

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

LINKSYS®

A Division of Cisco Systems, Inc.



10/100 8-Port VPN Router User Guide

WIRED

Model No. **RV082**

CISCO SYSTEMS

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

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

How to Use this Guide

This User Guide has been designed to make understanding networking with the Router easier than ever. Look for the following items when reading this Guide:



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



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



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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

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

Table of Contents

Chapter 1: Introduction 1
Welcome 1
What's in this Guide? 2
Chapter 2: Networking Basics 4
An Introduction to LANs 4
The Use of IP Addresses 4
Why do I need a VPN? 5
What is a VPN? 6
Chapter 3: Getting to Know the Router 8
The Front Panel 8
The Back Panel 9
Chapter 4: Connecting the Router 10
Overview 10
Connection Instructions 11
Chapter 5: Setting Up and Configuring the Router 12
Overview 12
How to Access the Web-based Utility 15
System Summary Tab 15
Setup Tab - Network 18
Setup Tab - Time 21
Setup Tab - DMZ Host 22
Setup Tab - Forwarding 22
Setup Tab - UPnP Page 24
Setup Tab - One-to-One NAT 24
Setup Tab - MAC Clone 25
Setup Tab - DDNS 25
Setup Tab - Advanced Routing 26
DHCP Tab - Setup 28
DHCP Tab - Status 29
System Management Tab - Dual-WAN 29
System Management Tab - SNMP 31
System Management Tab - Diagnostic 32

System Management Tab - Factory Default 33
System Management Tab - Firmware Upgrade 33
System Management Tab - Restart 34
System Management Tab - Setting Backup 34
Port Management Tab - Port Setup 34
Port Management Tab - Port Status 35
Firewall Tab - General 36
Firewall Tab - Access Rules 37
Firewall Tab - Content Filter 39
VPN Tab - Summary 40
VPN Tab - Gateway to Gateway 42
VPN Tab - Client to Gateway 47
VPN Tab - VPN Client Access 54
VPN Tab - VPN Pass Through 55
VPN Tab - PPTP Server 55
Log Tab - System Log 56
Log Tab - System Statistics 57
Wizard Tab 58
Support Tab 63
Logout Tab 63
Appendix A: Troubleshooting 64
Common Problems and Solutions 64
Frequently Asked Questions 74
Appendix B: Installing the Linksys VPN Client 78
Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter 80
Windows 98 or Me Instructions 80
Windows 2000 or XP Instructions 80
For the Router's Web-based Utility 81
Appendix D: Physical Setup of the Router 82
Setting up the Router 82
Appendix E: Battery Replacement 86
Replacing a Lithium Battery 86
Appendix F: Upgrading Firmware 87
Appendix G: Windows Help 88

Appendix H: Glossary 89
Appendix I: Specifications 93
Appendix J: Warranty Information 94
Appendix K: Regulatory Information 95
Appendix L: Contact Information 96

List of Figures

Figure 2-1: VPN Router-to-VPN Router VPN 7
Figure 2-2: Computer-to-VPN Router VPN 7
Figure 3-1: Front Panel 8
Figure 3-2: Back Panel 9
Figure 4-1: Example of a Typical Network 10
Figure 4-2: Connect a PC 11
Figure 4-3: Connect the Internet and DMZ/Internet 11
Figure 4-4: Connect the Power 11
Figure 5-1: Router's IP Address 15
Figure 5-2: Login Screen 15
Figure 5-3: System Summary 15
Figure 5-4: Site Map 16
Figure 5-5: Setup Tab - Network 18
Figure 5-6: WAN Connection Type - Obtain an IP Automatically 18
Figure 5-7: WAN Connection Type - Static IP 19
Figure 5-8: WAN Connection Type - PPPoE 19
Figure 5-9: WAN Connection Type - PPTP 19
Figure 5-10: WAN Connection Type - Transparent Bridge 20
Figure 5-11: WAN Connection Type - Heart Beat Signal 20
Figure 5-12: Setup Tab - Password 21
Figure 5-13: Setup Tab - Time 21
Figure 5-14: Setup Tab - DMZ Host 22
Figure 5-15: Setup Tab - Forwarding 22
Figure 5-16: Port Range Forwarding - Service Management 23
Figure 5-17: Setup Tab - UPnP 24
Figure 5-18: Setup Tab - One-to-One NAT 24
Figure 5-19: Setup Tab - MAC Clone 25
Figure 5-20: Setup Tab - DDNS 25

Figure 5-21: Setup Tab - Advanced Routing 26
Figure 5-22: Setup Tab - Routing Table Entry List 27
Figure 5-23: DHCP Setup 28
Figure 5-24: DHCP Status 29
Figure 5-25: System Management Tab - Dual-WAN 29
Figure 5-26: Protocol Binding - Service Management 30
Figure 5-27: System Management Tab - SNMP 31
Figure 5-28: System Management Tab - DNS Name Lookup 32
Figure 5-29: System Management Tab - Ping 32
Figure 5-30: System Management Tab - Factory Default 33
Figure 5-31: Are You Sure 33
Figure 5-32: System Management Tab - Firmware Upgrade 33
Figure 5-33: System Management Tab - Restart 34
Figure 5-34: System Management Tab - Setting Backup 34
Figure 5-35: Port Management Tab - Port Setup 34
Figure 5-36: Port Management Tab - Port Status 35
Figure 5-37: Firewall Tab - General 36
Figure 5-38: Firewall Tab - Access Rules 37
Figure 5-39: Firewall Tab - Add a New Access Rule 38
Figure 5-40: Settings are Successful 38
Figure 5-41: Firewall Tab - Content Filter 39
Figure 5-42: VPN Tab - Summary 40
Figure 5-43: VPN Tab - Summary Detail 40
Figure 5-44: VPN Tab - Mode Choose 41
Figure 5-45: VPN tab - Gateway to Gateway 42
Figure 5-46: VPN tab - Gateway to Gateway Local Group Setup 42
Figure 5-47: VPN tab - Gateway to Gateway Remote Group Setup 43
Figure 5-48: VPN tab - Gateway to Gateway IPSec Setup 44
Figure 5-49: VPN tab - Client to Gateway 48
Figure 5-50: VPN tab - Client to Gateway Local Group Setup 48

Figure 5-51: VPN tab - Client to Gateway Remote Group Setup 49
Figure 5-52: VPN tab - Client to Gateway IPSec Setup 51
Figure 5-53: VPN tab - Client to Gateway Advanced 53
Figure 5-54: VPN tab - VPN Client Access 54
Figure 5-55: VPN tab - VPN Pass Through 55
Figure 5-56: VPN tab - PPTP Server 55
Figure 5-57: Log tab - System Log 56
Figure 5-58: Log tab - View Log 57
Figure 5-59: Log tab - System Statistics 57
Figure 5-60: Wizard tab 58
Figure 5-61: Basic Setup Wizard - Dual WAN or DMZ 58
Figure 5-62: Basic Setup Wizard - Host and Domain Name 59
Figure 5-63: Basic Setup Wizard - Selecting WAN Connection Types 59
Figure 5-64: Basic Setup Wizard - Save Settings 59
Figure 5-65: Access Rule Wizard - What is Access Rules 60
Figure 5-66: Access Rule Wizard - Select the Action 60
Figure 5-67: Access Rule Wizard - Select the Service 61
Figure 5-68: Access Rule Wizard - Select the Source 61
Figure 5-69: Access Rule Wizard - Select the Destination 62
Figure 5-70: Access Rule Wizard - When it Works 62
Figure 5-71: Support tab 63
Figure 5-72: Access Rule Wizard - When it Works 63
Figure 5-73: Save Settings 63
Figure 5-74: Settings are Successful 63
Figure 5-75: Support 63
Figure B-1: Linksys VPN License Agreement 78
Figure B-2: Linksys VPN Installation Complete 78
Figure B-3: Linksys QuickVPN 79
Figure C-1: IP Configuration Screen 80
Figure C-2: MAC Address/Adapter Address 80

Figure C-3: MAC Address/Physical Address 81
Figure C-4: MAC Address Clone 81
Figure D-1: Mounting Brackets 82
Figure D-2: Attaching the Brackets to the Router and Rack-Mounting the Router 83
Figure D-3: Wall-Mounting the Router 84
Figure D-4: Wall-Mounting Hardware 85
Figure F-1: Upgrade Firmware 87

Chapter 1: Introduction

Welcome

Thank you for choosing the 10/100 8-Port VPN Router. The Linksys 10/100 8-Port VPN Router is an advanced Internet-sharing network solution for your small business needs. Like any router, it lets multiple computers in your office share an Internet connection. But the unique dual Internet ports on the 10/100 8-Port VPN Router let you connect a second Internet line as a backup to insure that you're never disconnected. Or, use both Internet ports at the same time, and let the router balance your office's requirements between them for maximum bandwidth efficiency.

The 10/100 8-Port VPN Router also features a built-in 8-port full-duplex 10/100 Ethernet switch to connect eight PCs directly, or you can connect more hubs and switches to create as big a network as you need.

The Virtual Private Network (VPN) capability creates encrypted “tunnels” through the Internet, allowing up to 50 remote office or traveling users to securely connect into your office network from off-site. Users connecting through a VPN tunnel are attached to your company's network — with secure access to files, e-mail, and your intranet — just as if they were in the building. You can also use the VPN capability to allow users on your small office network to securely connect out to a corporate network.

The 10/100 8-Port VPN Router can serve as a DHCP Server, and has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks. It can be configured to filter internal users' access to the Internet, and has IP address filtering so you can specify exactly who has access to your network. Configuration is a snap with the web browser-based configuration utility.

As the heart of your small office network, the connection-redundant Linksys 10/100 8-Port VPN Router gives you the connection reliability your business needs.

Bandwidth: *the transmission capacity of a given device or network*

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

Full-duplex: *the ability of a networking device to receive and transmit data simultaneously*

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

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

firewall: *security measures that protect the resources of a local network from intruders*

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

IP: *a protocol used to send data over a network*

IP Address: *the address used to identify a computer or device on a network*

What's in this Guide?

This user guide covers the steps for setting up and using the 10/100 8-Port VPN Router.

- Chapter 1: Introduction
  This chapter describes the 10/100 8-Port VPN Router and this User Guide.
- Chapter 2: Networking Basics
  This chapter describes the basics of networking.
- Chapter 3: Getting to Know the 10/100 8-Port VPN Router
  This chapter describes the physical features of the Router.
- Chapter 4: Connecting the 10/100 8-Port VPN Router
  This chapter instructs you on how to connect the Router to your network.
- Chapter 5: Set Up and Configure the Router
  This chapter explains how to use the Web-Based Utility to set up the Router and configure its settings.
- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the 10/100 8-Port VPN Router.
- Appendix B: Installing the Linksys VPN Client
  This appendix instructs you on how to install the Linksys QuickVPN Client for remote users.
- Appendix C: 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 Router's MAC address cloning feature.
- Appendix D: Physical Setup of the Router
  This appendix describes the physical setup of the Router, including the installation of the mounting brackets.
- Appendix E: Battery Replacement
  This appendix instructs you how to replace the Router's battery.
- Appendix F: Upgrading Firmware
  This appendix instructs you on how to upgrade the Router's firmware if you should need to do so.
- Appendix G: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

Adapter: *a device that adds network functionality to your PC.*

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

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

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

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

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

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

Chapter 2: Networking Basics

An Introduction to LANs

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

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

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

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

***FTP**: a standard protocol for sending files between computers over a TCP/IP network and the Internet*

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

The Use of IP Addresses

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

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

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

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

***ISP**: a company that provides access to the Internet*

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

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

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

***DSL:** an always-on broadband connection over traditional phone lines*

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

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

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

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

By default, a DHCP server (on the LAN side) is enabled on the Router. If you already have a DHCP server running on your network, you MUST disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Router, see the Basic Setup section in "Chapter 5: Setting up and Configuring the Router."

Why do I need a VPN?

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

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

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

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

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently.

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



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

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

A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

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

3) Man in the middle attacks

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

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

What is a VPN?

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

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

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Router using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:

***encryption**: encoding data to prevent it from being read by unauthorized people*

***IPSec**: a VPN protocol used to implement secure exchange of packets at the IP layer*

•VPN Router to VPN Router

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

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

VPN Router to VPN Router

An example of a VPN Router-to-VPN Router VPN would be as follows. (See Figure 2-1.) At home, a telecommuter uses his VPN Router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.



Figure 2-1: VPN Router-to-VPN Router VPN

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

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

For additional information and instructions about creating your own VPN, please visit Linksys’s website at www.linksys.com.



Figure 2-2: Computer-to-VPN Router VPN

Chapter 3: Getting to Know the Router

The Front Panel

The Router's LEDs, ports, and Reset button are located on the front panel of the Router.

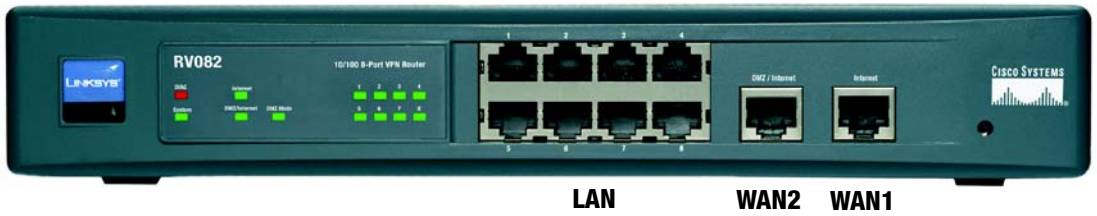


Figure 3-1: Front Panel

Ports

1-8 (LAN) These eight **LAN** (**Ethernet)** ports connect to network devices, such as PCs, print servers, or additional switches.

DMZ/Internet (WAN2) The **DMZ/Internet** port can be used in two different ways: a second Internet port, or DMZ port. When used as an additional Internet port, it connects to a cable or DSL modem. When used as a DMZ port, it connects to a hub, switch, or public server.

DMZ: *removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet*

Internet (WAN1) The **Internet** port connects to a cable or DSL modem.

LEDs

Diag Red. The **Diag** LED lights up when the system is not ready. The LED goes off when the system is ready.

System Green. The **System** LED lights up when the Router is powered on. If the LED is flashing, the Router is running a diagnostic test.

DMZ/Internet Green. The **DMZ/Internet** LED lights up when the Router is connected to your cable or DSL modem when used as an Internet port, and it lights up when the Router is connected to the hub, switch, or public server when used as a DMZ port.

Internet Green. The **Internet** LED lights up when the Router is connected to your cable or DSL modem.

DMZ Mode Green. The **DMZ Mode** LED lights up when the Router is using DMZ mode.

1-8 (LAN) Green. The **LAN** LED serves two purposes. If the LED is continuously lit, the Router is connected to a device through the corresponding port (1, 2, 3, 4, 5, 6, 7, or 8). If the LED is flashing, the Router is actively sending or receiving data over that port.

Reset Button The Reset button can be used in one of two ways:
If the Router is having problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the Reset button on your PC to reboot it.

If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for 30 seconds. This will restore the factory defaults and clear all of the Router's settings, such as port forwarding or a new password.

Boot: *to start a device and cause it to start executing instructions*

The Back Panel

The Router's Power port is located on the back panel of the Router.

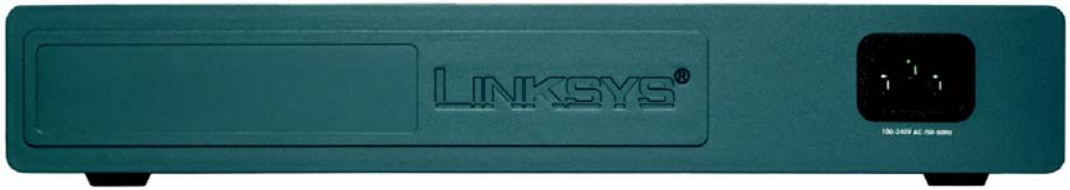


Figure 3-2: Back Panel

Power The **Power** port is where you connect the AC power cord.

Proceed to "Chapter 4: Connecting the Router."

Chapter 4: Connecting the Router

Overview

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

- Connect the Router to one of your PCs according to the instructions in this chapter.
- If necessary, configure your PCs to obtain an IP address automatically from the Router, according to "Appendix G: Windows Help". (By default, Windows 98, 2000, Millennium, and XP computers are set to obtain an IP address automatically, so unless you have changed the default setting, then you will not need to configure your PCs.)
- Set up and configure the Router with the setting(s) provided by your Internet Service Provider (ISP) according to "Chapter 5: Setting up and Configuring the Router."

