuring 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 fo the tunnel.

Figure E-1: Diagram of All VPN Tunnels

Before You Begin

The following is a list of equipment you need:

- Two Windows desktop PCs (each PC will be connected to a VPN Router)
- Two VPN Routers that are both connected to the Internet

NOTE: Each computer must have a network adapter installed.

Configuring the VPN Settings for the VPN Routers

Configuring VPN Router 1

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

1. Launch the web browser for a networked PC, designated PC 1.
2. Enter the VPN Router's local IP address in the *Address* field (default is **192.168.1.1**). Then press **Enter**.
3. A password request page will appear. (Non-Windows XP users will see a similar screen.) Complete the *User Name* and *Password* fields (**admin** is the default user name and password). Then click the **OK** button.
4. 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 E-2: Login Screen

Figure E-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 E-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, **28000**.
14. Click the **Save Settings** button on the *Auto (IKE) Advanced Settings* screen.
15. Click the **Save Settings** button on the *IPSec VPN* screen.

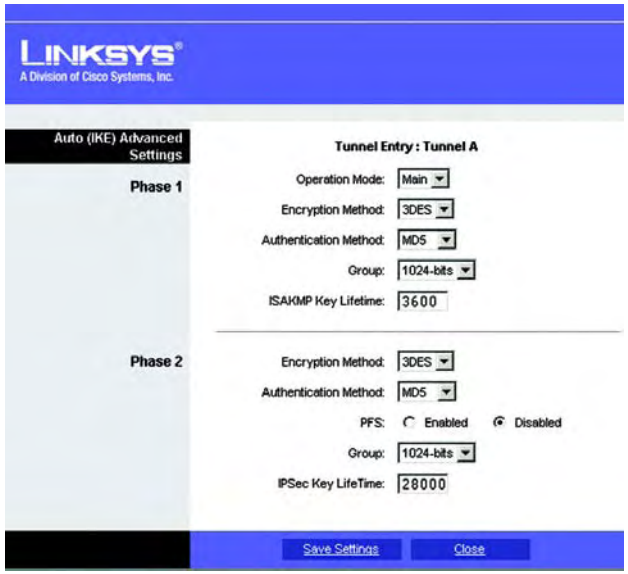


Figure E-5: Auto (IKE) Advanced Settings Screen

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 F: Finding the MAC Address and IP Address for your Ethernet Adapter

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

Windows 98 or Me Instructions

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

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

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

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

Figure F-1: IP Configuration Screen

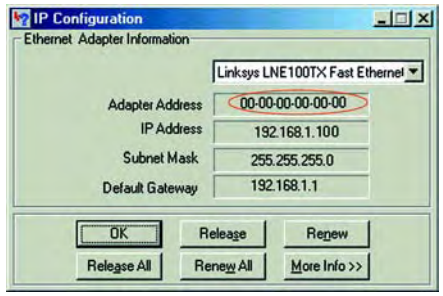


Figure F-2: MAC Address/Adapter Address