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

Broadband: *an always-on, fast Internet connection*

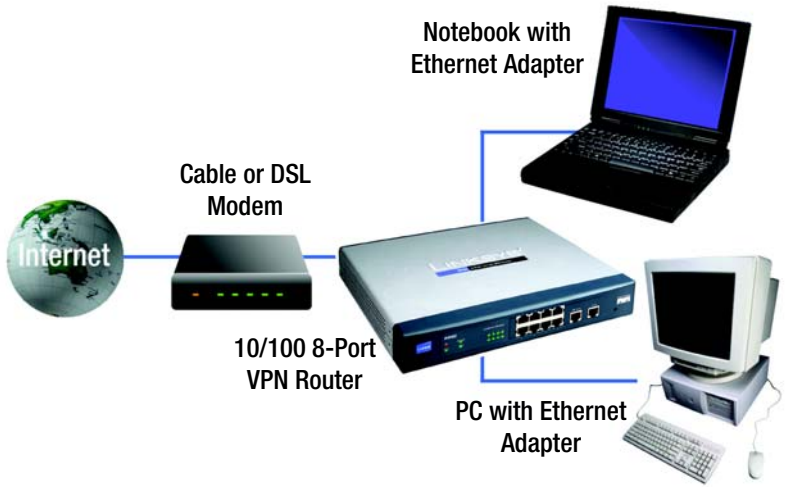


Figure 4-1: Example of a Typical Network

Connection Instructions

1. Before you begin, make sure that all of your hardware is powered off, including the Router, PCs, hubs, switches, and cable or DSL modem.

2. Connect one end of an Ethernet network cable to one of the numbered ports on the front of the Router. Connect the other end to an Ethernet port on a network device, e.g., a PC, print server, hub, or switch.

   Repeat this step to connect more PCs or other network devices to the Router.

3. Connect your cable or DSL modem's Ethernet cable to the Router's Internet port. If using the DMZ/Internet port, connect a second cable to it, and the other end to the network device, e.g., modem or public server.

4. Power on the cable or DSL modem and the other network device if using one.

5. Connect the included power adapter to the Router's Power port on the back of the Router, as shown in Figure 4-4, and then plug the power adapter into an electrical outlet.

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

If you need to configure your PCs, proceed to "Appendix G: Windows Help." Otherwise, proceed to "Chapter 5: Setting Up and Configuring the Router."

Hardware: *the physical aspect of computers, telecommunications, and other information technology devices*



Figure 4-2: Connect a PC



Figure 4-3: Connect the Internet and DMZ/Internet



Figure 4-4: Connect the Power

Chapter 5: Setting Up and Configuring the Router

Overview

The Router comes with a Web-based Utility that allows for easy set up and configuration. This chapter will explain all of the functions in this Utility. (You can access the web-based utility by accessing 192.168.1.1.)

There are eleven main tabs in the Utility: System Summary, Setup, DHCP, System Management, Port Management, Firewall, VPN, Log, Wizard, Support, and Logout. Sub-tabs are be available when you click one of the main tabs. The tabs are described below:

System Summary Tab

The System Summary Tab displays the Router's current status and settings. This information is read only. Some words are underlined on this screen and, if you click them, will take you to the Utility page appropriate for that word.

Setup Tab

From this tab, you can set the basic settings on your network. The screens available from this tab include:

- Network. Enter the Internet connection and network settings on this screen.
- Password. From this screen, you can change the Router's password on this screen. For network security, you should always change the password from its default setting.
- Time. Change the time shown on the network from this screen.
- DMZ Host. The DMZ (Demilitarized Zone) Host feature allows one network PC to be exposed to the Internet to use special-purpose services such as Internet gaming or video conferencing.
- Forwarding. Port forwarding can be used to set up public services on your network. You may use this function to establish a Web server or FTP server via an IP Gateway.
- UPnP. UPnP forwarding, set up on this screen, can be used to set up public services on your network.
- One-to-One NAT. Like the DMZ feature, One-to-One NAT opens the NAT firewall for one computer, but does it only for one Internet address. This feature is administered through this screen.

- MAC Clone. Some ISPs require that you register a MAC address. From this screen, you can "clone" your network adapter's MAC address onto the Router. This prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address.
- DDNS. DDNS (Dynamic DNS) service, on this screen, allows you to assign a fixed domain name to a dynamic Internet IP address. This allows you to host your own Web, FTP or other type of TCP/IP server in your network.
- Advanced Routing. The Router's dynamic routing feature can be set up on this screen to automatically adjust to physical changes in the network's layout.

DDNS: *the capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name*

Domain: *a specific name for a network of computers*

DHCP Tab

- Setup. From this screen, you can enable/disable the DHCP server, set up client lease time, DHCP IP Range, and the WINS Server IP address.
- Status. This Status page is available to review DHCP Server Status.

System Management Tab

- Dual WAN. The Dual WAN feature allows you to use two Broadband connections at once, specifying between using one as a Primary connection, with Smart Link Backup, and using both connections in concert, with Load Balance.
- SNMP. SNMP, or 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. SNMP can be managed from this screen.
- Diagnostic. From this screen, you can use the Router's two built-in tools to troubleshoot network problems.
- Factory Default. The "Factory Default" button on this screen can be used to clear all of your configuration information and restore the Router to its factory default settings. Only use this feature if you wish to discard all other configuration preferences.
- Firmware Upgrade. Users can use the function on this screen to upgrade the Router's firmware to the newest version.
- Restart. The recommended method of restarting your Router is to use the "Restart Router" button on this screen. Restarting with this button will send out your log file before the box is reset.
- Setting Backup. This screen allows you to make or import a backup file of your Preferences file for the Router.

Port Management Tab

- Port Setup. From this screen, users can configure the functionality for each port.
- LAN Status. Users can choose this screen to see the status of a selected port.

Firewall Tab

- General. From this screen, you can configure the Router's broadest settings for denying or allowing specific users from accessing the Internet.
- Access Rules. Access Rules determine how and when network traffic will be allowed access to the network or to the Internet, determining when traffic is allowed to pass through the firewall.
- Content Filter. This screen allows you to filter web access by site, keyword and time.

VPN Tab

- Summary. The VPN Summary screen displays a quick view of VPN activity and status.
- Gateway to Gateway. From this screen, users can administer tunnels between two VPN devices.
- Client to Gateway. From this screen, tunnels between a Local VPN device and a mobile user can be administered.
- VPN Client Access. From this screen, you can manage the use of the Linksys QuickVPN Client, the VPN Client software that came with this Router. This allows network users remote access via the VPN.
- VPN Pass Through. This tab allows you to enable or disable IPSec Pass Through, PPTP Pass Through, and L2TP Pass Through.
- PPTP Server. From this screen, you can manage access to the VPN Router, through its built-in PPTP Server, from those using Windows PPTP VPN software to gain access. This is less secure than the VPN Client Access feature.

Log Tab

- System Log. The System Log allows you to administer the Syslog, E-mail and Log Settings.
- System Statistics. This screen displays the system statistics.

Wizard Tab

- Wizard. Use this tab to access two Setup Wizards, the Basic Setup Wizard and Access Rule Setup Wizard.

Support Tab

- Support. The buttons on this tab allow you to access the user guide and the Linksys website.

Logout Tab

- Logout. Clicking this tab exits you from the Utility.

How to Access the Web-based Utility

To access the Router's 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 the **Enter** key.

A *Login* screen will appear asking you for your User name and Password. Enter **admin** in the *User name* field, and enter **admin** in the *Password* field. Then, click the **OK** button.

System Summary Tab

The first screen that appears is *System Summary Tab*. This screen displays the Router's current status and settings. This information is read-only. Words that are underlined will, when clicked, open the Setup page for that feature. On the right side of the screen and all other screens in the Utility will be a link to the *Site Map*, which has links to all of the Utility's tabs. Click the **Site Map** button to view the Site Map (shown in Figure 5-4). Then, click on desired tab subject.

System Information

Serial Number: The Router's serial number is displayed here.

Firmware version: This shows the current version number of the firmware installed on this unit.

CPU: This shows the type of processor installed on the Router.

DRAM: This displays the amount of Dynamic Random Access Memory (DRAM), in Megabytes, the Router has.

Flash: This displays the amount of Flash Memory, in Megabytes, the Router has.



Figure 5-1: Router's IP Address



Figure 5-2: Login Screen

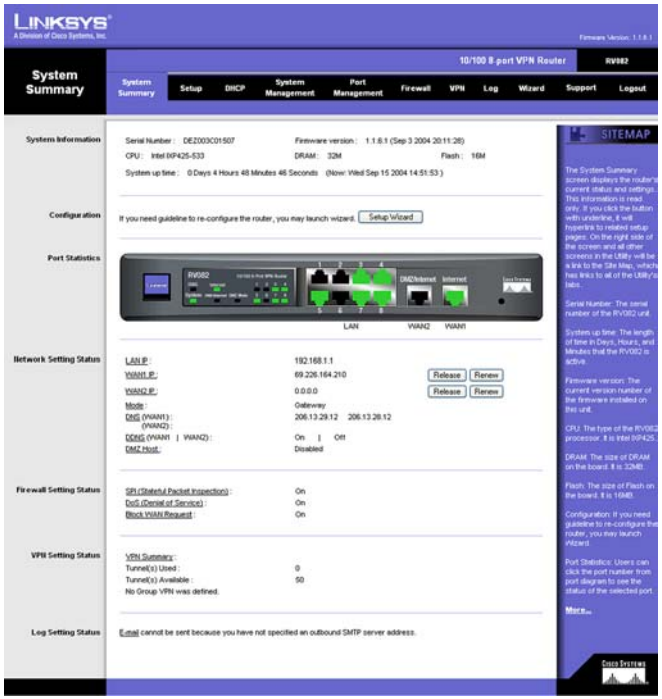


Figure 5-3: System Summary

System Up Time: This displays the length of time in Days, Hours, and Minutes that the Router has been active, along with the current time.

Configuration

If you need help configuring the router, click the **Setup Wizard** button. A complete walk-through of the Setup Wizard is shown in the Wizard Tab section.

Port Statistics

You can check the status of any of the Router's ports simply by clicking the port number on the port diagram. If the port is disabled, it will be red; if enabled, it will be black. If it is connected, it will be green.

This will open up a summary table. This summary table will show the port's settings, such as Type, Link Status (up or down), Port Disable (on or off), Priority (High or Normal), Speed Status (10Mbps or 100Mbps), Duplex Status (half or full), Auto negotiation (enable or disable). The statistics table will show the amounts of packets and bytes received or sent by a port as well as the Port Packet Error Count of the selected port. The LAN ports can be configured from the LAN Setup page of the LAN Management Tab.

Network Setting Status

LAN IP: This shows the Router's current LAN IP Address, and hyperlinks to that section of the Setup Tab.

WAN1 IP: This shows the IP Address of the WAN1 IP port, hyperlinked to that section of the Setup Tab. When WAN1 is set up to *Obtain an IP automatically*, two buttons will be shown here: *Release* and *Renew*. Click the **Release** button to release the current IP Address and click the **Renew** button to update the DHCP Lease Time or get a new IP. When WAN1 is set up with *PPPoE* or *PPTP*, these two buttons will be displayed as *Connect* and *Disconnect*.

WAN2/DMZ IP: This shows the IP Address of the WAN2 IP port, or DMZ IP when DMZ is selected, hyperlinked to that section of the Setup Tab.

Mode: This tells you if the Router's Working Mode is *Gateway* or *Router*, hyperlinked to that section of the Setup Tab

DNS: All DNS Server Addresses are displayed here, with hyperlinks to that section of the Setup Tab.

DDNS: This shows if the DDNS status is *On* or *Off*, with hyperlinks to that section of the Setup Tab.

DMZ Host: If this feature is enabled, the DMZ Private Address will be displayed. This is also hyperlinked to that section of the Setup Tab.

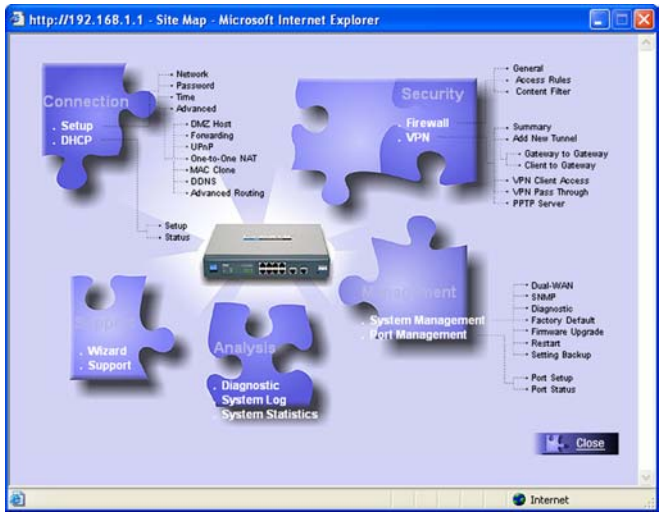


Figure 5-4: Site Map

***DNS** the IP address of your ISP's server, which translates the names of websites into IP addresses*

Firewall Setting Status

SPI (Stateful Packet Inspection): This shows if the SPI status is *On* or *Off*, hyperlinked to that section of the Firewall Tab.

DoS (Denial of Service): This shows if the DoS status is *On* or *Off*, hyperlinked to that section of the Firewall Tab.

Block WAN Request: This shows if the Block WAN Request status is *On* or *Off*, hyperlinked to that section of the Firewall Tab.

VPN Setting Status

VPN Summary: This hyperlink will take you to the Summary page of the VPN Tab.

Tunnel(s) Used: This displays the amount of VPN Tunnels used.

Tunnel(s) Available: This displays the amount of VPN Tunnels available.

Current Connected (The Group Name of GroupVPN1) users: This displays the amount of VPN users connected via GroupVPN1.

Current Connected (The Group Name of GroupVPN2) users: This displays the amount of VPN users connected via GroupVPN2.

(If GroupVPN is disabled, it will show "No Group VPN was defined.")

Log Setting Status:

This hyperlink will take you to the System Log page of the Log Tab.

If you have not set up the Log's mail server, this will show "E-mail cannot be sent because you have not specified an outbound SMTP server address."

If you have set up the mail server but the log has not come out due to Log Queue Length and Log Time Threshold settings, this will show "E-mail settings have been configured."

If you have set up the mail server and the log has been sent to the mail server, this will show "E-mail settings have been configured and sent out normally."

If you have set up the mail server and the log cannot be sent to mail server successfully, this will show "E-mail cannot be sent out, probably use incorrect settings."

Setup Tab - Network

The Setup screen contains all of the Router's basic setup functions. These functions can be set from this screen but normally don't need to be adjusted, as the Router has been designed to be used in most network settings without changing any of the default values. Some users, however, may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL, cable modem) carrier.

Network

Host Name & Domain Name: Some ISPs may require a Host Name and Domain Name for identification, and can provide them to you. In most cases, though, leaving these fields blank will work.

LAN Setting

This is the Router's LAN IP Address and Subnet Mask. The default value is **192.168.1.1** for IP address and **255.255.255.0** for the Subnet Mask.

Dual-WAN / DMZ Setting

Before choosing the WAN Connection Type, select between a Dual-WAN or DMZ Setting. The Dual-WAN Setting will allow you to connect two Broadband connections to the Router at once, specifying between using one as a Primary connection, with Smart Link Backup, and using both connections in concert, with Load Balance. These settings can be found on the Dual-Wan screen of the Systems Management Tab. The DMZ setting allows one network PC to be exposed to the Internet to use special-purpose services such as Internet gaming or video conferencing.

There are two different DMZ types: Subnet and Range. If you choose Subnet, enter the IP Address and Subnet Mask of the PC connected to the DMZ port; this DMZ must have a Static IP address. If Range is selected, the DMZ port and the WAN port will be in the same subnet. Enter the IP Range for the DMZ port.

WAN Connection Type

Obtain an IP Automatically

If your ISP automatically assigns an IP Address, select **Obtain an IP automatically**. If you check the box for **Use the Following DNS Server Addresses**, enter a specific DNS Server IP Address. Multiple DNS IP Settings are common. In most cases, the first available DNS entry is used.



Figure 5-5: Setup Tab - Network

cable modem: *a device that connects a computer to the cable television network, which in turn connects to the Internet*

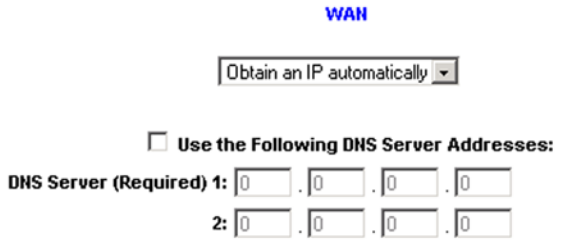


Figure 5-6: WAN Connection Type - Obtain an IP Automatically

Static IP

If you have to specify the WAN IP Address, Subnet Mask, Default Gateway Address, and DNS Server, select **Static IP**. All of this information can be obtained from your ISP.

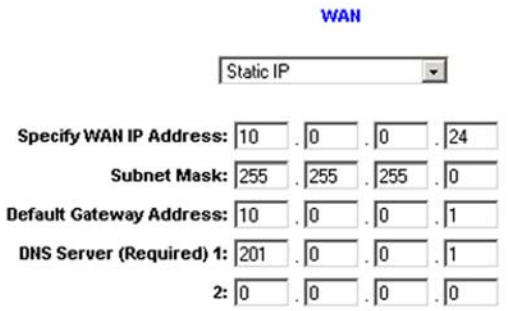


Figure 5-7: WAN Connection Type - Static IP

PPPoE (Point-to-Point Protocol over Ethernet) (most DSL users)

Your ISP will let you know whether PPPoE should be enabled or not, which will be determined by if they use this protocol. To enable PPPoE:

1. Enter the User Name and Password you use to access your ISP account.
2. By selecting the **Connect on Demand** option, the PPPoE connection will be disconnected if it has been idle for a period longer than the Max Idle Time setting.
3. By selecting the **Keep Alive** option, the Router will keep the connection alive by sending out a few data packets at the Redial Period, so your Internet service thinks that the connection is still active.

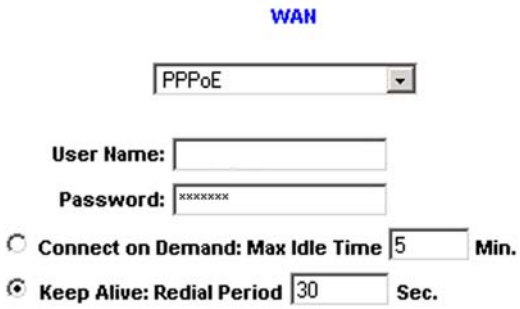


Figure 5-8: WAN Connection Type - PPPoE

PPTP (Point-to-Point Tunneling Protocol)

1. Enter the WAN IP Address, Subnet Mask and Default Gateway Address provided by your ISP.
2. Enter the User Name and Password you use to access your ISP account.
3. By selecting the **Connect on Demand** option, the connection will be disconnected if it has been idle for a period longer than the Max Idle Time setting.

By selecting the **Keep Alive** option, the Router will keep the connection alive by sending out a few data packets at the Redial Period, so your Internet service thinks that the connection is still active.

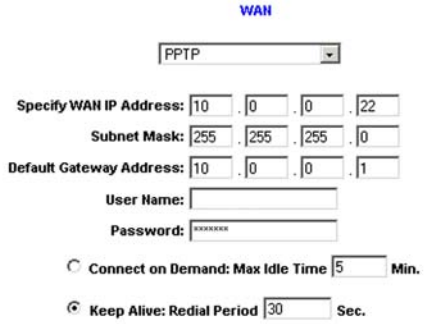


Figure 5-9: WAN Connection Type - PPTP

Transparent Bridge

Transparent Bridging is used when you have two large networks that you wish to bridge together. Your network administrator should fill in the information for both network segments, including the range of IP addresses each network includes. When this is selected, the WAN and LAN must be in the same subnect and only one WAN port can be set in Transparent Bridge mode.

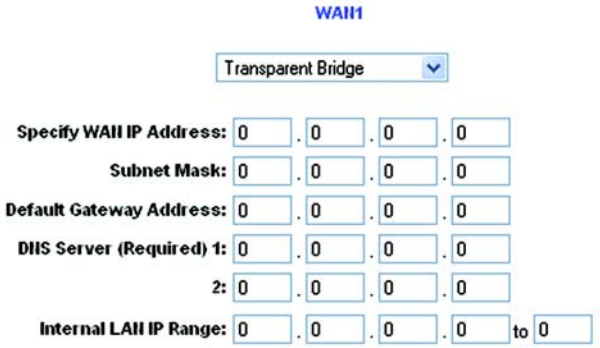


Figure 5-10: WAN Connection Type - Transparent Bridge

Heart Beat Signal

Heart Beat Signal is a service used in Australia only. If you are using a Heart Beat Signal connection, check with your ISP for the necessary setup information.

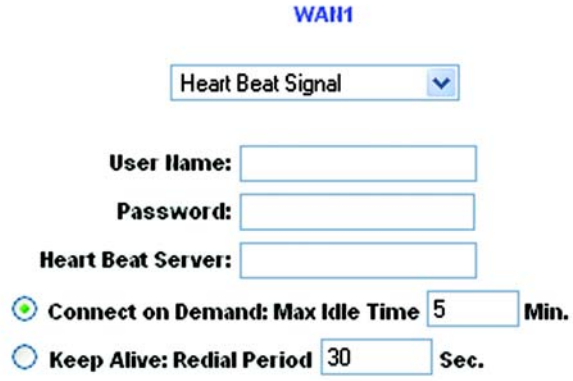


Figure 5-11: WAN Connection Type - Heart Beat Signal

Setup Tab - Password

The Router's default User Name and Password is **admin**. For greater network security, you should change the Router's password from this default. If you leave the password field blank, all users on your network will be able to access the Router simply by entering **admin** into the password field.



Figure 5-12: Setup Tab - Password

Old Password: Enter the old password.

NOTE: The password cannot be recovered if it is lost or forgotten. If the password is lost or forgotten, you have to reset the Router to its factory default settings.

New Password: Enter a new password for the Router. Your password must be less than 64 alphanumeric characters long and it can't contain any spaces.

Confirm New Password: Re-enter the new password for confirmation.

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

Setup Tab - Time

Time

The Router uses the time settings to time stamp log events, to automatically update the Content Filter List, and for other internal purposes.



Figure 5-13: Setup Tab - Time

Set the local time with **Set the local time using Network Time Protocol (NTP) automatically** or **Set the local time Manually**. When you choose to have the time set by using Network Time Protocol, the Router will automatically connect to an NTP server, providing the correct time.

Automatic: Select the Time Zone and enter the Daylight Saving and NTP Server. The default Time Zone is Pacific Time.

Manual: Enter the Hours, Minutes, Seconds, Month, Day and Year.

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

Setup Tab - DMZ Host

The DMZ (Demilitarized Zone) Host feature opens the firewall for one of your network's users so they can access the Internet to use a special-purpose service such as Internet gaming or video conferencing. This user, however, is unprotected by the firewall.

To open the firewall for one network user to access one website, and visa versa, utilize the One-to-One NAT feature.

Enter the **DMZ Private IP Address** to access the DMZ Host settings. The Default value zero (0) will deactivate the DMZ Host.

Click the **Save Settings** button to save the DMZ Host setting or click the **Cancel Changes** button to undo the changes.



Figure 5-14: Setup Tab - DMZ Host

http: *the communications protocol used to connect to servers on the World Wide Web.*

Setup Tab - Forwarding

Port forwarding can be used to set up public services on your network. When users outside your network (i.e., from the Internet) make certain requests on your network, the Router can forward those requests to the appropriate computers equipped to handle the requests. If, for example, you set port number 80 (HTTP) to be forwarded to IP Address 192.168.1.2, then all HTTP requests from outside users will be forwarded to 192.168.1.2.

You may use this function to establish a Web server or FTP server via an IP Gateway. Be sure that you enter a valid IP Address. (You may need to establish a static IP address in order to properly run an Internet server.) For added security, those outside your network (i.e., from the Internet) will be able to communicate with the server but they will not actually be connected. Those packets will simply be forwarded through the Router.



Figure 5-15: Setup Tab - Forwarding

Port Range Forwarding

1. Select the Service from the pull-down menu, shown in Figure 5-15.
2. If the Service you need is not listed in the menu, please click the **Service Management** button to add the new Service Name, and enter the Protocol and Port Range. This will open the Service Management screen. Click the **Add to List** button. Then, click the **Save Setting** button. Click the **Exit** button.
3. Enter the IP Address of the server that you want the Internet users to access. Then enable the entry.
4. Click the **Add to List** button, and configure as many entries as you would like. You also can **Delete selected application**.

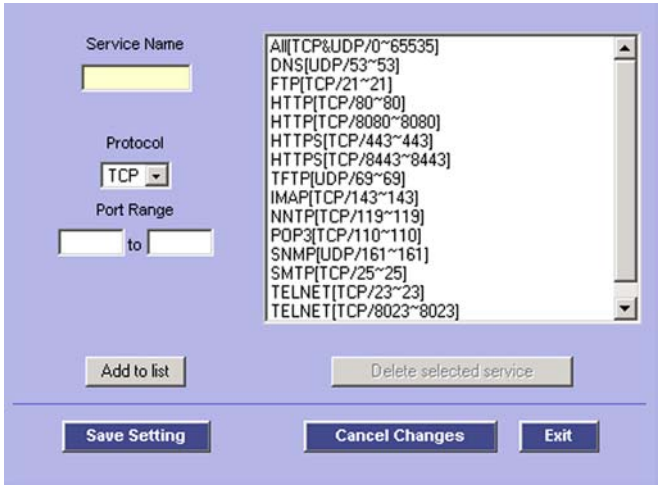


Figure 5-16: Port Range Forwarding - Service Management

Port Triggering

Some Internet applications or games use alternate ports to communicate between server and LAN host. When you want to use those applications, enter the triggering (outgoing) port and alternate incoming port in this table. The Router will forward the incoming packets to the LAN host.

1. Enter the application name, range of port numbers, and the incoming port range.
2. You can click the **Add to List** button, shown in Figure 5-15, to add Port Triggering or **Delete selected application**.

Click the **Save Settings** button to save the settings, click the **Cancel Changes** button to undo your changes, click the Show Tables to see the details.

NOTE: The Router's WAN IP (NAT Public) Address may not be included in a range.

NOTE: One-to-One NAT does not change the way the firewall functions work. Access to machines on the LAN from the Internet will not be allowed unless Network Access Rules are set.

Setup Tab - UPnP Page

UPnP forwarding can be used to set up public services on your network. Windows XP can modify those entries via UPnP when UPnP function is enabled.

UPnP Function: Enable this function by selecting **Yes**. The default setting for this feature is **No**.

To add a UPnP function:

1. Select the Service from the pull-down menu.
2. If the Service you need is not listed in menu, please click the **Service Management** button to add the new Service Name, and enter the Protocol and Port Range. Click the **Add to List** button. Then, click the **Save Setting** button. Click the **Exit** button.
3. Enter the Name or IP Address of the server that you want the Internet users to access. Then enable the entry.

Click the **Add to List** button, and configure as many entries as you would like. You also can **Delete selected application**. You can also see the specifics of each service you've added by clicking the **Show Tables** button.



Figure 5-17: Setup Tab - UPnP

Setup Tab - One-to-One NAT

One-to-One NAT opens the firewall for one network user a lot like the DMZ host feature. In this feature, however, the network user is restricted to a single website.

To enable One-to-One NAT, check the **Enable** box at the top of the screen.

To set this up, you must define internal and external address ranges of equal length. Set the beginning of the Private Range - this will be a range of IP Addresses on your network. Then, set the beginning of the Public Range - this is the range of IP Addresses on the Internet. Lastly, set the Range Length. For however long this length is, each first address will correspond and connect, as will the second, third, forth, etc. Up to 64 ranges may be added. To map a single address, use a Range Length of 1.

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



Figure 5-18: Setup Tab - One-to-One NAT

NOTE: One-to-One NAT does change the way the firewall functions work. Access to machines on the LAN from the Internet will be allowed unless Network Access Rules are set.

Setup Tab - MAC Clone

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

Enter the MAC Address in the User Defined WAN1 or WAN2 MAC Address field or select **MAC Address from this PC**.

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



Figure 5-19: Setup Tab - MAC Clone

Setup Tab - DDNS

DDNS (Dynamic DNS) service allows you to assign a fixed domain name to a dynamic WAN IP address. This allows you to host your own Web, FTP or other type of TCP/IP server in your LAN.

Before configuring DDNS, you need to visit *www.dyndns.org* or *www.3322.org* and register a domain name. (The DDNS service is provided by DynDNS.org).

DDNS Service: The DDNS feature is disabled by default. To enable this feature, just select **DynDNS.org** or **3322.org** from the pull-down menu, and enter the User name, Password, and Host Name of the account you set up with the DDNS service.

Your IP Address: The current IP Address for the WAN port (1 or 2) is displayed here. Because it is dynamic, this will change.

Status: The status of the DDNS function and Internet status is displayed.

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



Figure 5-20: Setup Tab - DDNS

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

Setup Tab - Advanced Routing

Dynamic Routing

The Router's dynamic routing feature can be used to automatically adjust to physical changes in the network's layout. The Router uses the dynamic RIP protocol, which is a networking protocol to manage network communications or communications between networks. It determines the route that the network packets take based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

Working Mode: Select **Gateway** mode if the Router is hosting your network's connection to the Internet. Select **Router** mode if the Router exists on a network with other routers, including a separate network gateway that handles the Internet connection. When this Router is in Router Mode, you must have another router function as the gateway in order for any computer connected to the Router to be able to connect to the Internet.

RIP (Routing Information Protocol): The Router, using the RIP protocol, calculates the most efficient route for the network's data packets to travel between the source and the destination, based upon the shortest paths.

Receive RIP versions: Choose the protocol for receiving data from the network. (None, RIPv1, RIPv2, Both RIPv1 and v2).

Transmit RIP versions: Choose the protocol for transmitting data on the network. (None, RIPv1, RIPv2-Broadcast, RIPv2-Multicast)



Figure 5-21: Setup Tab - Advanced Routing

Static Routing

You will need to configure Static Routing if there are multiple routers connected to your network. The static routing function determines the path data follows over your network. Static routing allows different IP domain users to access the Internet through this device. This is an advanced feature. Please proceed with caution.

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

Enter the following data to create a static route entry:

1. Destination IP: Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be zero.
2. Subnet Mask: Enter the Subnet Mask used on the destination LAN IP domain. For Class C IP domains, the Subnet Mask is 255.255.255.0.
3. Default Gateway: If this Router is used to connect your network to the Internet, then your gateway IP is the Router's IP Address. If you have another router handling your network's Internet connection, enter the IP Address of that router instead.
4. Hop Count (max. 15): This value gives the number of nodes that a data packet passes through before reaching its destination. A node is any device on the network, such as switches, PCs, etc.
5. Interface: (LAN, WAN1, WAN2/DMZ) This setting directs where the static route is going, either to a PC in your network or to the Internet. If you're connecting to a network, select **LAN**. If you're connecting to another network through the Internet, select **WAN**.

Click **Add to list** to add a route entry or click **Delete Selected IP** to delete the static route entry.

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

Clicking the **Show Routing Table** button will open the *Routing Table Entry List*. This will show the routes you have established, with network information, number of hops for each route, and the type of interface used. Click the **Refresh** button to update the screen or **Close** to close it.

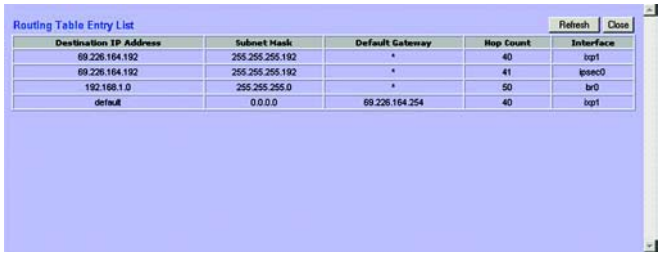


Figure 5-22: Setup Tab - Routing Table Entry List

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

node: *a network junction or connection point, typically a computer or work station*

DHCP Tab - Setup

Setup

The Router can be used as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server assigns available IP addresses to each computer on your network automatically. If you choose to enable the DHCP server option, you must configure all of the PCs on your LAN to connect to a DHCP server. (See Appendix G: Windows Help.)

Enable DHCP Server: Check the box to enable the DHCP Server. If you already have a DHCP server on your network, leave the box blank.

Dynamic IP

Client Lease Time: This is the amount of time each network PC will have an IP Address assigned to it before it dynamically changes. The range is 5 ~ 43,200 Minutes.

Range Start/End: Enter a starting IP address and ending IP address to make a range to assign dynamic IPs. The default range is 100~149.

Static IP

The Static IP section of this screen is provided in the event you want the IP Addresses of certain PCs on your network to remain static. In this event, enter the Static IP Address in the space provided, along with that PC's MAC Address.

Click **Add to list** to add a route entry or click **Delete Selected IP** to delete the static route entry.

DNS

For faster access to DNS Servers through the DHCP Server, enter the IP Address of the DNS Servers in the spaces provided.

WINS

Windows Internet Naming Service (WINS) is a service that turns NetBIOS names to IP addresses. Enter the WINS IP Address here. If you do not know the WINS, leave it as 0.

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

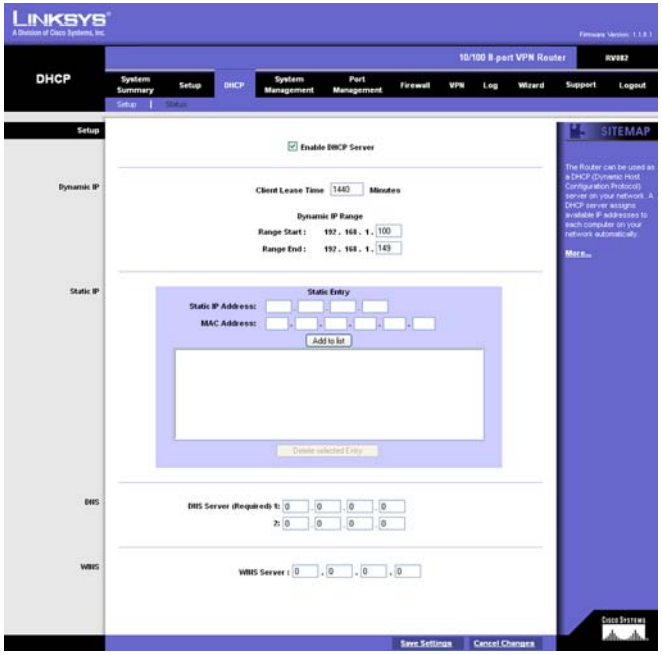


Figure 5-23: DHCP Setup

DHCP Tab - Status

The DHCP Server Status reports the IP of the DHCP Server, the number of Dynamic IP Addresses and Static IP Addresses Used, DHCP Addresses Available and Total Addresses within the Range set.

The Client Table shows the information related to each PC on the network: Client Host Name, IP Address, MAC Address, and Leased Time. Click the **Trash Can** icon to terminate the DHCP lease, releasing the IP Address of the Client Host, or click the **Refresh** button to refresh the Client Table.



Figure 5-24: DHCP Status

System Management Tab - Dual-WAN

Dual-WAN

There are two functions provided for users – Smart Link Backup and Load Balance. If you selected DMZ on the Setup Tab's Network screen (shown in Figure 5-5), you will not be able to set up Dual-WAN.

If Smart Link Backup is selected, you will need to choose which WAN port is the primary, leaving the other as backup. Load Balance automatically manages the Internet connection through both WAN ports.

Network Service Detection

Network Service Detection helps manage your connection and can report when your connection experiences problems. To utilize this service, select **Enable Network Service Detection**. Select **Remove the Connection** if you do not wish to utilize this feature.

Retry Count: If your connection fails, the Router will try to reconnect as many times as you specify in this space.

Retry Timeout: This shows how many times the router will try to make a connection to your ISP before it times out.

When Fail: Should the connection not be reestablished, you can set this to either include this in the system log (by choosing **Generate the Error Condition in the System Log**) or not.

Network Service Detection can either test this using the Default Gateway by pinging the Default Gateway or by pinging a specific IP Address for an ISP Host, Remote Host, or DNS Lookup Host

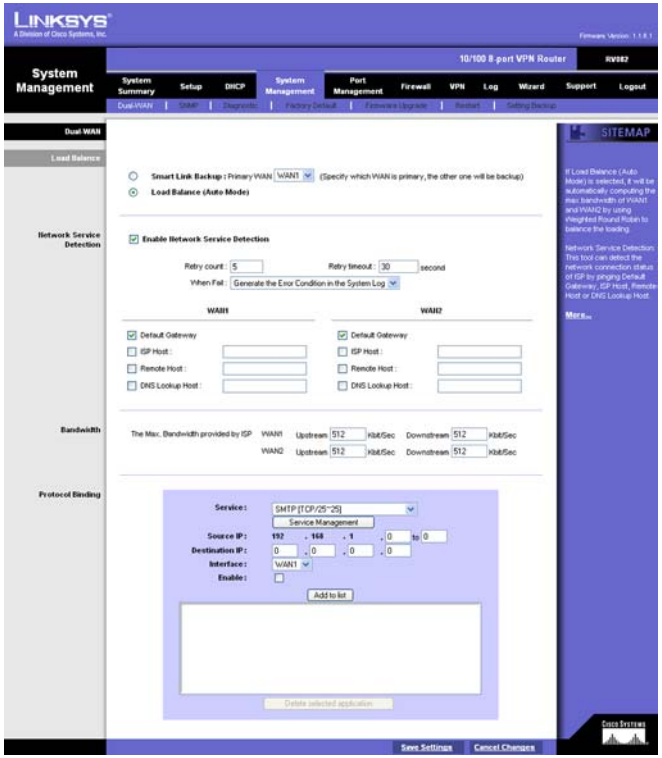


Figure 5-25: System Management Tab - Dual-WAN

Bandwidth

Enter the maximum Bandwidth of Upstreamand Downstream for WAN1 and WAN2, as provided by your ISP.

Protocol Binding

Select a Protocol from the drop-down menu next to **Service** or, if the one you're looking for isn't available, set up a new one by clicking the **Service Management** button. This should be used to specify the IP Address and/or service that will go through a specific WAN port.

To set up a new Service:

1. Select the Service from the pull-down menu, shown in Figure 5-24.
2. If the Service you need is not listed in the menu, please click the **Service Management** button to add the new Service Name, and enter the Protocol and Port Range. This will open the Service Management screen. Click the **Add to List** button. Then, click the **Save Setting** button. Click the **Exit** button.
3. Enter the IP Address of the server that you want the Internet users to access. Then enable the entry.
4. Click the **Add to List** button, and configure as many entries as you would like. You also can **Delete selected application**.

Enter the appropriate Source IP Address and Destination IP Address in the spaces provided. Select the WAN port from the **Interface** drop-down menu. Then, click **Enable**.

Once this is done, click the **Add to list** button and the Service will appear in the box below. To remove this service, click the **Delete selected application** button.

Click the **Save Settings** button to save the Dual-WAN settings or click the **Cancel Changes** button to undo the changes.

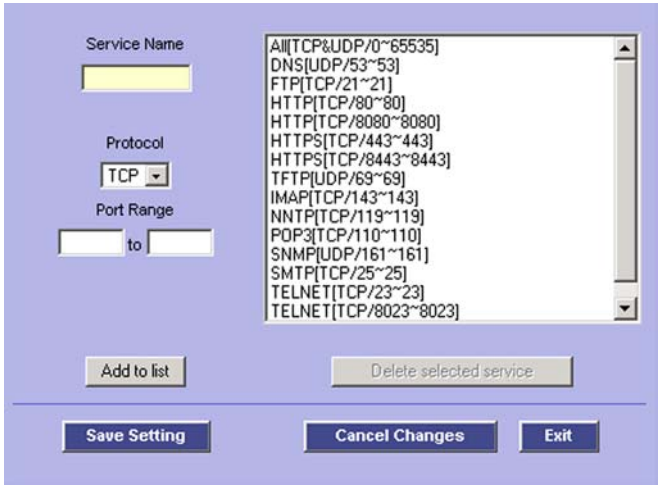


Figure 5-26: Protocol Binding - Service Management

System Management Tab - SNMP

SNMP, or 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. The Router supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups. The appliance replies to SNMP Get commands for MIBII via any interface and supports a custom MIB for generating trap messages. See Figure 5-24.



Figure 5-27: System Management Tab - SNMP

To configure SNMP, enter the necessary information in the following fields:

SNMP Enable: SNMP is enabled by default. To disable the SNMP agent, click this box to remove the check mark.

System Name: Set the hostname far the Router.

System Contact: Enter the name of the network administrator who can be contacted with updates about the Router.

System Location: The network administrator's contact information is placed into this field. Enter an E-mail address, telephone number, or pager number.

Get Community Name: Create a name, no more than 64 alphanumeric characters in length, for a group or community of administrators who can view SNMP data. The default value is “Public”.

Set Community Name: Create a name for a group or community of administrators who can receive SNMP traps, messages regarding the Router’s status. A name of no more than 64 alphanumeric characters long must be entered.

Trap Community Name: Type the Trap Community Name, which is the password sent with each trap to the SNMP manager. A name of no more than 64 alphanumeric characters long must be entered.

Send SNMP Trap to: Enter the IP Address or Domain Name in this field where the Router can send traps.

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

System Management Tab - Diagnostic

The Router has two built-in tools that will help with troubleshooting network problems.

DNS Name Lookup

The Domain Name Service (DNS) allows to look up websites by entering an easily remembered host name, such as www.RV082.com, instead of numerical TCP/IP addresses to access Internet resources. The Router has a DNS lookup tool that will return the numerical TCP/IP address of a host name.

NOTE: The DNS Server's IP address must be entered in the Network page of the Setup Tab (see Figure 5-5) for the DNS Name Lookup feature to function.

Enter the host name in the **Look up the name** field and click the **Go** button. Do not add the prefix "http://", otherwise the search will result in an "Address Resolving Failed" message. The Router will then query the DNS server and display the result below.



Figure 5-28: System Management Tab - DNS Name Lookup

Ping

ping: *an Internet utility used to determine whether a particular IP address is online*

The Ping test bounces a packet of data off an IP Address and back again to the sender. This test shows if the Router is able to contact the remote host. If users on the network are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP's location. If this test is successful, try pinging other IP Addresses. This will show if the problem lies with the ISP's connection or the other IP Address.

NOTE: The Ping test requires an IP address. The Router's DNS Name Lookup tool may be used to find the IP address.

Enter the IP address being pinged and click the **Go** button. The test will take a few seconds to complete. Once completed, a message showing the results will be displayed at the bottom of the Web browser window. The results include Packets transmitted / received / loss and Round Trip Time (Minimum, Maximum, and Average).



Figure 5-29: System Management Tab - Ping

System Management Tab - Factory Default

The *Factory Default* button can be used to clear all of your configuration information and restore the Router to its factory default settings. Only use this feature if you wish to discard all other configuration preferences.

Click the **Return to Factory Default Setting** button if you want to restore the Router to the factory default settings. After clicking the button, another screen, asking if you are sure you want to restore the settings to default will appear. Click **OK** to continue. Another screen will then appear to show that the system is rebooting.



Figure 5-30: System Management Tab - Factory Default

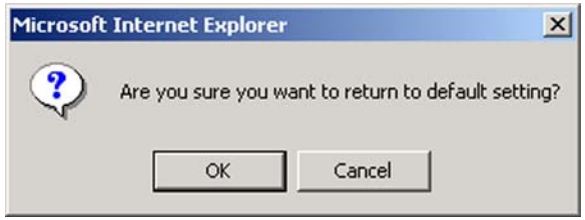


Figure 5-31: Are You Sure

System Management Tab - Firmware Upgrade

download: *to receive a file transmitted over a network*

Firmware Upgrade

Use this function to upgrade the Router's firmware to the newest version. If you have already downloaded the firmware into your computer, then click the **Browse** button to look for the file. Then, click the **Firmware Upgrade Right Now** button.

Firmware Download

Click the **Firmware Download from Linksys Web Site** button to download the Router's Firmware from the Linksys Support page. Select the Router from the pull-down menu and choose the firmware from the options. After downloading the firmware, follow the *Firmware Upgrade* instructions above.



Figure 5-32: System Management Tab - Firmware Upgrade

System Management Tab - Restart

When restarting the Router, you should use this Restart tool. Restarting with this button will send out a log file before the box is reset. Select the **Active Firmware Version** or **Backup Firmware Version**. Click the **Restart Router** button to restart the Router.



Figure 5-33: System Management Tab - Restart

System Management Tab - Setting Backup

From this screen, you can make a backup file of the Router's Preferences.

Import Configuration File:

You will need to specify where your Preferences file is located. Click the **Browse** button and select a Preferences file. This should have been previously saved using the Export button. After you select the file, click the **Import** button. This process may take up to a minute. You will then need to restart the Router in order for the changes to take effect.

Export Configuration File:

Click the **Export** button and choose where you would like to store your Preferences file. This file will be called "RV082.exp" by default, but you may rename it if you wish. This process may take up to a minute.



Figure 5-34: System Management Tab - Setting Backup

Port Management Tab - Port Setup

From this screen, you can configure the connection status for each port, such as Priority, Speed, Duplex and Auto Negotiation.

Basic Per Port Config.

The port information and modifications are displayed according to the following columns.

Port ID: This signifies which port is being configured.

Interface: This column shows the type of port you are configuring.

Disable: Checking this box will disable the corresponding port.

Priority: Select **High** or **Normal** for Port-based QoS (Quality of Service). Port-based QoS is used to maximize network performance and this setting allows you to prioritize performance on eight LAN ports.

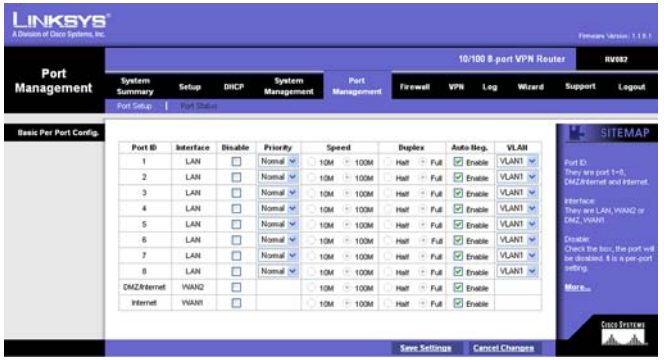


Figure 5-35: Port Management Tab - Port Setup

Speed: This allows you to manually configure the per-port speed as **10Mbps** or **100Mbps**.

Duplex: This configures the port to half-duplex or full-duplex throughput.

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

Auto Negotiation: If enabled, every LAN port will be set as auto negotiated, which will automatically manage speed and throughput.

VLAN: For each LAN port, a VLAN (a Virtual LAN, or network within your network) can be established. Up to eight VLANs can be established.

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

Port Management Tab - Port Status

Users can choose the port number from the pull down menu to see the status of the selected port.

The Summary table will show the settings for the selected port, such as Type, Link Status (up or down), Port Activity (Enabled or Disabled), Priority (High or Normal), Speed Status (10Mbps or 100Mbps), Duplex Status (Half or Full), Auto negotiation (Enabled or Disabled).

The Statistics table will show the port receive/transmit packet count/packet byte count and Port Packet Error Count of the selected port. Click the **Refresh** button to refresh the port status.



Figure 5-36: Port Management Tab - Port Status

Firewall Tab - General

From the Firewall Tab, you can configure the Router to deny or allow users from accessing the Internet or even network servers. You can set up different packet filters for different users within your network based on their network Port number or access from the Internet based on their IP addresses.

Firewall: The Firewall function is enabled by default. If this function is disabled, SPI, DoS, Block WAN Request will also be disabled. Remote Management will be enabled and Access Rules and Content Filter will be disabled.

SPI (Stateful Packet Inspection): The Router's Firewall uses Stateful Packet Inspection to maintain connection information that passes through the firewall. It will inspect all packets based on the established connection, prior to passing the packets for processing through a higher protocol layer.

DoS (Denial of Service): Protect internal networks from Internet attacks, such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing and reassembly attacks.

Block WAN Request: This feature is designed to prevent attacks through the Internet. When it is enabled, the Router will drop both the unaccepted TCP request and ICMP packets from the WAN side. The hacker will not find the Router by pinging the WAN IP address. If DMZ is enabled, this function will be disabled.

Remote Management: This Router supports remote management. If you want to manage this Router through the WAN connection, click **Enable**. Then, specify which port you wish to use for remote management (eg. 80 or 8080).

HTTPS: Enabling this function allows remote login to the Router using SSL as well as remote access to your network through the Linksys QuickVPN software will be available.

Multicast Pass Through: IP Multicasting occurs when a single data transmission is sent to multiple recipients at the same time. Using this feature, the Router allows IP multicast packets to be forwarded to the appropriate computers.

MTU (Maximum Transmission Unit): This feature is enabled by default and should remain enabled. It specifies the largest packet size permitted for network transmission. The default of MTU size is 1500 bytes.

Restrict WEB features

Select which type of Internet feature - **Java**, **Cookies**, **ActiveX**, or **Access to HTTP Proxy Servers** - you would like to restrict by click on the box beside them. If you would like to leave trusted sites unblocked, click **Don't Block Java/ActiveX/Cookies/Proxy To Trusted Domains**.



Figure 5-37: Firewall Tab - General

multicasting: *sending data to a group of destinations at once*

Firewall Tab - Access Rules



Figure 5-38: Firewall Tab - Access Rules

Network Access Rules evaluate the network traffic's Source IP address, Destination IP address, and IP protocol type to decide if the IP traffic is allowed to pass through the firewall.

When defining Network Access Rules, remember that it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting Network Access Rules. Custom rules can be created to override Default Rules, but there are four default rules that will be always active, and custom rules cannot override these four rules. These are:

* HTTP service from LAN side to RV082 is always allowed.
* DHCP service from LAN side is always allowed.
* DNS service from LAN side is always allowed.
* Ping service from LAN side to RV082 is always allowed.

The Network Access Rules are broken into a table, with these features:

Jump to: Select from this pull-down menu which page of Rules you wish to display.

Entries Per Page: From this pull-down menu, you can select how many entries will be displayed per page.

Priority: This shows, depending upon the number of Rules entered, the numeric order of Rules having higher or lower priority.

Enable: Enable or disable Rules by clicking on the corresponding box.

Action: Allow or Deny traffic to or from specific network or Internet destinations.

Service: This shows the services on your network to which this Rule will apply?

Source Interface: This shows to which port this rule applies.

Source: Displays the source of the traffic affected by the Rule. For instance, if the source of the traffic is on your network, this will display *LAN*. *Any* means that the traffic can originate from any source.

Destination: Displays the destination of the traffic affected by the Rule. For instance, if the destination of the traffic is your network, this will display LAN. Any means that the traffic can go to any destination.

Time: This displays the hours (in military time) during which the Rules apply.

Day: This displays the day(s) on which the Rule applies.

Edit: Clicking the **Edit** button will open the Add a New Access Rule screen, where you can edit any of the Rule's settings.

Delete: Clicking the **TrashCan** icon will delete this Rule.

Click the **Restore to Default Rules** to restore the Network Access Rules to their default settings. To add a new Network Access Rule and open the *Add a New Access Rule* screen, click the **Add New Rule** button.

Add a New Access Rule

Services

This screen allows you to set Access Rules, either through a Wizard, by clicking the Wizard button, or directly on this screen, by entering the information in the spaces provided.

Services: Click **Wizard** to run the Access Rule Setup Wizard. To view the figures for the Access Rule Setup Wizard, see Figure 5-65.

Action: Select **Allow** or **Deny** from the pull-down menu, depending on if you'd like to allow or deny access.

Service: Select the service from the Service pull-down menu. If the service you need is not listed in the menu, click the **Service Management** button to add a new Service. Enter the Service Name, Protocol and Port Range, and then click **Add to list**.

Source Interface: Select the source to which this service will apply. **WAN** sources are over the Internet. **LAN** sources are within your network.

Source/Destination IP: For network sources and destinations, select **Single** for a single IP Address, and enter it. For sources over the Internet, select **Range** for a range of IP Addresses, and enter that range. If you select ANY, this source could be over a LAN, WAN, or DMZ.

Scheduling

Here you can select when this rule will apply, how often, and even at what specific times.

Click the **Return** button to return to the previous screen. Click the **Save Settings** button to save the Service Management settings or click the **Cancel Changes** button to undo your changes. When your settings are correct, a screen will let you know that settings are successful.



Figure 5-39: Firewall Tab - Add a New Access Rule



Figure 5-40: Settings are Successful

Editing an Access Rule

To Edit an Access Rule, click the Edit button on the Access Rule screen. The Edit screen looks very much like the screen for adding a new Access Rule. Enter your changes and click the **Save Settings** button to save the Service Management settings or click the **Cancel Changes** button to undo your changes. When your settings are correct, a screen will let you know that settings are successful. Click the **Return** button to return to the previous screen.

Firewall Tab - Content Filter

Forbidden Domains

This allows to you increase network security by blocking websites those in your network can access. Click the **Block Forbidden Domains** box to enable this function. Then, enter in the IP Address(es) for those websites you wish to restrict, clicking the **Add to List** button after you enter each IP Address.

Website Blocking by Keywords

This allows a further increase to network security by blocking websites that use keywords, designated by you in this list. Click the **Enable Website Blocking by Keywords** box to enable this function. Then, enter in the keyword(s) you wish your network to restrict access by, clicking the **Add to List** button after you enter each keyword.

Scheduling

Here you can select when this rule will apply, how often, and even at what specific times.

Click the **Save Settings** button when you finish the Content Filter settings, or click the **Cancel Changes** button to undo your changes.

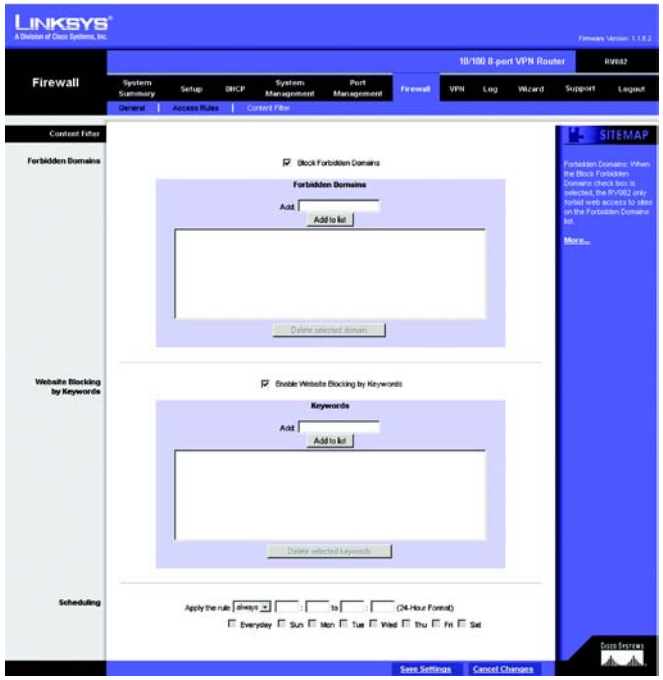


Figure 5-41: Firewall Tab - Content Filter

VPN Tab - Summary

Summary

The VPN Summary displays summary information about the VPN (Virtual Private Network), along with the Tunnel Status, GroupVPN Status, and VPN Clients Status.

Summary: It shows the number of Tunnel(s) Used and Tunnel(s) Available. The 10/100 8-Port VPN Router supports 50 tunnels.

Detail: Click the **Detail** button to see detail of the VPN Summary.

Tunnel Status:

Add New Tunnel: Click the **Add New Tunnel** button to add a Gateway to Gateway or Client to Gateway tunnel. Select the type of tunnel you'd like to add from the *Mode Choose* screen (shown in Figure 5-44). A Gateway to Gateway tunnel is created between two VPN routers. A Client to Gateway tunnel is created between the 10/100 8-Port VPN Router and a PC using the Linksys VPN Client Software. Click the **Add Now** button, which will open the appropriate screen for setting up that type of tunnel.

From this section, you can jump to different pages of tunnels and also select how many tunnels you would like listed per page. These tunnels will then be displayed here, with the following information about each tunnel:

Tunnel No.: As the tunnels are listed here, they are put in order, 1~50.

Tunnel Name: This is the Tunnel Name or Group ID Name that you entered when creating the tunnel.

Status: This will show the status of the tunnel, whether it is Connected, Hostname Resolution Failed, Resolving Hostname or Waiting for Connection. If you select Manual on the IPSec Setup page, this will show Manual or no Tunnel Test function for Manual Keying Mode.

Phase2 Encrypt/Auth/Group: This will show the Encryption type (DES/3DES), Authentication type (MD5/SHA1) and Group (1/2/5) selected from the IPSec Setup sections of the *Gateway to Gateway* and *Client to Gateway* screens. If you chose Manual mode, this field will show the Encryption and Authentication method set up in Manual mode.

Local Group: This will show the IP address and subnet mask of the Local Group.

Remote Group: This will show the IP address and subnet mask of the Remote Group.

Remote Gateway: This will show the IP address of the Remote Gateway.



Figure 5-42: VPN Tab - Summary

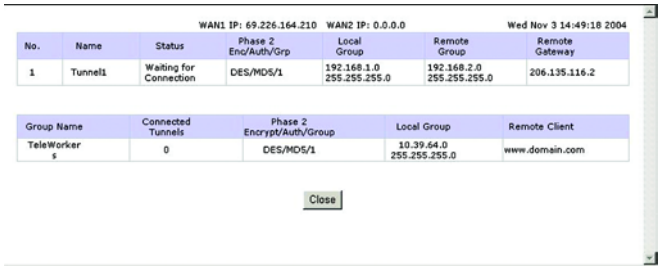


Figure 5-43: VPN Tab - Summary Detail

Tunnel Test: Click the **Connect** button to verify the tunnel status. The test result will be updated in Status. If the tunnel is connected, a *Disconnect* button will be available so you can disconnect the VPN connection.

Configure: This includes options for editing the tunnel, by clicking **Edit**, or deleting the tunnel, by clicking the **Trash Can**.

Tunnel(s) Enable and **Tunnel(s) Defined**: This will show the amount of tunnels enabled and tunnels defined.

GroupVPN Status:

This section displays the status of VPN tunnels created with the Linksys VPN Client Software. These tunnels will then be displayed here, with the following information about each tunnel:

Group Name: This will show the name you entered when creating the Client to Gateway tunnel.

Connected Tunnels: This will show the number of users logged in to the Group VPN.

Phase2 Encrypt/Auth/Group: This will show the Encryption (DES/3DES), Authentication (MD5/SHA1) and Group (1/2/5) selected from the IPSec Setup sections of the *Gateway to Gateway* and *Client to Gateway* screens.

Local Group: This will show the IP address and Subnet Mask of the Local Group set up.

Remote Client: This column will show the remote client authentication type that is used for this specific GroupVPN.

Remote Clients Status: Clicking **Detail List** will display the Group Name, IP address and Connection Time of this Group VPN.

Tunnel Test: Click the **Connect** button to verify the tunnel status. The test result will be updated in Status. If the tunnel is connected, a *Disconnect* button will be available so you can disconnect the VPN connection.

Configure: This includes options for editing the tunnel, by clicking **Edit**, or deleting the tunnel, by clicking the **Trash Can**.

VPN Clients Status:

This section identifies each user logged onto your network through the Linksys VPN Client software, and will display the status of their connection, along with how long and when they connected and disconnected. If you'd like to disconnect any user, select the box in the Disconnect column and then click the **Disconnect** button.



Figure 5-44: VPN Tab - Mode Choose

VPN Tab - Gateway to Gateway

This screen allows you to create VPN tunnels between VPN routers. You can reach this page by clicking the Gateway to Gateway tab or from the Mode Choose screen (figure 5-44).

Tunnel No.: This shows the number assigned to this tunnel, from 1~50, depending on how many tunnels you have already set up.

Tunnel Name: Enter the Tunnel Name, such as LA Office, Branch Site, Corporate Site, etc. 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.

Interface: All VPN tunnels go out through one of the Router's WAN ports. When Dual-WAN is enabled, you will have the option of two ports: WAN1 or WAN2.

Enable: Checking this box enables the VPN tunnel you're creating.

Local Group Setup

The Local Group Setup section configures the local settings for the VPN tunnel you are creating. Remember, all settings for the Local Group must be exactly the same as those for the Remote Group.

Local Security Gateway Type: There are five types. They are **IP Only**, **IP + Domain Name (FQDN) Authentication**, **IP + E-mail Addr. (USER FQDN) Authentication**, **Dynamic IP + Domain Name (FQDN) Authentication**, **Dynamic IP + E-mail Addr. (USER FQDN) Authentication**. The type of Local Security Gateway Type must match the Remote Security Gateway Type of VPN devices in the other end of tunnel. The first three options are easier to use because the IP Addresses are static and do not change.

IP Only: If you select IP Only, only the specific IP Address set will be able to access the tunnel. The Router's WAN IP address (set above) will automatically appear in this field.

IP + Domain Name (FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

IP + E-mail Addr. (USER FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same email. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

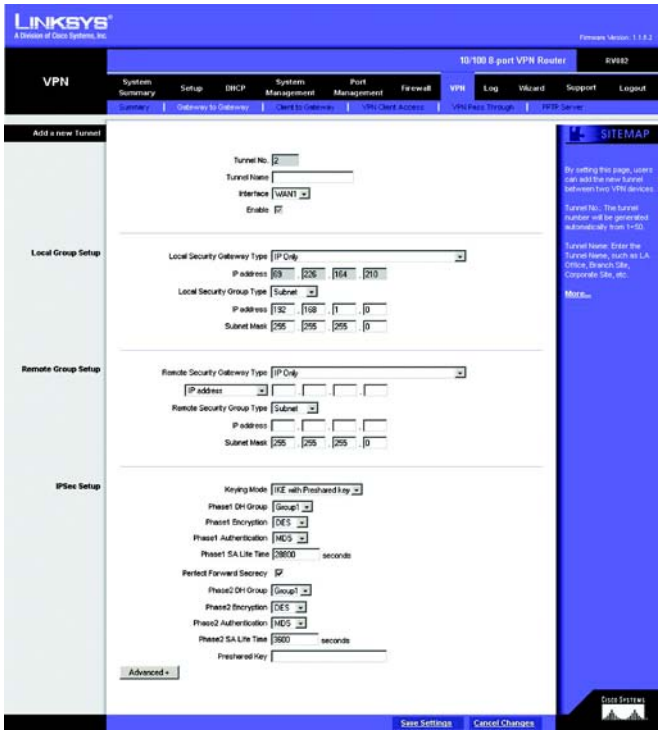


Figure 5-45: VPN tab - Gateway to Gateway

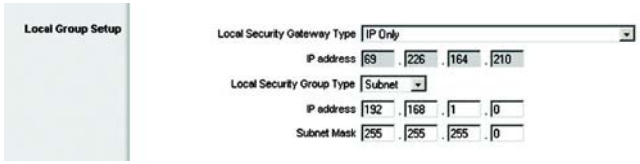


Figure 5-46: VPN tab - Gateway to Gateway Local Group Setup

Dynamic IP + Domain Name (FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of a domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of an email address. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Local Security Group Type. Select the local LAN user(s) that can use this VPN tunnel. Local Security Group Type may be a single IP address, a Subnet or an IP address range. The Local Secure Group must match the Remote Secure Group on the other end of the tunnel. Selecting **IP Address** allows only one computer, with the specific IP Address, access to the tunnel. (The default IP is 192.168.1.0.) If you select **Subnet**, all computers on the local subnet can access the tunnel. The default IP is 192.168.1.0, and default Subnet Mask is 255.255.255.192. If you select **IP Range**, you can specify a range of IP Addresses to access the tunnel. The default IP Range is 192.168.1.0~254.

Remote Group Setup:

The Remote Group Setup section configures the remote settings for the VPN tunnel you are creating. Remember, all settings for the Remote Group must be exactly the same as those for the Local Group.

Remote Security Gateway Type: There are five types. They are **IP Only**, **IP + Domain Name (FQDN) Authentication**, **IP + E-mail Addr. (USER FQDN) Authentication**, **Dynamic IP + Domain Name (FQDN) Authentication**, **Dynamic IP + E-mail Addr. (USER FQDN) Authentication**. The type of Remote Security Gateway Type must match the Local Security Gateway Type of VPN devices in the other end of tunnel. The first three options are easier to use because the IP Addresses are static and do not change.

IP Only: If you select IP Only, only the specific IP Address that you enter will be able to access the tunnel. It's the IP Address of the remote VPN Router or device which you wish to communicate. The remote VPN device can be another VPN Router or a VPN Server. If you know the static IP address of remote VPN device, select IP address from drop-down menu. If you don't know the static IP address of remote VPN device, but the domain name of remote VPN device is known, you can select IP by DNS Resolved, and enter the real domain name on the Internet. RV082 will get the IP address of remote VPN device by DNS Resolved, and IP address of remote VPN device will be displayed on VPN Status of Summary page.

IP + Domain Name (FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

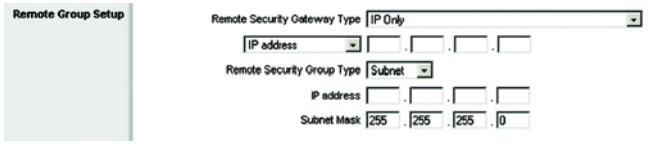


Figure 5-47: VPN tab - Gateway to Gateway Remote Group Setup

IP + E-mail Addr. (USER FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same email. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + Domain Name (FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of a domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of an email address. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Remote Security Group Type. Select the local LAN user(s) that can use this VPN tunnel. Remote Security Group Type may be a single IP address, a Subnet or an IP address range. The Remote Secure Group must match the Local Secure Group on the other end of the tunnel. Selecting **IP Address** allows only one computer, with the specific IP Address, access to the tunnel. (The default IP is 192.168.1.0.) If you select **Subnet**, all computers on the local subnet can access the tunnel. The default IP is 192.168.1.0, and default Subnet Mask is 255.255.255.192. If you select **IP Range**, you can specify a range of IP Addresses to access the tunnel. The default IP Range is 192.168.1.0~254.

IPSec Setup

In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a “key” to the encryption code. There are two Keying Modes of key management, Manual and IKE with Preshared Key (automatic).

Manual

If you select **Manual**, you generate the key yourself, and no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes. Both sides must use the same Key Management method.

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

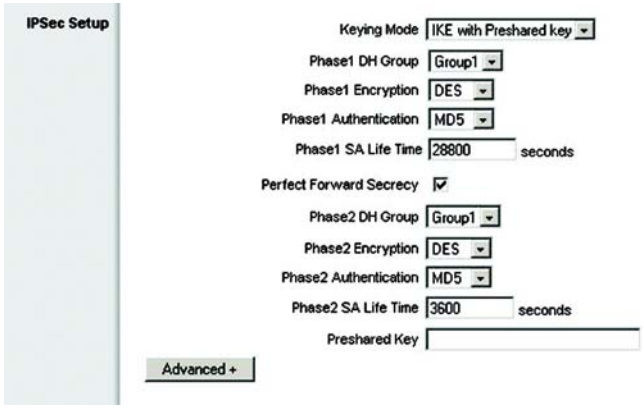


Figure 5-48: VPN tab - Gateway to Gateway IPSec Setup

Bit: *a binary digit*

Encryption: There are two methods of encryption, DES and 3DES. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure, and both sides must use the same Encryption method.

Authentication: There are two methods of authentication, MD5 and SHA. The Authentication method determines a method to authenticate the ESP packets. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure, and both sides must use the same Authentication method.

Encryption Key: This field specifies a key used to encrypt and decrypt IP traffic, and the Encryption Key is generated yourself. The hexadecimal value is acceptable in this field. Both sides must use the same Encryption Key. If DES is selected, the Encryption Key is 16-bit. If users do not fill up to 16-bit, this field will be filled up to 16-bit automatically by 0. If 3DES is selected, the Encryption Key is 48-bit. If users do not fill up to 48-bit, this field will be filled up to 48-bit automatically by 0.

Authentication Key: This field specifies a key used to authenticate IP traffic and the Authentication Key is generated yourself. The hexadecimal value is acceptable in this field. Both sides must use the same Authentication key. If MD5 is selected, the Authentication Key is 32-bit. If users do not fill up to 32-bit, this field will be filled up to 32-bit automatically by 0. If SHA1 is selected, the Authentication Key is 40-bit. If users do not fill up to 40-bit, this field will be filled up to 40-bit automatically by 0.

IKE with Preshared Key (automatic)

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

Phase 1 DH Group: Phase 1 is used to create a security association (SA). DH (Diffie-Hellman) is a key exchange protocol that used during phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1,024 bits and Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.

Phase 1 Encryption: There are two methods of encryption, DES and 3DES. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. Both sides must use the same Encryption method. 3DES is recommended because it is more secure.

Phase 1 Authentication: There are two methods of authentication, MD5 and SHA. The Authentication method determines a method to authenticate the ESP packets. Both sides must use the same Authentication method. MD5 is a one-way hashing algorithm that produces a 128-bit digest.

SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure, and both sides must use the same Authentication method.

Phase 1 SA Life Time: This field allows you to configure the length of time a VPN tunnel is active in Phase 1. The default value is **28,800** seconds.

Perfect Forward Secrecy: If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. If PFS is enabled, a hacker using brute force to break encryption keys is not able to obtain other or future IPSec keys.

Phase 2 DH Group: There are three groups of different prime key lengths. Group1 is 768 bits, Group2 is 1,024 bits and Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You can choose the different Group with the Phase 1 DH Group you chose. If Perfect Forward Secrecy is disabled, there is no need to setup the Phase 2 DH Group since no new key generated, and the key of Phase 2 will be same with the key in Phase 1.

Phase 2 Encryption: Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. There are two methods of encryption, DES and 3DES. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. Both sides must use the same Encryption method. If users enable the AH Hash Algorithm in Advanced, then it is recommended to select **Null** to disable encrypting/decrypting ESP packets in Phase 2, but both sides of the tunnel must use the same setting.

Phase 2 Authentication: There are two methods of authentication, MD5 and SHA. The Authentication method determines a method to authenticate the ESP packets. Both sides must use the same Authentication method. MD5 is a one-way hashing algorithm that produces a 128-bit digest. If users enable the AH Hash Algorithm in Advanced, then it is recommended to select **Null** to disable authenticating ESP packets in Phase 2, but both sides of the tunnel must use the same setting.

Phase 2 SA Life Time: This field allows you to configure the length of time a VPN tunnel is active. The default value is 3,600 seconds.

Preshared Key: Use character and hexadecimal values in this field, e.g. “My_@123” or “4d795f40313233.” The max entry of this field is 30-digit. Both sides must use the same Pre-shared Key. It’s recommended to change Preshared keys regularly to maximize VPN security.

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

Advanced

For most users, the settings on the VPN page should be satisfactory. This device provides an advanced IPSec setting page for some special users such as reviewers. Click the **Advanced** button to link you to that page. Advanced settings are only for IKE with Preshared Key mode of IPSec.

Aggressive Mode: There are two types of Phase 1 exchanges: Main mode and Aggressive mode.

Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, select Main mode. When users select the Dynamic IP in Remote Security Gateway Type, it will be limited as Aggressive Mode.

Compress (Support IP Payload compression Protocol (IP Comp)

The Router supports IP Payload Compression Protocol. IP Payload Compression is a protocol to reduce the size of IP datagrams. If Compress is enabled, the Router will propose compression when initiating a connection. If the responders reject this propose, the Router will not implement the compression. When the Router works as a responder, the Router will always accept compression even without enabling compression.

Keep-Alive: This mechanism helps to keep up the connection of IPSec tunnels. Whenever a connection is dropped and detected, it will be re-established immediately.

AH Hash Algorithm: AH (Authentication Header) protocol describe the packet format and the default standards for packet structure. With the use of AH as the security protocol, protected is extended forward into IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. There are two algorithms, MD5 and SHA1. MD5 produces a 128-bit digest to authenticate packet data and SHA1 produces a 160-bit digest to authenticate packet data. Both sides of the tunnel should use the same algorithm.

NetBIOS broadcast: Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, RV082 blocks these broadcasts.

Dead Peer Detection (DPD): When DPD is enabled, the RV082 will send the periodic HELLO/ACK messages to prove the tunnel liveliness when both peers of VPN tunnel provide DPD mechanism. Once a dead peer has detected, the RV082 will disconnect the tunnel so the connection can be re-established.

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

VPN Tab - Client to Gateway

With Tunnel Enabled

This screen allows you to create VPN tunnels from remote PCs (with Linksys VPN Client Software) to VPN routers. You can reach this page by clicking the Client to Gateway tab or from the Mode Choose screen (figure 5-44).

Tunnel No.: This shows the number assigned to this tunnel, from 1~5, depending on how many tunnels you have already set up.

Tunnel Name: Enter the Tunnel Name, such as LA Office, Branch Site, Corporate Site, etc. 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.

Interface: All VPN tunnels go out through one of the Router's WAN ports. When Dual-WAN is enabled, you will have the option of two ports: WAN1 or WAN2.

Enable: Checking this box enables the VPN tunnel you're creating.

Local Group Setup

The Local Group Setup section configures the local settings for the VPN tunnel you are creating. Remember, all settings for the Local Group must be exactly the same as those for the Remote Group.

Local Security Gateway Type: There are five types. They are **IP Only**, **IP + Domain Name (FQDN) Authentication**, **IP + E-mail Addr. (USER FQDN) Authentication**, **Dynamic IP + Domain Name (FQDN) Authentication**, **Dynamic IP + E-mail Addr. (USER FQDN) Authentication**. The type of Local Security Gateway Type must match the Remote Security Gateway Type of VPN devices in the other end of tunnel. The first three options are easier to use because the IP Addresses are static and do not change.

IP Only: If you select IP Only, only the specific IP Address set will be able to access the tunnel. The Router's WAN IP address (set above) will automatically appear in this field.

IP + Domain Name (FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

IP + E-mail Addr. (USER FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same email. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + Domain Name (FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of a domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of an email address. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

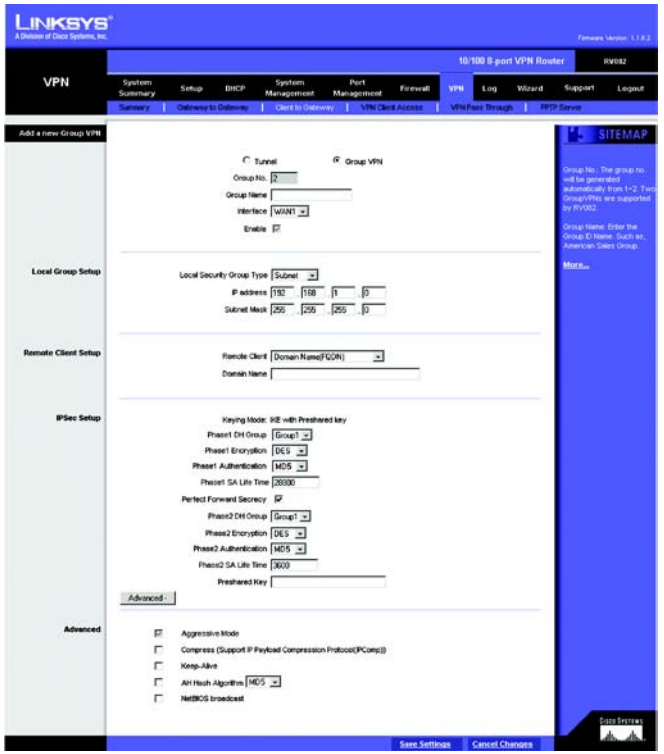


Figure 5-49: VPN tab - Client to Gateway

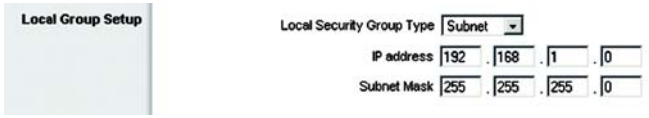


Figure 5-50: VPN tab - Client to Gateway Local Group Setup

Local Security Group Type. Select the local LAN user(s) that can use this VPN tunnel. Local Security Group Type may be a single IP address, a Subnet or an IP address range. The Local Secure Group must match the Remote Secure Group on the other end of the tunnel. Selecting **IP Address** allows only one computer, with the specific IP Address, access to the tunnel. (The default IP is 192.168.1.0.) If you select **Subnet**, all computers on the local subnet can access the tunnel. The default IP is 192.168.1.0, and default Subnet Mask is 255.255.255.192. If you select **IP Range**, you can specify a range of IP Addresses to access the tunnel. The default IP Range is 192.168.1.0~254.

Remote Group Setup:

The Remote Group Setup section configures the remote settings for the VPN tunnel you are creating. Remember, all settings for the Remote Group must be exactly the same as those for the Local Group.

Remote Security Gateway Type: There are five types. They are **IP Only**, **IP + Domain Name (FQDN) Authentication**, **IP + E-mail Addr. (USER FQDN) Authentication**, **Dynamic IP + Domain Name (FQDN) Authentication**, **Dynamic IP + E-mail Addr. (USER FQDN) Authentication**. The type of Remote Security Gateway Type must match the Local Security Gateway Type of VPN devices in the other end of tunnel. The first three options are easier to use because the IP Addresses are static and do not change.

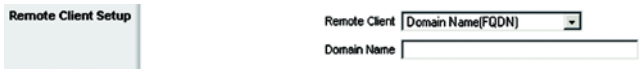


Figure 5-51: VPN tab - Client to Gateway Remote Group Setup

IP Only: If you select IP Only, only the specific IP Address that you enter will be able to access the tunnel. It's the IP Address of the remote VPN Router or device which you wish to communicate. The remote VPN device can be another VPN Router or a VPN Server. If you know the static IP address of remote VPN device, select IP address from drop-down menu. If you don't know the static IP address of remote VPN device, but the domain name of remote VPN device is known, you can select IP by DNS Resolved, and enter the real domain name on the Internet. RV082 will get the IP address of remote VPN device by DNS Resolved, and IP address of remote VPN device will be displayed on VPN Status of Summary page.

IP + Domain Name (FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

IP + E-mail Addr. (USER FQDN) Authentication: This selection affords a greater amount of security because each side of the tunnel must use the same IP Address as well as the same email. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + Domain Name (FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of a domain name. Only one domain name can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication: This setting uses a dynamic IP address, which is constantly changing. In addition, the tunnel is confirmed through use of an email address. Only one email address can be used for one tunnel and may not be applied to another tunnel.These settings must match the Remote Group Setup on the other end of the tunnel.

Remote Security Group Type. Select the local LAN user(s) that can use this VPN tunnel. Remote Security Group Type may be a single IP address, a Subnet or an IP address range. The Remote Secure Group must match the Local Secure Group on the other end of the tunnel. Selecting **IP Address** allows only one computer, with the specific IP Address, access to the tunnel. (The default IP is 192.168.1.0.) If you select **Subnet**, all computers on the local subnet can access the tunnel. The default IP is 192.168.1.0, and default Subnet Mask is 255.255.255.192. If you select **IP Range**, you can specify a range of IP Addresses to access the tunnel. The default IP Range is 192.168.1.0~254.

With Group VPN enabled:

Further Remote Client Setup options become available when you select GroupVPN. There are three types of Remote Client: **Domain Name (FQDN)**, **E-mail Address (User FQDN)**, and **Microsoft XP/2000 VPN Client**.

Domain Name (FQDN) (Fully Qualified Domain Name): Enter the Domain Name of the Remote Client. When the Remote Client requests to create a tunnel with the Router, the Router will act as a responder. The Domain Name must match the local settings of the Remote Client.

E-mail Address (User FQDN): Enter the Email Address of the Remote Client. When the Remote Client requests to create a tunnel with the Router, the Router will act as a responder. The Email Address must match the local settings of the Remote Client.

Microsoft XP/2000 VPN Client: This option is used for Dynamic IP users (e.g. PPPoE or DHCP) which using Microsoft VPN client. The difference between Microsoft and other VPN client is that Microsoft client does not support Aggressive mode and FQDN/USER FQDN ID options.

IPSec Setup

In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a “key” to the encryption code. There are two Keying Modes of key management, Manual and IKE with Preshared Key (automatic). If GroupVPN is enabled, the key management will be IKE with Preshared Key only.

Manual

If you select **Manual**, you generate the key yourself, and no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes. Both sides must use the same Key Management method.

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

Encryption: There are two methods of encryption, DES and 3DES. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure, and both sides must use the same Encryption method.

Authentication: There are two methods of authentication, MD5 and SHA. The Authentication method determines a method to authenticate the ESP packets. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure, and both sides must use the same Authentication method.

Encryption Key: This field specifies a key used to encrypt and decrypt IP traffic, and the Encryption Key is generated yourself. The hexadecimal value is acceptable in this field. Both sides must use the same Encryption Key. If DES is selected, the Encryption Key is 16-bit. If users do not fill up to 16-bit, this field will be filled up to 16-bit automatically by 0. If 3DES is selected, the Encryption Key is 48-bit. If users do not fill up to 48-bit, this field will be filled up to 48-bit automatically by 0.

Authentication Key: This field specifies a key used to authenticate IP traffic and the Authentication Key is generated yourself. The hexadecimal value is acceptable in this field. Both sides must use the same Authentication key. If MD5 is selected, the Authentication Key is 32-bit. If users do not fill up to 32-bit, this field will be filled up to 32-bit automatically by 0. If SHA1 is selected, the Authentication Key is 40-bit. If users do not fill up to 40-bit, this field will be filled up to 40-bit automatically by 0.

IKE with Preshared Key (automatic)

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

Phase 1 DH Group: Phase 1 is used to create a security association (SA). DH (Diffie-Hellman) is a key exchange protocol that is used during phase 1 of the authentication process to establish pre-shared keys. There are three

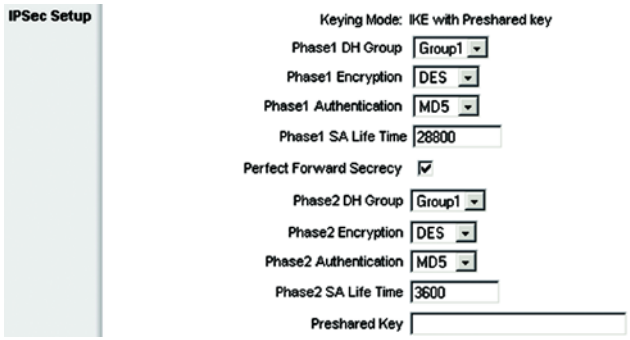


Figure 5-52: VPN tab - Client to Gateway IPSec Setup

groups of different prime key lengths. Group 1 is 768 bits, Group 2 is 1,024 bits and Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.

Phase 1 Encryption: There are two methods of encryption, DES and 3DES. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. Both sides must use the same Encryption method. 3DES is recommended because it is more secure.

Phase 1 Authentication: There are two methods of authentication, MD5 and SHA. The Authentication method determines a method to authenticate the ESP packets. Both sides must use the same Authentication method. MD5 is a one-way hashing algorithm that produces a 128-bit digest.

SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure, and both sides must use the same Authentication method.

Phase 1 SA Life Time: This field allows you to configure the length of time a VPN tunnel is active in Phase 1. The default value is **28,800** seconds.

Perfect Forward Secrecy: If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. If PFS is enabled, a hacker using brute force to break encryption keys is not able to obtain other or future IPSec keys.

Phase 2 DH Group: There are three groups of different prime key lengths. Group1 is 768 bits, Group2 is 1,024 bits and Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You can choose the different Group with the Phase 1 DH Group you chose. If Perfect Forward Secrecy is disabled, there is no need to setup the Phase 2 DH Group since no new key generated, and the key of Phase 2 will be the same with the key in Phase 1.

Phase 2 Encryption: Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. There are two methods of encryption, DES and 3DES. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. Both sides must use the same Encryption method. If users enable the AH Hash Algorithm in Advanced, then it is recommended to select **Null** to disable encrypting/decrypting ESP packets in Phase 2, but both sides of the tunnel must use the same setting.

Phase 2 Authentication: There are two methods of authentication, MD5 and SHA. The Authentication method determines a method to authenticate the ESP packets. Both sides must use the same Authentication method. MD5 is a one-way hashing algorithm that produces a 128-bit digest. If users enable the AH Hash Algorithm in Advanced, then it is recommended to select **Null** to disable authenticating ESP packets in Phase 2, but both sides of the tunnel must use the same setting.

Phase 2 SA Life Time: This field allows you to configure the length of time a VPN tunnel is active. The default value is 3,600 seconds.

Preshared Key: Character and hexadecimal values are acceptable in this field, e.g. "My_@123" or "4d795f40313233." The max entry of this field is 30-digit. Both sides must use the same Pre-shared Key. It's recommended to change Preshared keys regularly to maximize VPN security.

Click the **Save Settings** button to save the settings or click the **Cancel Change**s button to undo the changes.

Advanced

For most users, the settings on the VPN page should be satisfactory. This device provides an advanced IPSec setting page for some special users such as reviewers. Click the **Advanced** button to link you to that page. Advanced settings are only for IKE with Preshared Key mode of IPSec.

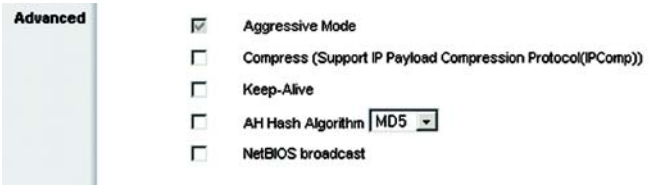


Figure 5-53: VPN tab - Client to Gateway Advanced

Aggressive Mode: There are two types of Phase 1 exchanges: Main mode and Aggressive mode.

Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, select Main mode. If network speed is preferred, select Aggressive mode. When Group VPN is enabled, it will be limited as Aggressive Mode. If you select Dynamic IP in Remote Client Type in tunnel mode, it will also be limited as Aggressive Mode.

Compress (Support IP Payload compression Protocol (IP Comp)

The Router supports IP Payload Compression Protocol. IP Payload Compression is a protocol to reduce the size of IP datagrams. If Compress is enabled, the Router will propose compression when initiating a connection. If the responders reject this propose, the Router will not implement the compression. When the Router works as a responder, the Router will always accept compression even without enabling compression.

Keep-Alive: This mechanism helps to keep up the connection of IPSec tunnels. Whenever a connection is dropped and detected, it will be re-established immediately.

AH Hash Algorithm: AH (Authentication Header) protocol describes the packet format and the default standards for packet structure. With the use of AH as the security protocol, protected is extended forward into IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. There are two algorithms, MD5 and SHA1. MD5 produces a 128-bit digest to authenticate packet data and SHA1 produces a 160-bit digest to authenticate packet data.

NetBIOS broadcast: Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, RV082 blocks these broadcasts.

Dead Peer Detection (DPD): When DPD is enabled, the RV082 will send the periodic HELLO/ACK messages to prove the tunnel liveliness when both peers of VPN tunnel provide DPD mechanism. Once a dead peer has detected, the RV082 will disconnect the tunnel so the connection can be re-established.

The Interval is the number of seconds between DPD messages. The default is DPD enabled, and default Interval is 10 seconds.

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

VPN Tab - VPN Client Access

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



Figure 5-54: VPN tab - VPN Client Access

Username: Enter the user's name here.
New Password: Enter the user's password here.
Confirm New Password: Confirm that password by re-entering it here.
Change Password Allowed: If you want to allow users the right to change their password, click the radio button beside **Yes**. If not, click the radio button beside **No**.
Active: Clicking this box will make the new user active.
Add to List: Clicking this button adds the user to the list at the bottom of the screen.

All of these settings can be changed by clicking the user's name in the box at the bottom half of the screen. The *Add to List* button changes to *Update this user.* Click the **Update this user** button to change the user's settings.

Delete selected users: You can delete users by clicking their name(s) in the list and then clicking the Delete selected users button. Hold down the CTRL key when selecting multiple users.
Add New: Clicking this button also allows you to add new users to the VPN Client Access list.

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

When you first save these settings, a message will appear, asking if you'd like the Router to automatically change the LAN IP Address to prevent conflicting IP addresses. Clicking **Yes** will change the LAN IP Address. In the event of an IP conflict, the VPN Client will not connect to the Router.

VPN Tab - VPN Pass Through

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

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

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



Figure 5-55: VPN tab - VPN Pass Through

VPN Tab - PPTP Server

The PPTP Server is intended for users logging in remotely with Windows XP or 2000, using PPTP to create VPN connections.

Enable PPTP Server: Checking this box enables the PPTP Server.

IP Address Range

Enter the internal IP Address Range for remote users connecting to your Local Network. The Router supports up to five PPTP connections. The default IP range is 200 ~ 204.

Users Setting

Enter the remote users' User Name and Password. Then, enter the password in the *Confirm the Password* field and click the **Add to list** button. When remote users request to create VPN connections with the Router, the PPTP Server will identify the users' information. The Router will support up to such connections.

To delete users from the list, select the user and click the **Delete selected users** button.

Connection List
This list will show all users connected through the PPTP Server, with their User Name, Remote Address and PPTP IP Address displayed on the list.

Click the **Save Settings** button to save the settings or click the **Cancel Changes** button to undo your changes. Clicking the **Refresh** button will update the screen's display.



Figure 5-56: VPN tab - PPTP Server

Log Tab - System Log

The System Log screen allows to configure the Router's log, keeping track of the Router's performance.



Figure 5-57: Log tab - System Log

Syslog

Enable Syslog: Checking this box enables the Logging feature, called Syslog.

Syslog Server: In addition to the standard event log, the Router can send a detailed log to an external Syslog server. Syslog is an industry-standard protocol used to capture information about network activity. The Router's Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. Enter the Syslog server name or IP address in the Syslog Server field. Click the **Save Settings** button and then restart the Router for the change to take effect.

E-mail

Enable E-Mail Alert: Checking this box enables E-Mail Alert, which are emailed log entries and alerts.

Mail Server: If you wish to have any log or alert information E-mailed to you, then you must enter the name or numerical IP address of your SMTP server. Your Internet Service Provider can provide you with this information.

Send E-mail To: This is the E-mail address where the log files will be sent.

Log Queue Length (entries): This instructs the Router how often to email log entries by quantity of entries. When the number of queues is reached (i.e. the queue length), the log is sent. The default length is 50 entries.

Log Time Threshold (minutes): This instructs the Router how frequently to email log entries by amount of time. When the time threshold is reached, the log is sent. The default time is 10 minutes.

E-mail Log Now: Clicking the **E-mail Log Now** button immediately sends the log to the address in the Send E-mail to field.

Log Setting

Alert Log

You can receive alert logs for any of these events when you check its box on the screen: Syn Flooding, IP Spoofing, Win Nuke, Ping of Death and Unauthorized Login Attempt.

General Log

You can receive alert logs for any of these events when you check its box on the screen: System Error Messages, Deny Policies, Allow Policies, Content Filtering, Data Inspection, Authorized Login, Configuration Changes.

View System Log: Click this button to view all logs: System Log, Access Log, Firewall Log, or VPN Log.

Outgoing Log Table: Click this button to view information about the outgoing logs: LAN IP, Destination URL/IP and Service/Port number.

Incoming Log Table: Click this button to view information about the incoming logs: Source IP and Destination Port number.

Clear Log Now: This button will clear out your log without e-mailing it. Clicking this button will delete all log information.

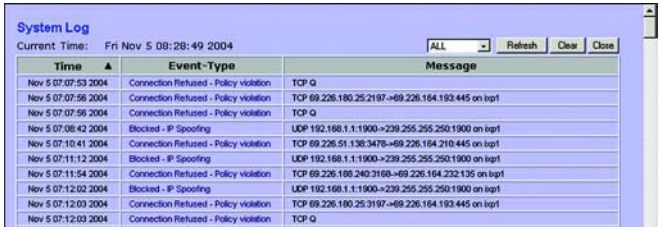


Figure 5-58: Log tab - View Log

Log Tab - System Statistics

This tab displays the system statistics including the Device Name, Status, IP Address, MAC Address, Subnet Mask, Default Gateway, Received Packets, Sent Packets, Total Packets, Received Bytes, Sent Bytes, Total Bytes, Error Packets Received, and Dropped Packets Received for LAN, WAN1 and WAN2.



Figure 5-59: Log tab - System Statistics

Wizard Tab

Use this tab to access the Router's two Setup Wizards: the Basic Setup Wizard and the Access Rule Setup Wizard. They will help you to set up the Router to access the Internet and set up a Firewall security policy, or Access Rule.



Figure 5-60: Wizard tab

Basic Setup

1. Click the **Launch Now** button to run the Basic Setup Wizard to quickly set up the Router to access the Internet.

2. The first screen that appears requests whether the WAN2 (DMZ/Internet) port will be used as a WAN (Internet) port or DMZ port. Select **Dual WAN** to use the port as a WAN port or select **DMZ** to use the port as a DMZ port. Click **Next** to continue. Click **Exit** if you want to exit the wizard.

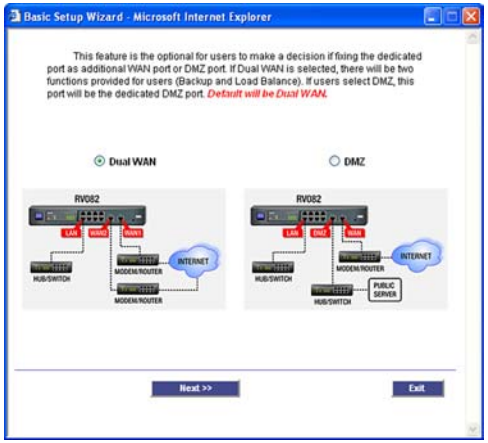


Figure 5-61: Basic Setup Wizard - Dual WAN or DMZ

3. The information on the next screen is used if your Internet Service Provider (ISP) requires a host and domain name. Complete this information, if required by your ISP, and click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.



Figure 5-62: Basic Setup Wizard - Host and Domain Name

4. You will now need to set up the connection types for the WAN ports. These WAN Connection Types were shown in Figures 6-6 through 6-11, and can be referred back to for help.

   If you chose Obtain an IP automatically, select **Use DNS Server provided by ISP (default)** or **Use the Following DNS Server Addresses**, if you want to enter a specific IP. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

   If you chose Static IP, enter the **Static IP**, **Subnet Mask**, and **Default Gateway** provided by your ISP. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

   If you chose PPPoE, enter the **User Name** and **Password** provided by your ISP. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

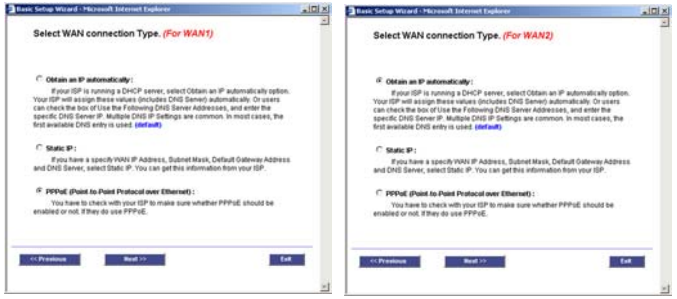


Figure 5-63: Basic Setup Wizard - Selecting WAN Connection Types

5. At the final screen, click **Save Settings** if you are satisfied with all of your settings. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.



Figure 5-64: Basic Setup Wizard - Save Settings

Access Rule Setup

You can access this Setup Wizard through the Wizard tab (shown in Figure 5-60) or by clicking the Wizard button on the Add New Access Rule screen (shown in Figure 5-39).

1. From the Wizard tab, click the **Launch Now** button to run the Access Rule Wizard to help you easily set up the Firewall security policy for the Router.

2. The first screen to appear explains the Access Rules. Click **Next** to continue. Click **Exit** if you want to exit the wizard.

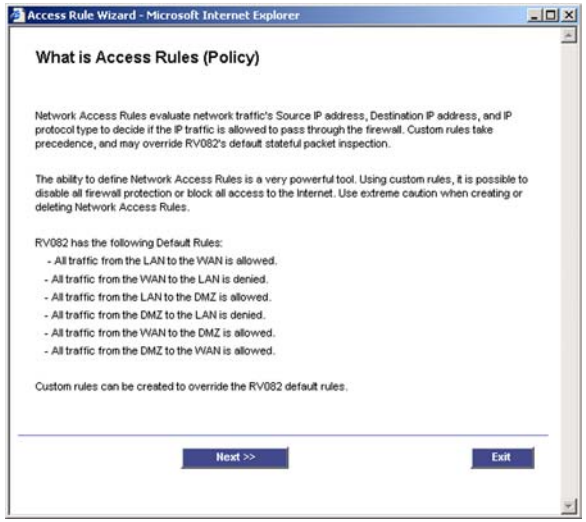


Figure 5-65: Access Rule Wizard - What is Access Rules

3. From the next screen choose if you'd like to **Allow** or **Deny** the action you'll be choosing for the rule. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.



Figure 5-66: Access Rule Wizard - Select the Action

4. Next select the service from the drop-down menu that will be allowed or denied from the Service menu. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

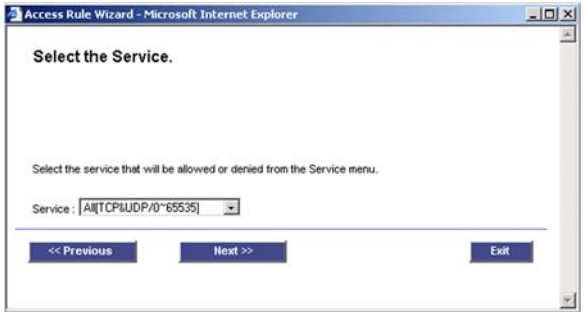


Figure 5-67: Access Rule Wizard - Select the Service

5. From the next screen, select the Source from the Ethernet drop-down menu. Then, select the users from the drop-down menu, Any, single, or Range. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

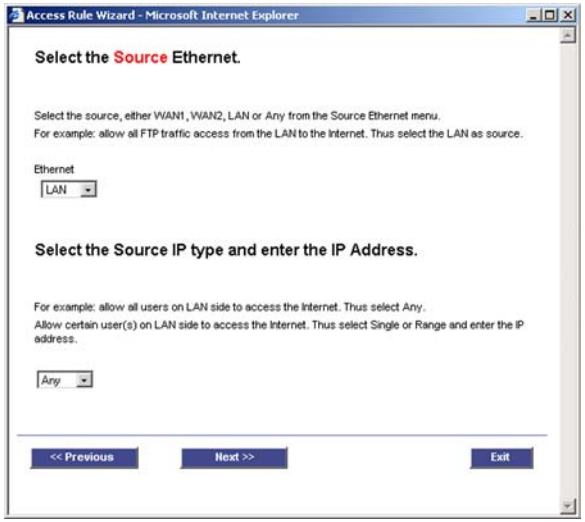


Figure 5-68: Access Rule Wizard - Select the Source

6. Next, choose the destination, either **Any**, **Single**, or **Range**, from the drop-down menu. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

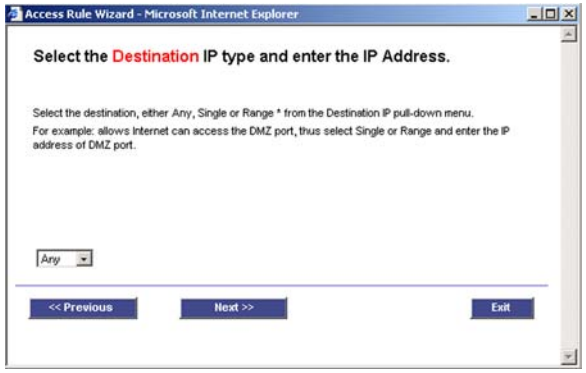


Figure 5-69: Access Rule Wizard - Select the Destination

7. From the next screen, select the scheduling for the rule, **Always**, if the Rule is always in effect, or **Scheduling**, if you want to define a range for a specific time and day of the week. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard.

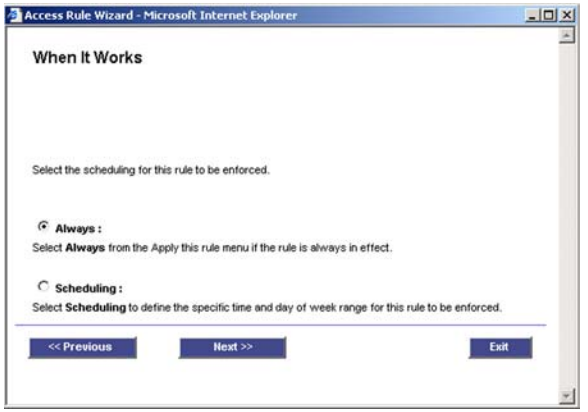


Figure 5-70: Access Rule Wizard - When it Works

8. At the final screen, if you don't need to make any changes click **Save Settings.** Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the wizard. The screen in Figure 5-72 will appear when the settings are correct.

Support Tab

On Line Manual

Click the **On Line Manual** button, and it will link to the Support page of the Linksys website. Click the **Downloads** button from the Technical Support menu, then select the RV082 from the drop-down menu, select your operating system, then click **Downloads for this Product**. Click **User Guide**.

Linksys Web Site

Click the **Linksys Web Site** button, and it will link to the Support page of the Linksys Web Site, www.linksys.com.



Figure 5-71: Support tab

Logout Tab

The Logout tab is located on the upper left corner of the Web Interface. Clicking this tab will terminate the management session. After you click the Logout tab, you will be asked to confirm that you want to terminate the session. You will need to re-enter your User Name and Password to log in and continue to manage the Router.

Appendix A: Troubleshooting

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

Common Problems and Solutions

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

   For Windows 98 and Millennium:

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

For Windows 2000:

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

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

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

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98 and Millennium:

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

For Windows 2000:

1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
2. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
3. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
4. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
5. Restart the computer if asked.
6. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
7. Restart the computer if asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click **Start** and **Control Panel**.
2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
4. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

B. Open a command prompt.

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

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

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

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

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

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

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

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

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

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

Access the Router's web interface by going to **http://192.168.1.1** or the IP address of the Router, and go to the **VPN** => **VPN Pass Through** tab. Make sure you have IPsec passthrough and/or PPTP passthrough enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Basic Setup tab of the Web-based Utility. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

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

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

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

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

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

A. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Setup** => **Forwarding** tab.
B. Select the Service from the pull-down menu. If the Service you need is not listed in the menu, click the **Service Management** button to add the new Service Name, and enter the Protocol and Port Range. Click the **Add to List** button. Then click the **Save Setting** button. Click the **Exit** button.
C. Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address. Then check the **Enable** checkbox for the entry. Consider the examples below:

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

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

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

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

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

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

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

C. Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address. Then check the **Enable** checkbox for the entry. Consider the examples below:

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

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

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

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

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

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

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

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

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

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

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

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

For Microsoft Internet Explorer 5.0 or higher:

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

For Netscape 4.7 or higher:

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

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

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

12. I need to upgrade the firmware.

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

A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware, or use the Web-based Utility to be automatically redirected to the download webpage. Go to System Management - Firmware Upgrade, and click the **Firmware Download from Linksys Web Site** button. Select the Router from the pull-down menu and choose the firmware from the options.
A. Extract the firmware file on your computer.
B. To upgrade the firmware, follow the steps in the Upgrade section found in "Chapter 5: Setting Up and Configuring the Router" or "Appendix F: Upgrading Firmware."

13. The firmware upgrade failed.

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

C. Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

   IP Address: 192.168.1.50
   Subnet Mask: 255.255.255.0
   Gateway: 192.168.1.1

D. Perform the upgrade using the Router's Web-based Utility through its System Management => Firmware Upgrade tab.

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

If you want to use a backup firmware version, go to System Management => Restart. Select **Backup Firmware Version**. Click the **Restart Router** button to restart the Router.

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

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

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

F. 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.

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

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

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

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

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

16. I need to use port triggering.

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

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

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

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

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

Frequently Asked Questions

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

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

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

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

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

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

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

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

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

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

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

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?
Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at *www.linksys.com* for more information.

If all else fails in the installation, what can I do?
Reset the Router by holding down the Reset button for ten seconds. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

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

Will the Router function in a Macintosh environment?
Yes, but the Router's setup pages are accessible only through Internet Explorer 5.0 or Netscape Navigator 5.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

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

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

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

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

How many ports can be simultaneously forwarded?
Theoretically, the Router can establish 4,000 sessions at the same time, but you can only forward 30 ranges of ports.

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

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

What is the maximum number of VPN sessions allowed by the Router?
The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

How can I check whether I have static or DHCP IP addresses?
Ask your ISP to find out.

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

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

Appendix B: Installing the Linksys VPN Client

When using your PC to log onto the Router from remote locations, you'll want to use the Linksys QuickVPN Client. Installing this Client takes just a few steps, provided below.

1. Insert the RV082 User Guide CD into your PC's CD-ROM drive.
2. Click the **Start** button, select **Run**, and, in the window that appears, type **D:\Linksys_QuickVPN_1028.exe** (where D: is your CD-ROM drive). Then, click the **OK** button. The Client will immediately begin installing the software onto your hard drive at C:\Program Files\Linksys\Linksys VPN Client.
3. The License Agreement screen will appear. Read the agreement and click the **Yes** button to proceed. Clicking the **Back** or **No** buttons will close the installation.



Figure B-1: Linksys VPN License Agreement

4. The Linksys VPN Client software will now be installed. When it is finished, an screen will appear to tell you that the installation is complete. Click the **Finish** button.

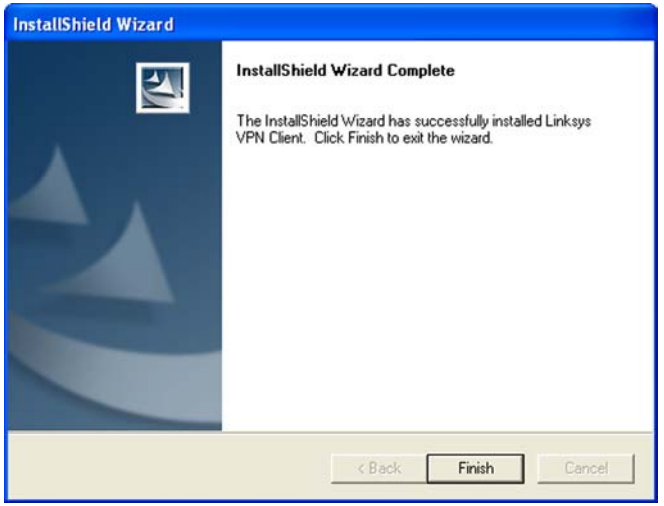


Figure B-2: Linksys VPN Installation Complete

5. At this point, the Linksys VPN Client (or QuickVPN) will open. From this screen, you can sign in with your Profile Name, Username, and Password. Then, enter the Server Address of the VPN connection onto which you will be logging. Once you're done, click the **Connect** button to connect to the VPN connect. you can save your VPN connection information by clicking the **Save** button or delete it by clicking the **Delete** button. Clicking the **Help** button will open a help screen.

For future connections, there is an icon that gets placed on the desktop labeled: Linksys QuickVPN.



Figure B-3: Linksys QuickVPN

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

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

Windows 98 or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Router via a CAT 5 Ethernet network cable.
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.

   The example in Figure C-2 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.



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



Figure C-1: IP Configuration Screen



Figure C-2: MAC Address/Adapter Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.
2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

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

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

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

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

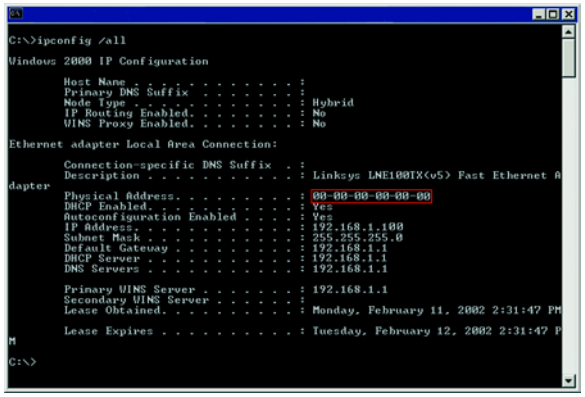


Figure C-3: MAC Address/Physical Address

For the Router's Web-based Utility

For MAC address cloning, enter the MAC Address in the User Defined WAN1 or WAN2 MAC Address field or select **MAC Address from this PC**.

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



Figure C-4: MAC Address Clone

Appendix D: Physical Setup of the Router

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

Setting up the Router

You can set the Router on a desktop, install it in a rack with attached brackets, or mount it on the wall.

Placement of the Router

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

Rack-Mounting the Router

The Router comes with two brackets and eight screws for mounting on a 19-inch rack.

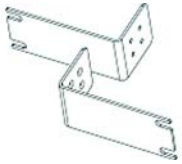


Figure D-1: Mounting Brackets

Line up the bracket holes with the holes in the Router and attach with the screws, using four on each side of the Router. After the brackets are attached to the Router by screws, you can rack-mount it. Attach the Router to the rack with two screws on each side.

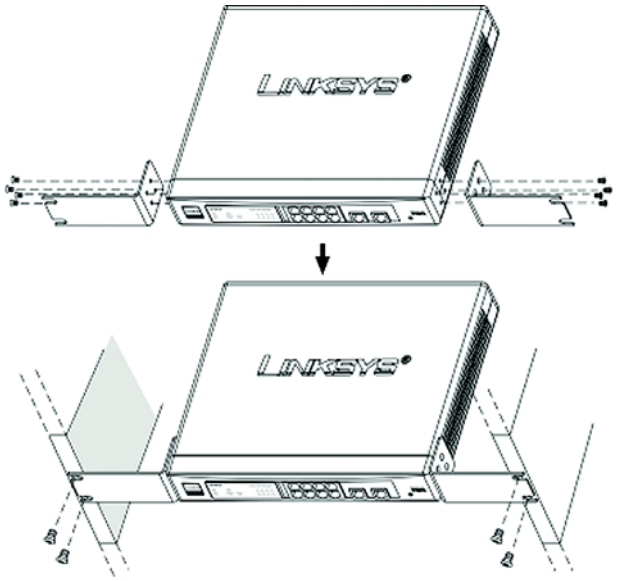


Figure D-2: Attaching the Brackets to the Router and Rack-Mounting the Router

Wall-Mounting the Router

The Router is shown in Figure D-3 with two holes on the bottom. The horizontal distant between the two holes is 3.701 in (94mm). Install two screws or nails into the wall, 3.701 in (94 mm) apart. After the nails are secured on the wall, line up the Router's holes with the screws on the wall to wall-mount it. The wall-mount holes are shown below, in Figure D-3. The suggested mounting hardware is shown in Figure D-4.

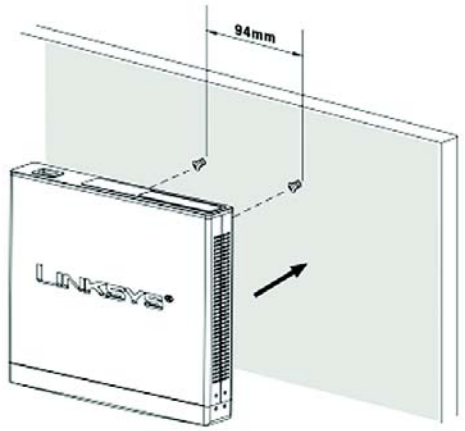


Figure D-3: Wall-Mounting the Router

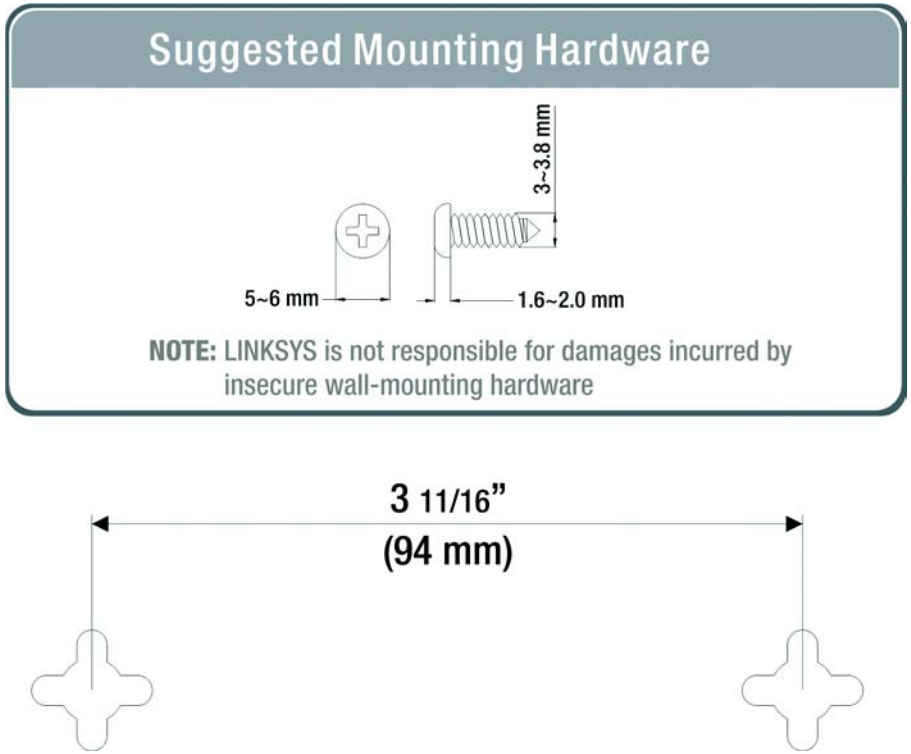


Figure D-4: Wall-Mounting Hardware

Appendix E: Battery Replacement

This section instructs the user on battery replacement.

Replacing a Lithium Battery

The Router has a lithium battery, number CR2032, on its main circuit board. This battery has an operating life of about 1~2 years. When the battery loses its charge, the Router cannot update the correct time except when connected to the NTP Server.



WARNING: The lithium battery can explode if replaced incorrectly. It must be replaced with an equivalent CR2032 lithium battery. Do not replace this battery yourself. Contact Linksys Technical Support.

Do not attempt to replace this battery yourself. You must call Linksys Technical Support to replace the battery. Danger of explosion exists if the lithium battery is incorrectly replaced. The battery can only be replaced with the same or equivalent type of CR2032 lithium battery.

Appendix F: Upgrading Firmware

You can use the Router's Web-based Utility to upgrade the firmware; however, if you do so, you may lose the settings you have configured on the Router.

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

1. Download the Router's firmware upgrade file from the Linksys website, *www.linksys.com* or click the **Firmware Download from Linksys Web Site** button. Select the Router from the pull-down menu and choose the firmware from the options.
2. Extract the file on your computer.
3. Click the **System Management Tab** and then the **Firmware Upgrade** page.
4. On the Firmware Upgrade screen, enter the location of the extracted firmware upgrade file, or click the **Browse** button to find this file.
5. Click the **Firmware Upgrade Right Now** button, and follow the on-screen instructions.



Figure F-1: Upgrade Firmware

Appendix G: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix H: Glossary

Adapter - A device that adds network functionality to your PC.

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

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

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

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

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

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

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

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

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

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

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

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

Gateway - A system that interconnects networks.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

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

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

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

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

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

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

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

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

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

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

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

Upload - To transmit a file over a network.

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

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

WAN (Wide Area Network) - The Internet.

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

Appendix I: Specifications

Standards	IEEE 802.3, 802.3u
Ports	8 10/100 RJ-45 Ports, 1 10/100 RJ-45 Internet Port, 1 10/100 RJ-45 DMZ/Internet Port
Button	Reset
Cabling Type	Ethernet Category 5
LEDs	System, Internet, DMZ/Internet, DMZ Mode, Diag, 1-8
UPnP able/cert	Yes
Security Features	SPI Firewall, DES and 3DES Encryption for IPSec VPN Tunnel
Dimensions (W x H x D)	11" x 1.75" x 9.50" (279.4 mm x 44.45 mm x 241.3 mm)
Unit Weight	52 oz. (1.47 kg)
Power	Input: AC100~240V, 0.4A; Output: DC 3.3V / 3A
Certifications	FCC Class B, CE Class B
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	0ºC to 70ºC (32ºF to 158ºF)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix J: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix K: Regulatory Information

FCC STATEMENT

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

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

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

EC DECLARATION OF CONFORMITY (EUROPE)

In compliance with the EMC Directive 89/336/EEC, Low Voltage Directive 73/23/EEC, and Amendment Directive 93/68/EEC, this product meets the requirements of the following standards:

- EN55022 Emission
- EN55024 Immunity

Appendix L: Contact Information

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

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP