

LINKSYS[®]
A Division of Cisco Systems, Inc.



10/100
16-Port VPN Router

User Guide



Model No. **RV016**



Copyright and Trademarks

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.

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	10
Chapter 4: Connecting the Router	11
Overview	11
Connection Instructions	12
Chapter 5: Configuring the PCs	13
Overview	13
Configuring Windows 98 and Millennium PCs	13
Configuring Windows 2000 PCs	14
Configuring Windows XP PCs	14
Chapter 6: Setting up and Configuring the Router	16
Overview	16
How to Access the Web-based Utility	19
System Summary Tab	19
Setup Tab - Network	22
Setup Tab - Password	25
Setup Tab - Time	25
Setup Tab - DMZ Host	26
Setup Tab - Forwarding	26
Setup Tab - UPnP	28
Setup Tab - One-to-One NAT	29
Setup Tab - MAC Clone	30
Setup Tab - DDNS	31

Setup Tab - Advanced Routing	32
DHCP Tab - Setup	34
DHCP Tab - Status	36
System Management Tab - Multi-WAN	37
System Management Tab - SNMP	40
System Management Tab - Diagnostic	41
System Management Tab - Factory Default	42
System Management Tab - Firmware Upgrade	42
System Management Tab - Restart	43
System Management Tab - Setting Backup	43
Port Management Tab - Port Setup	44
Port Management Tab - Port Status	45
Firewall Tab - General	46
Firewall Tab - Access Rules	47
Firewall Tab - Content Filter	49
VPN Tab - Summary	50
VPN Tab - Gateway to Gateway	52
VPN Tab - Client to Gateway	59
VPN Tab - VPN Pass Through	68
Log Tab - System Log	69
Log Tab - System Statistics	71
Wizard Tab	72
Support Tab	81
Logout Tab	81
Appendix A: Troubleshooting	82
Common Problems and Solutions	82
Frequently Asked Questions	93
Appendix B: Upgrading Firmware	97
Appendix C: Finding the MAC Address and IP Address for Your	
Ethernet Adapter	98
Windows 98 or Me Instructions	98
Windows 2000 or XP Instructions	98
For the Router's Web-based Utility	99
Appendix D: Physical Setup of the Router	100
Setting up the Router	100

Appendix E: Battery Replacement	104
Replacing a Lithium Battery	104
Appendix F: Windows Help	105
Appendix G: Glossary	106
Appendix H: Specifications	113
Appendix I: Warranty Information	114
Appendix J: Regulatory Information	115
Appendix K: Contact Information	116

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	10
Figure 4-1: Example of a Typical Network	11
Figure 4-2: Connect a PC	12
Figure 4-3: Connect the Internet	12
Figure 4-4: Connect the DMZ	12
Figure 4-5: Connect the Power	12
Figure 5-1: TCP/IP for Windows 98 and Me	13
Figure 5-2: Obtain an IP address automatically for Windows 98 and Me	13
Figure 5-3: Internet Protocol (TCP/IP) for Windows 2000	14
Figure 5-4: Obtain an IP address automatically for Windows 2000	14
Figure 5-5: Internet Protocol (TCP/IP) for Windows XP	15
Figure 5-6: Obtain an IP address automatically for Windows XP	15
Figure 6-1: Router's IP Address	19
Figure 6-2: Login Screen	19
Figure 6-3: System Summary	19
Figure 6-4: Site Map	20
Figure 6-5: Port Information	20
Figure 6-6: Setup Tab	22
Figure 6-7: Save New Number of WAN Ports	22
Figure 6-8: Obtain an IP Automatically	23
Figure 6-9: Static IP	23
Figure 6-10: PPPoE	23
Figure 6-11: PPTP	24
Figure 6-12: DMZ	24
Figure 6-13: Password	25

Figure 6-14: Time - Automatic	25
Figure 6-15: Time - Manual	25
Figure 6-16: DMZ Host	26
Figure 6-17: Forwarding	26
Figure 6-18: Service Management	27
Figure 6-19: UPnP	28
Figure 6-20: One-to-One NAT	29
Figure 6-21: MAC Clone	30
Figure 6-22: Edit MAC Clone	30
Figure 6-23: DDNS	31
Figure 6-24: Edit DDNS	31
Figure 6-25: Advanced Routing	32
Figure 6-26: DHCP Setup	34
Figure 6-27: DHCP Status	36
Figure 6-28: Multi-WAN Load Balance	37
Figure 6-29: Save New Mode	37
Figure 6-30: Intelligent Balancer - Edit Load Balance	37
Figure 6-31: IP Group (By Users)	38
Figure 6-32: IP Group (By Users) - Edit Load Balance	38
Figure 6-33: SNMP	40
Figure 6-34: DNS Name Lookup	41
Figure 6-35: Ping	41
Figure 6-36: Factory Default	42
Figure 6-37: Confirm Return to Factory Default Settings	42
Figure 6-38: Firmware Upgrade	42
Figure 6-39: Restart	43
Figure 6-40: Setting Backup	43
Figure 6-41: Port Setup	44
Figure 6-42: Port Status	45
Figure 6-43: General Firewall	46

Figure 6-44: Access Rules	47
Figure 6-45: Add a New Access Rule	48
Figure 6-46: Content Filter	49
Figure 6-47: VPN Summary	50
Figure 6-48: VPN Tunnel Details	50
Figure 6-49: Types of VPN Tunnels	50
Figure 6-50: GroupVPN List	51
Figure 6-51: Gateway to Gateway	52
Figure 6-52: Local Security Gateway Type - IP Only	53
Figure 6-53: Local Security Gateway Type - IP + Domain Name (FQDN) Authentication	53
Figure 6-54: Local Security Gateway Type - IP + E-mail Addr. (USER FQDN) Authentication	53
Figure 6-55: Local Security Gateway Type - Dynamic IP + Domain Name (FQDN) Authentication	53
Figure 6-56: Local Security Gateway Type - Dynamic IP + E-mail Addr. (USER FQDN) Authentication	53
Figure 6-57: Local Security Group Type - IP	53
Figure 6-58: Local Security Group Type - Subnet	53
Figure 6-59: Local Security Group Type - IP Range	54
Figure 6-60: Remote Security Gateway Type - IP Only	54
Figure 6-61: Remote Security Gateway Type - IP + Domain Name (FQDN) Authentication	54
Figure 6-62: Remote Security Gateway Type - IP + E-mail Addr. (USER FQDN) Authentication	54
Figure 6-63: Remote Security Gateway Type - Dynamic IP + Domain Name (FQDN) Authentication	55
Figure 6-64: Remote Security Gateway Type - Dynamic IP + E-mail Addr. (USER FQDN) Authentication	55
Figure 6-65: Remote Security Group Type - IP	55

Figure 6-66: Remote Security Group Type - Subnet	55
Figure 6-67: Remote Security Group Type - IP Range	55
Figure 6-68: IPSec Setup - IKE with Preshared Key	56
Figure 6-69: IPSec Setup - Manual	57
Figure 6-70: IKE with Preshared Key - Advanced	58
Figure 6-71: Client to Gateway	59
Figure 6-72: Local Security Gateway Type - IP Only	60
Figure 6-73: Local Security Gateway Type - IP + Domain Name (FQDN) Authentication	60
Figure 6-74: Local Security Gateway Type - IP + E-mail Addr. (USER FQDN) Authentication	61
Figure 6-75: Local Security Gateway Type - Dynamic IP + Domain Name (FQDN) Authentication	61
Figure 6-76: Local Security Gateway Type - Dynamic IP + E-mail Addr. (USER FQDN) Authentication	61
Figure 6-77: Local Security Group Type - IP	61
Figure 6-78: Local Security Group Type - Subnet	61
Figure 6-79: Local Security Group Type - IP Range	61
Figure 6-80: Remote Client for VPN Tunnel - IP Only	62
Figure 6-81: Remote Client for VPN Tunnel - IP + Domain Name (FQDN) Authentication	62
Figure 6-82: Remote Client for VPN Tunnel - IP + E-mail Addr. (User FQDN) Authentication	62
Figure 6-83: Remote Client for VPN Tunnel - Dynamic IP + Domain Name (FQDN) Authentication	62
Figure 6-84: Remote Client for VPN Tunnel - Dynamic IP + E-mail Addr. (User FQDN) Authentication	63
Figure 6-85: Remote Client for Group VPN - Domain Name (FQDN)	63
Figure 6-86: Remote Client for Group VPN - E-mail Address (USER FQDN)	63
Figure 6-87: Remote Client for Group VPN - Microsoft XP/2000 VPN Client	63

Figure 6-88: IPSec Setup - IKE with Preshared Key	64
Figure 6-89: IPSec Setup - Manual	65
Figure 6-90: IKE with Preshared Key - Advanced	66
Figure 6-91: VPN Pass Through	68
Figure 6-92: System Log	69
Figure 6-93: View All Logs	70
Figure 6-94: View VPN Log	70
Figure 6-95: View Outgoing Log Table	70
Figure 6-96: View Incoming Log Table	70
Figure 6-97: System Statistics	71
Figure 6-98: Wizard	72
Figure 6-99: Basic Setup Wizard - Change Number of WAN Ports	72
Figure 6-100: Change Number of WAN Ports	72
Figure 6-101: Save Settings	73
Figure 6-102: Basic Setup Wizard - Edit Network Settings	73
Figure 6-103: Host and Domain Name	73
Figure 6-104: WAN Connection Type	74
Figure 6-105: Obtain an IP Automatically	74
Figure 6-106: Static IP	75
Figure 6-107: Static IP - DNS Servers	75
Figure 6-108: PPPoE	76
Figure 6-109: PPPoE - Connect on Demand or Keep Alive	76
Figure 6-110: DMZ	77
Figure 6-111: Save Settings	77
Figure 6-112: Access Rules	78
Figure 6-113: Action	78
Figure 6-114: Service	79
Figure 6-115: Log	79
Figure 6-116: Source	79
Figure 6-117: Destination	80

Figure 6-118: Scheduling	80
Figure 6-119: Save Settings	80
Figure 6-120: Support	81
Figure 6-121: Logout	81
Figure B-1: Upgrade Firmware	97
Figure C-1: IP Configuration Screen	98
Figure C-2: MAC Address/Adapter Address	98
Figure C-3: MAC Address/Physical Address	99
Figure C-4: MAC Clone	99
Figure C-5: Edit MAC Clone	99
Figure D-1: Mounting Brackets	100
Figure D-2: Attaching the Brackets to the Router and Rack-Mounting the Router	101
Figure D-3: Wall-Mounting the Router	102
Figure D-4: Wall-Mounting Hardware	103

Chapter 1: Introduction

Welcome

Thank you for choosing the 10/100 16-Port VPN Router. The Linksys 10/100 16-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 16 ports on this Router feature unprecedented versatility. Two are dedicated Internet ports that let you connect a second Internet line as a backup to ensure that you're never disconnected. Or, you can use both Internet ports at the same time, and let the router balance your office's requirements between them for maximum bandwidth efficiency.

Not enough? Up to five of the thirteen full-duplex switched 10/100 Ethernet ports can be reconfigured as Internet ports, for an up to seven-port failover or load balanced redundancy! Finally, a dedicated DMZ port gives you a publicly accessible channel so you can set up a web or FTP server, unimpeded by the powerful security features of the Router.

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 16-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 16-Port VPN Router gives you the connection reliability your business needs.

Use the instructions in this Guide to help you connect the Router, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the 10/100 16-Port VPN Router.

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

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

What's in this Guide?

This user guide covers the steps for setting up and using the 10/100 16-Port VPN Router.

- **Chapter 1: Introduction**
This chapter describes the 10/100 16-Port VPN Router applications and this User Guide.
- **Chapter 2: Networking Basics**
This chapter describes the basics of networking.
- **Chapter 3: Getting to Know the 10/100 16-Port VPN Router**
This chapter describes the physical features of the Router.
- **Chapter 4: Connecting the 10/100 16-Port VPN Router**
This chapter instructs you on how to connect the Router to your network.
- **Chapter 5: Configuring the PCs**
This chapter explains how to configure the PCs for your network.
- **Chapter 6: Setting up and Configuring the Router**
This chapter explains how to use the Web-based Utility to set up the Router and configure its settings.
- **Appendix A: Troubleshooting**
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the 10/100 16-Port VPN Router.
- **Appendix B: Upgrading Firmware**
This appendix instructs you on how to upgrade the firmware on your Router if you should need to do so.
- **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 MAC address cloning feature of the Router.
- **Appendix D: Physical Setup of the Router**
This appendix describes the physical setup of the Router, including installation of the mounting brackets.
- **Appendix E: Battery Replacement**
This appendix explains how to replace the Router's battery.
- **Appendix F: Windows Help**
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

10/100 16-Port VPN Router

- **Appendix G: Glossary**
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix H: Specifications**
This appendix provides the technical specifications for the Router.
- **Appendix I: Warranty Information**
This appendix supplies the warranty information for the Router.
- **Appendix J: Regulatory Information**
This appendix supplies the regulatory information regarding the Router.
- **Appendix K: 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 Stateful Packet Inspection (SPI) firewall and 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.

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.

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.

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

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

SPI (Stateful Packet Inspection) firewall: a technology that inspects every incoming packet of information before allowing it to enter the network.

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

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

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

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

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

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

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

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.

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



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:

10/100 16-Port VPN Router

- 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 10/100 16-Port VPN 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 his computer were physically connected.

Computer 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 10/100 16-Port 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 her computer were physically connected.

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

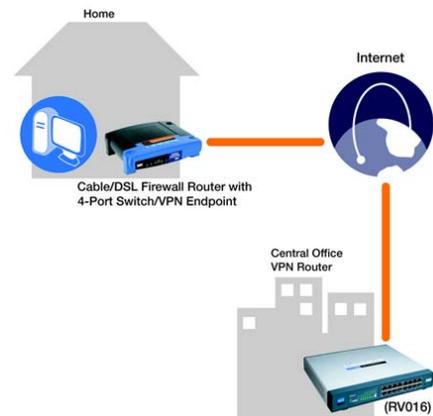


Figure 2-1: VPN Router-to-VPN Router VPN

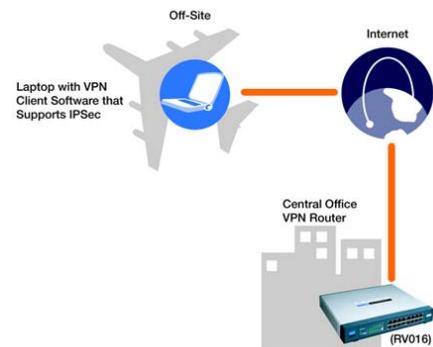


Figure 2-2: Computer-to-VPN Router VPN

Chapter 3: Getting to Know the Router

The Front Panel

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



Figure 3-1: Front Panel

LEDs

- DIAG** Orange. The **DIAG** LED lights up when the system is not ready. The LED turns off when the system is ready.
- System** Green. The **System** LED lights up when the Router is powered on. When the LED is flashing, the Router is running a diagnostic test.
- LAN/Act (1-13)** Green. Each **LAN/Act** 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, 8, 9, 10, 11, 12, 13). If the LED is flashing, the Router is actively sending or receiving data over that port.

LAN/Act LEDs 9-13 and Internet/Act LEDs 3-7 represent the dual-function ports, which can be used as LAN or Internet ports. These are LAN ports 9-13 (white print) or Internet ports 3-7 (dark print) on the Router's front panel.
- Internet/Act (1-7)** Green. Each **Internet/Act** LED serves two purposes. If the LED is continuously lit, the Router is connected to an Internet device, such as a cable or DSL modem, through the corresponding port. If the LED is flashing, the Router is actively sending or receiving data over that port.

Internet/Act LEDs 1 and 2 are labeled Internet because they can be used only as Internet ports.

DMZ Orange. The **DMZ** LED serves two purposes. If the LED is continuously lit, the Router is connected to a DMZ host through the DMZ port. If the LED is flashing, the Router is actively sending or receiving data over that port.

Ports

1-13 (LAN) These thirteen **LAN** Ethernet ports connect to network devices, such as PCs, print servers, or additional switches.

LAN ports 9-13 can also be used as Internet ports.

Internet (1-7) The seven **Internet** Ethernet ports connect to an Internet device, such as a cable or DSL modem.

Internet ports 1 and 2 are labeled Internet because they can be used only as Internet ports. When used as an additional Internet port, it connects to a cable or DSL modem.

Internet ports 3-7 can also be used as LAN ports.

DMZ The **DMZ** Ethernet port connects to a hub, switch, or public server.

Button

Reset Button

The Reset button can be used in one of two ways:

If the Router is having problems connecting to the Internet, press the Reset button with a paper clip or a pencil tip for four seconds. This performs a warm reset, similar to rebooting your PC. You will see the Diag LED flash slowly until the warm reset is complete.

If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for ten seconds. This will restore the factory defaults and clear all of the Router's settings, such as port range forwarding entries or a new password. You will see the Diag LED flash quickly until the factory defaults have been restored.

The Back Panel

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

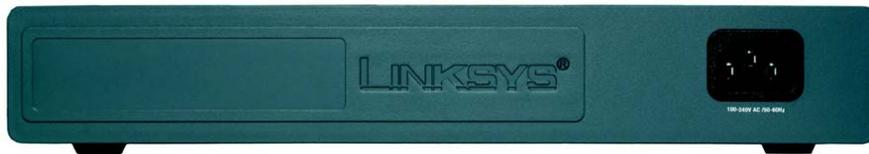


Figure 3-2: Back Panel

Power

The Power port is where you connect the power adapter.

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 “Chapter 5: Configuring the PCs.” (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 6: Set up and Configure the Router.”

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

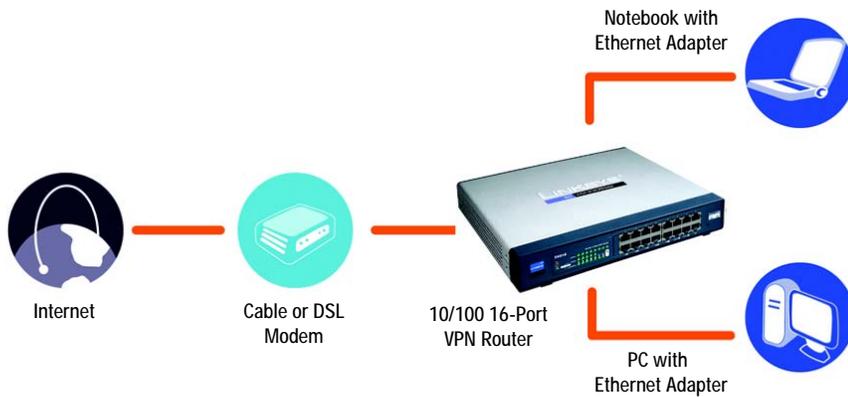


Figure 4-1: Example of a Typical Network

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 (see Figure 4-2). 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 one of the Router's Internet ports.

Repeat this step to connect additional Internet devices to the Router's other Internet ports.

4. If you want to use the DMZ port, connect an Ethernet cable to it, and connect the other end to the appropriate network device, such as a public server.
5. Power on the cable or DSL modem and the other network device(s).
6. Connect the included power cord to the Router's Power port on the back of the Router, as shown in Figure 4-4, and then plug the power cord 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 "Chapter 5: Configuring the PCs." Otherwise, proceed to "Chapter 6: Setting up and Configuring the Router."

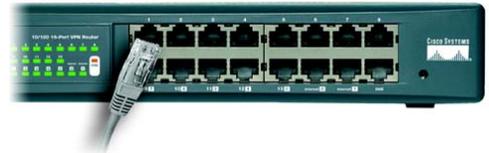


Figure 4-2: Connect a PC



Figure 4-3: Connect the Internet



Figure 4-4: Connect the DMZ



Figure 4-5: Connect the Power

Chapter 5: Configuring the PCs

Overview

The instructions in this chapter will help you configure each of your computers so they will be able to communicate with the Router. Each PC must be set to obtain an IP address (or TCP/IP) address automatically (called DHCP). Computers use IP addresses to communicate with each other across a network or the Internet.



Note: These instructions apply only to Windows 98, Millennium, 2000, or XP computers. By default, Windows 98, 2000, Millennium, and XP have TCP/IP installed and are set to obtain an IP address automatically. If you have not made any changes to your PC's default network settings, then proceed to "Chapter 6: Setting up and Configuring the Router."

Find out which operating system your computer is running, such as Windows 98, Millennium, 2000, or XP. If you're not sure, you can find out by clicking the Start button. On the left side of the taskbar, it will say which operating system your computer is using.

You may need to do this for each computer you are connecting to the Router.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet card or adapter has been successfully installed in each PC you will configure. Once you've configured your computers, proceed to "Chapter 6: Setting up and Configuring the Router."

Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network** icon.
2. On the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter, as shown in Figure 5-1. Do not choose a TCP/IP entry whose name mentions Dial-Up Adapter, PPPoE, VPN, or AOL. If the word TCP/IP appears by itself, select that line. (If there is no TCP/IP line listed, refer to Windows Help or your Ethernet adapter's documentation to install TCP/IP now.) Click the **Properties** button.
3. Click the **IP Address** tab and select **Obtain an IP address automatically**, as shown in Figure 5-2.
4. Now click the **Gateway** tab to ensure that the *Installed Gateway* field is left blank. Click the **OK** button.

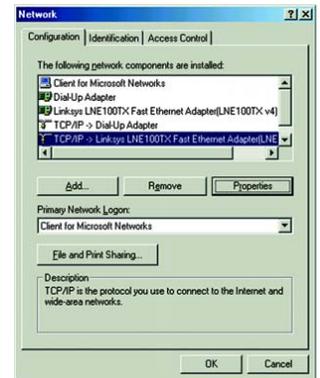


Figure 5-1: TCP/IP for Windows 98 and Me

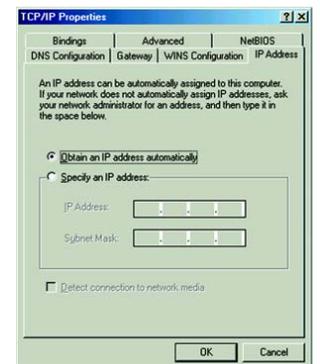


Figure 5-2: Obtain an IP address automatically for Windows 98 and Me

- Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Supply them by pointing to the correct file location, e.g., D:\win98, D:\win9x, c:\windows\options\cabs, etc. (if "D" is the letter of your CD-ROM drive).
- Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

Go to "Chapter 6: Setting up and Configuring the Router."

Configuring Windows 2000 PCs

- Click the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network and Dial-up Connections** icon.
- Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button.
- Select **Internet Protocol (TCP/IP)**, and click the **Properties** button. See Figure 5-3.
- Select **Obtain an IP address automatically** (see Figure 5-4). Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.
- Restart your computer.

Go to "Chapter 6: Setting up and Configuring the Router."

Configuring Windows XP PCs

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

- Click the **Start** button. Click **Settings** and then **Control Panel**. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
- Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button.

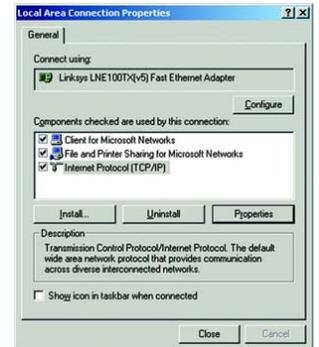


Figure 5-3: Internet Protocol (TCP/IP) for Windows 2000

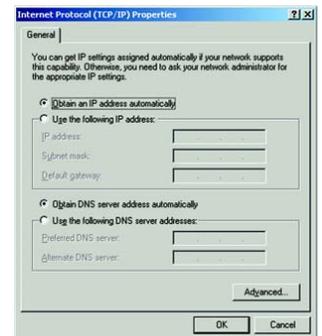


Figure 5-4: Obtain an IP address automatically for Windows 2000

3. Select **Internet Protocol (TCP/IP)**, and click the **Properties** button. See Figure 5-5.
4. Select **Obtain an IP address automatically** (see Figure 5-6). Once the new window appears, click the **OK** button. Click the **OK** button again (or the **Close** button if any settings were changed) to complete the PC configuration.
5. Restart your computer.

Go to "Chapter 6: Setting up and Configuring the Router."

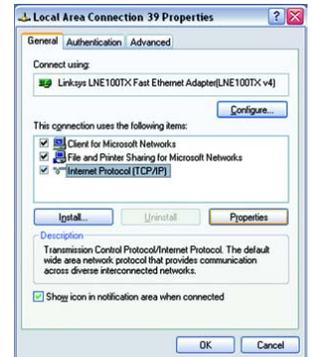


Figure 5-5: Internet Protocol (TCP/IP) for Windows XP

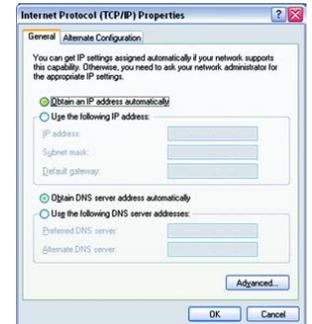


Figure 5-6: Obtain an IP address automatically for Windows XP

Chapter 6: Setting up and Configuring the Router

Overview

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

There are eleven main tabs in the Utility: System Summary, Setup, DHCP, System Management, Port Management, Firewall, VPN, Log, Wizard, Support, and Logout. Additional tabs will be available after 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. If you click any underlined text, the related setup page will appear.

Setup Tab

- **Network.** Enter the Internet connection and network settings on this screen.
- **Password.** You can change the Router's password on this screen. It is strongly recommended that you change the Router's password from the default.
- **Time.** On this screen, configure the Router's time settings. You can set the time, select a time zone, enable or disable the Daylight Savings feature, and configure the NTP (Network Time Protocol) settings.
- **DMZ Host.** The DMZ (Demilitarized Zone) Host feature allows one local user to be exposed to the Internet for use of a special-purpose service 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 (Universal Plug and Play) forwarding can be used to set up public services on your network.
- **One-to-One NAT.** One-to-One NAT (Network Address Translation) creates a relationship that maps valid external addresses to internal addresses hidden by NAT.
- **MAC Clone.** Some ISPs require that you register a MAC address. This feature "clones" your network adapter's MAC address onto the Router, so you don't have to call your ISP and change the registered MAC address to the Router's MAC address.

10/100 16-Port VPN Router

- **DDNS.** DDNS (Dynamic Domain Name Service) 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.
- **Advanced Routing.** On this screen, you can enable the Router's dynamic routing feature so it will automatically adjust to physical changes in the network's layout. You can also set up static routes.

DHCP Tab

- **Setup.** You can enable/disable the DHCP server, set up client lease time, configure the DHCP IP range, assign static IP addresses to specific clients, assign DNS server(s) to clients, and enter the WINS server IP address.
- **Status.** A Status page is available to review the status of the DHCP server and its clients.

System Management Tab

- **Multi-WAN.** There are two modes provided for the Load Balance function – Intelligent Balancer (Auto Mode) and IP Group (By Users).
- **SNMP.** SNMP (Simple Network Management Protocol) is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network. (SNMP can only be used to monitor and configure the Router from inside the local network.)
- **Diagnostic.** The Router has two built-in tools that will help with troubleshooting network problems.
- **Factory Default.** Use this screen to clear all of your configuration information and restore the Router to its factory default settings. Only use this feature if you want to remove all of your custom configuration settings.
- **Firmware Upgrade.** You can use this screen to upgrade the Router's firmware to the latest version.
- **Restart.** The recommended method of restarting the Router is to use the Restart tool available on this page. When you use this method, the Router will send out your log file before it is reset.
- **Setting Backup.** This tab allows you to make a backup file of your configuration file for the Router.

Port Management Tab

- **Port Setup.** You can configure the connection settings for each port, such as priority, speed, duplex, and auto negotiation.
- **Port Status.** You can select a port number to view its settings.

Firewall Tab

- **General.** Use this screen to enable or disable various firewall and security features, including SPI (Stateful Packet Inspection), DoS (Denial of Service), and Remote Management.
- **Access Rules.** Access Rules evaluate the network traffic's source IP address, destination IP address, and IP protocol type to decide whether the IP traffic is allowed to pass through the firewall. You can set up custom Access Rules from this screen.
- **Content Filter.** This tab allows you to filter web access according to a list of forbidden domains and a schedule.

VPN Tab

- **Summary.** This screen displays the Summary, Tunnel Status, and GroupVPN Status settings and information.
- **Gateway to Gateway.** Use this screen to create a new tunnel between two VPN devices.
- **Client to Gateway.** From this screen, create a new tunnel between a local VPN device and a mobile user, or set up a Group VPN.
- **VPN Pass Through.** This tab allows you to disable IPSec, PPTP, and/or L2TP Pass Through.

Log Tab

- **System Log.** The System Log displays the syslog, e-mail alert, and log settings.
- **System Statistics.** This tab 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.** Use this screen to conveniently access this User Guide and the Linksys website.

Logout Tab

- **Logout.** Click the Logout tab to exit the Utility.

How to Access the Web-based Utility

To access the Web-based Utility of the Router, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field, as shown in Figure 6-1. Press the **Enter** key.

A screen will appear asking you for your User Name and Password, as shown in Figure 6-2. 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 the System Summary tab, which displays the Router's current status and settings. (See Figure 6-3.) This information is read-only. Underlined text is hyperlinked to related setup pages, so if you click a hyperlink, the related setup screen will appear. On the right-hand side of this screen and all other screens of the Utility is 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, which is shown in Figure 6-4. Then, click the desired tab.

System Information

Serial Number. The serial number of the Router.

Firmware version. The current version number of the firmware installed on the Router.

CPU. The type and speed of the processor installed on the Router.

DRAM. The size of DRAM installed on the Router's motherboard.

Flash. The size of flash memory installed on the Router's board.

System Up Time. The length of time in days, hours, and minutes that the Router has been active. The current time and date are also displayed.

Configuration

If you need help to set up the Router, click the **Setup Wizard** button. For more details, see the Wizard Tab section.



Figure 6-1: Router's IP Address



Figure 6-2: Login Screen

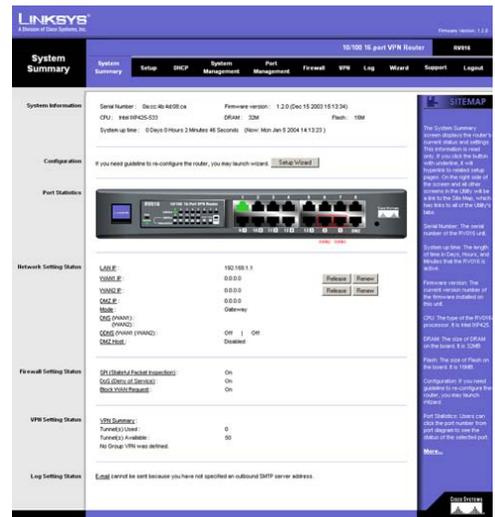


Figure 6-3: System Summary

Port Statistics

Click any port on the Router's front panel image to see the status of the selected port. If the port is disabled, it will be red; if enabled, it will be black. If the port is connected, it will be green. Information about the selected port will appear in a separate window. The port's Summary table will show the settings of the selected port, including Type, Interface, Link Status, Port Activity, Priority, Speed Status, Duplex Status, and Auto negotiation. For the selected port, the statistics table will show this information: number of packets received, number of packet bytes received, number of packets transmitted, number of packet bytes transmitted, and number of packet errors. To update the on-screen information, click the **Refresh** button. To exit this screen, click the **Close** button.

Network Setting Status

LAN IP. It shows the current LAN IP Address of the Router, as seen by internal users on the network, and it hyperlinks to the LAN Setting section on the Network page of the Setup tab.

WAN IP. These show the current WAN IP Addresses for the WAN ports of the Router, as seen by external users on the Internet. These hyperlink to the WAN setting on the Network page of the Setup tab. If a WAN port is set to *Obtain an IP automatically*, two buttons, *Release* and *Renew*, will be available. Click the **Release** button to release the IP address of a specific WAN port, and click the **Renew** button to update the DHCP Lease Time or get a new IP address. If a WAN port is set to *PPPoE* or *PPTP*, two buttons, *Connect* and *Disconnect*, will be available.

DMZ IP. It shows the current IP Address of the Router's DMZ port, as seen by external users on the Internet. It hyperlinks to the DMZ setting on the Network page of the Setup tab.

Mode. It shows the Router's Working Mode (Gateway or Router), and it hyperlinks to the Dynamic Routing section on the Advanced Routing page of the Setup tab.

DNS. It shows all DNS Server Addresses and hyperlinks to the WAN setting on the Network page of the Setup tab.

DDNS. It shows the DDNS settings of the Router's WAN ports and hyperlinks to the DDNS page of the Setup tab.

DMZ Host. It shows the DMZ Private Address and hyperlinks to the DMZ Host page of the Setup tab. The default is **Disabled**.

Firewall Setting Status

SPI (Stateful Packet Inspection). It shows the status (On/Off) of the SPI setting and hyperlinks to the General page of the Firewall tab.

DoS (Denial of Service). It shows the status (On/Off) of the DoS setting and hyperlinks to the General page of the Firewall tab.

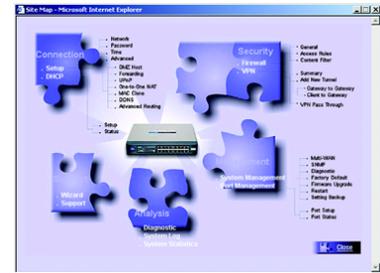


Figure 6-4: Site Map

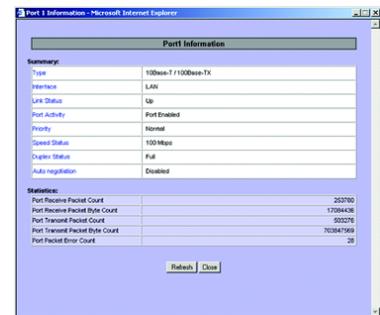


Figure 6-5: Port Information

10/100 16-Port VPN Router

Block WAN Request. It shows the status (On/Off) of the Block WAN Request setting and hyperlinks to the General page of the Firewall tab.

VPN Setting Status

VPN Summary. It hyperlinks to the Summary page of the VPN tab.

Tunnel(s) Used. It shows the number of VPN tunnels used.

Tunnel(s) Available. It shows the number of VPN tunnels available.

Current Connected (the Group Name of the GroupVPN) users. It shows the number of users. If GroupVPN is disabled, the message, "No Group VPN was defined," will be displayed.

Log Setting Status

It hyperlinks to the System Log page of the Log tab.

If you have not set up the e-mail server on the Log tab, the message, "E-mail cannot be sent because you have not specified an outbound SMTP server address," will be displayed.

If you have set up the mail server but the log has not been generated due to the Log Queue Length and Log Time Threshold settings, the message, "E-mail settings have been configured," will be displayed.

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

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

Setup Tab - Network

The *Setup* screen shows all of the Router's basic setup functions. The Router can be used in most network setups without changing any of the default values; however, you may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL or cable) carrier.

Network

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

LAN Setting

These are the Router's Device IP Address and Subnet Mask. The default values are **192.168.1.1** for the local IP address and **255.255.255.0** for the Subnet Mask.

WAN Setting

From the *WAN Setting* drop-down menu, select how many WAN ports you want to use. The default is 2, and the maximum number is 7. You can also change the number of WAN ports using the Port Setup page of the Port Management tab. If you change the number on this screen, then the number on the *Port Setup* screen will change accordingly. Make sure the network configuration matches the number of WAN port settings on this screen.

If you change the number of WAN ports, click the **Save Settings** button to save your change. A confirmation message will appear. Then click the **OK** button to save the new setting.

The WAN Setting table will display the WAN port numbers in the Interface column and their respective connection types in the Connection Type column. Click **Edit** in the Config. column to change the WAN settings of the selected WAN port. You must save the new number of WAN ports before you can click Edit to change the settings of any new WAN ports.

The Connection Type column will display the word "Undefined" if you changed the number of WAN ports but did not click the Save Settings button. After you save this setting, the Connection Type column will display, "Obtain an IP automatically." The default Connection Type of all WAN ports is **Obtain an IP automatically**.

WAN Setting Table

Interface. The WAN port number is displayed.

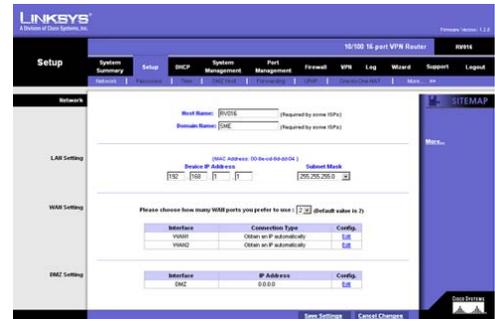


Figure 6-6: Setup Tab



Figure 6-7: Save New Number of WAN Ports

Connection Type. There are four connection types available. They are described in more detail on the following pages.

Config. Click **Edit** to change the selected WAN port's WAN settings. In the *Interface* field, you will see the WAN port number displayed. From the *WAN Connection Type* drop-down menu, choose one of the following: **Obtain an IP automatically**, **Static IP**, **PPPoE**, or **PPTP**. Depending on which connection type you select, you will see various settings.

Obtain an IP Automatically

If your ISP automatically assigns an IP address, select **Obtain an IP automatically**. Your ISP will assign these values. If you check the box for **Use the Following DNS Server Addresses**, enter your DNS server IP address(es) (you must enter at least one). Multiple DNS server IP settings are common. In most cases, the first available DNS server entry is used. Most cable modem subscribers use this connection type.

Static IP

If you are required to use a permanent IP address, select **Static IP**. Then enter your settings in the *WAN IP Address*, *Subnet Mask*, *Default Gateway Address*, and *DNS Server* fields (at least one DNS Server IP address is required). Check your service installation receipt for this information; otherwise, request these settings from your ISP.

PPPoE (Point-to-Point Protocol over Ethernet)

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable it. To enable PPPoE, follow these instructions:

1. Select **PPPoE**.
2. Enter your User Name and Password. The maximum number of characters is 60.
3. If you select the *Connect on Demand* option, the PPPoE connection will be disconnected after a specified period of inactivity (*Max Idle Time*). If you have been disconnected due to inactivity, *Connect on Demand* enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. Enter the number of minutes you want to have elapsed before your Internet access disconnects. The default is 5 minutes.

If you select the *Keep Alive* option, the Router will keep the connection alive by sending out a few data packets periodically, so your ISP thinks that the connection is still active. This option keeps your PPPoE-enabled connection active indefinitely, even when it sits idle. The default *Redial Period* is 30 seconds.

The screenshot shows the WAN settings for interface WAN3. The 'WAN Connection Type' is set to 'Obtain an IP automatically'. There is an unchecked checkbox for 'Use the Following DNS Server Addresses'. Below it, two rows of IP address input fields are shown, both containing '0.0.0.0'.

Figure 6-8: Obtain an IP Automatically

The screenshot shows the WAN settings for interface WAN3. The 'WAN Connection Type' is set to 'Static IP'. There are input fields for 'Specify WAN IP Address', 'Subnet Mask', 'Default Gateway Address', and 'DNS Server (Required) 1' and '2'. All fields contain '0.0.0.0'.

Figure 6-9: Static IP

The screenshot shows the WAN settings for interface WAN3. The 'WAN Connection Type' is set to 'PPPoE'. There are input fields for 'User Name' and 'Password'. Below them are two radio button options: 'Connect on Demand: Max Idle Time 5 Min.' (selected) and 'Keep Alive: Redial Period 30 Sec.'.

Figure 6-10: PPPoE

PPTP (Point-to-Point Tunneling Protocol)

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

1. Enter your settings in the *WAN IP Address*, *Subnet Mask*, and *Default Gateway Address* fields. This information is provided by your ISP.
2. Enter your User Name and Password. The maximum number of characters is 60.
3. If you select the *Connect on Demand* option, the PPPoE connection will be disconnected after a specified period of inactivity (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. Enter the number of minutes you want to have elapsed before your Internet access disconnects. The default is 5 minutes.

If you select the *Keep Alive* option, the Router will keep the connection alive by sending out a few data packets periodically, so your Internet service thinks that the connection is still active. This option keeps your PPPoE-enabled connection active indefinitely, even when it sits idle. The default Redial Period is 30 seconds.

DMZ Setting

The Router comes with a special DMZ port, which is used for setting up public servers. The DMZ port sits between the local network ports and the Internet port. Servers on the DMZ are publicly accessible. Use of the DMZ port is optional; it may be left unconnected.

Using the DMZ is preferred and is, if practical, a strongly recommended alternative to using public LAN servers or putting these servers on WAN ports where they are not protected and not accessible by users on the LAN.

Each of the servers on the DMZ will need a unique, public Internet IP address. The ISP you use to connect your network to the Internet should be able to provide these addresses, as well as information on setting up public Internet servers. If you plan to use the DMZ setting, contact your ISP for the static IP information.

Click **Edit** in the Config. column to edit the DMZ setting. The *Edit DMZ Connection* screen will appear.

In the *Interface* field, the DMZ port is displayed. Enter the DMZ port's settings in the *Specify DMZ IP Address* and *Subnet Mask* fields.

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

Figure 6-11: PPTP

Figure 6-12: DMZ

Setup Tab - Password

The Router's default User Name and Password is **admin**, and it is strongly recommended that you change the Router's password from the default to a unique password.

Old Password. Enter the old password. The default Password is **admin** when you first power up the Router.

(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, which will remove all of your configuration changes.)

New Password. Enter a new password for the Router. Your password must have 15 or fewer characters and cannot contain any spaces.

Confirm New Password. Re-enter the new password to confirm it.

Click the **Save Settings** button to save your new password, or click the **Cancel Changes** button to undo the change.

Setup Tab - Time

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

To set the local time, select **Set the local time using the Network Time Protocol (NTP) automatically** or **Set the local time Manually**.

Automatic

Select your time zone from the *Time Zone* drop-down menu. If you use Daylight Savings, then click the checkbox and enter the appropriate dates. Enter the URL or IP address of the NTP server in the *NTP Server* field. The default Time Zone is **Pacific Time**.

Manual

Enter the time in the *Hours*, *Minutes*, and *Seconds* fields. Then enter the date in the *Month*, *Day*, and *Year* fields.

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



Figure 6-13: Password

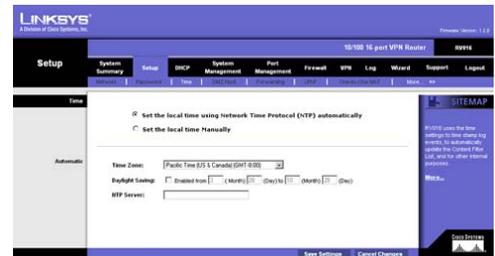


Figure 6-14: Time - Automatic

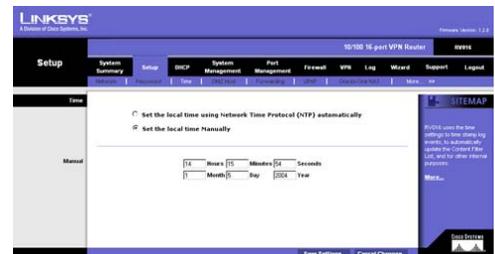


Figure 6-15: Time - Manual

Setup Tab - DMZ Host

The DMZ (Demilitarized Zone) Host feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or video conferencing. Although Port Range Forwarding can only forward 10 ranges of ports maximum, DMZ hosting forwards all the ports to one PC at the same time.

In the *DMZ Private IP Address* field, enter the local IP address of the computer you want to expose. The default value of 0 deactivates the DMZ Host.

Click the **Save Settings** button to save your change, or click the **Cancel Changes** button to undo the change.

Setup Tab - Forwarding

The *Forwarding* screen allows you to set up port range forwarding and port triggering applications. Port range forwarding can be used to set up public services or other specialized Internet applications on your network, while port triggering can be used to set up triggered ranges and forwarded ranges for Internet applications.

Port Range Forwarding

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Router can forward those requests to computers equipped to handle the requests. If, for example, you set the 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. Make 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, Internet users will be able to communicate with the server, but they will not actually be connected. The packets will simply be forwarded through the Router.

1. Select the Service you want from the pull-down menu.
2. If the Service you need is not listed in the menu, click the **Service Management** button to add the new service. The *Service Management* screen will appear. Enter a name in the *Service Name* field. From the *Protocol* drop-down menu, select the protocol it uses. Enter its range in the *Port Range* fields. Click the **Add to List** button. Then, click the **Save Setting** button to save your changes. Click the **Cancel Changes** button to cancel your changes. Click the **Exit** button to return to the *Forwarding* screen.

If you want to modify a service you have created, select it and click the **Update this service** button. Then, click the **Save Setting** button to save your changes. Click the **Exit** button to return to the *Forwarding* screen.



Figure 6-16: DMZ Host



Figure 6-17: Forwarding

If you want to delete a service you have created, select it and click the **Delete selected service** button. Then, click the **Save Setting** button to save your changes. Click the **Exit** button to return to the *Forwarding* screen.

If you want to add another service, click the **Add New** button. Enter a name in the *Service Name* field. From the *Protocol* drop-down menu, select the protocol it uses. Enter its range in the *Port Range* fields. Click the **Add to List** button. Then, click the **Save Setting** button to save your changes. Click the **Cancel Changes** button to cancel your changes. Click the **Exit** button to return to the *Forwarding* screen.

3. On the *Forwarding* screen, enter the IP address of the server that you want the Internet users to access. Then click the **Enable** checkbox to enable this port range forwarding entry.
4. Click the **Add to List** button, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click the **Delete selected application** button.

Port Triggering

Port triggering allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

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

1. For each application, complete the *Application Name*, *Trigger Port Range*, and *Incoming Port Range* fields.
2. Click the **Add to List** button, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click the **Delete selected application** button.

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. Click the **Show Tables** button to see the details of your port range forwarding and port triggering entries.

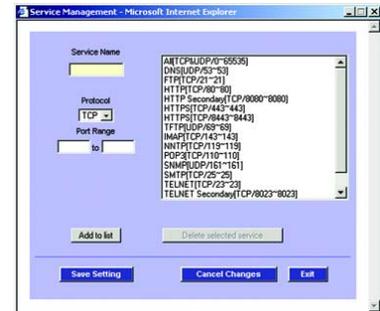


Figure 6-18: Service Management

Setup Tab - UPnP

UPnP, Universal Plug and Play, can be used to set up public services on your network. When the UPnP function is enabled, Windows XP can modify these entries via UPnP.

1. Select **Yes** to enable the UPnP function.
1. Select the Service you want from the pull-down menu.
2. If the Service you need is not listed in the menu, click the **Service Management** button to add the new service. A new screen will appear. Enter a name in the *Service Name* field. From the *Protocol* drop-down menu, select the protocol it uses. Complete the *Internal* and *External Port* fields. Click the **Add to List** button. Then, click the **Save Setting** button to save your changes. Click the **Cancel Changes** button to cancel your changes. Click the **Exit** button to return to the *UPnP* screen.

If you want to modify a service you have created, select it and click the **Update this service** button. Then, click the **Save Setting** button to save your changes. Click the **Exit** button to return to the *UPnP* screen.

If you want to delete a service you have created, select it and click the **Delete selected service** button. Then, click the **Save Setting** button to save your changes. Click the **Exit** button to return to the *UPnP* screen.

If you want to add another service, click the **Add New** button. Enter a name in the *Service Name* field. From the *Protocol* drop-down menu, select the protocol it uses. Complete the *Internal* and *External Port* fields. Click the **Add to List** button. Then, click the **Save Setting** button to save your changes. Click the **Cancel Changes** button to cancel your changes. Click the **Exit** button to return to the *UPnP* screen.

3. On the *UPnP* screen, enter the name or IP address of the server that you want the Internet users to access. Then click the **Enable** checkbox to enable this UPnP entry.
4. Click the **Add to List** button, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click the **Delete selected application** button.

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



Figure 6-19: UPnP

Setup Tab - One-to-One NAT

One-to-One NAT (Network Address Translation) creates a relationship that maps valid external addresses to internal addresses hidden by NAT. Devices with internal addresses may be accessed at the corresponding external IP addresses, as long as they are valid.

To create this relationship between internal and external addresses, define internal and external address ranges of equal length. (The Router's WAN IP address may not be included in the range of external addresses.) Once that relationship is defined, the device with the first internal address is accessible at the first IP address in the external address range, the second device at the second external IP address, and so forth.

For example, consider a LAN to which the ISP has assigned external IP addresses ranging from 209.19.28.16 to 209.19.28.31, with 209.19.28.16 used as the Router's WAN IP (NAT public) address. The internal address range of 192.168.168.1 to 192.168.168.255 is used for the devices on the LAN. Typically, only devices that have been designated as public LAN servers will be accessible from the Internet. However, with One-to-One NAT, the machines with the internal IP addresses of 192.168.168.2 to 192.168.168.15 may be accessed at the corresponding external IP addresses.

One-to-One NAT does not change how the firewall functions work. Access to LAN devices from the Internet will not be allowed unless the appropriate network access rules are established, the appropriate forwarding entries are enabled, or the appropriate authenticated user sessions are established.

Before configuring the One-to-One NAT settings, set up the appropriate Access Rules on the *Firewall - Access Rules* screen, or set up the appropriate forwarding entries on the *Setup - Forwarding* screen.

To use the One-to-One NAT feature, click the **Enable** box. To set up a One-to-One NAT entry, follow these instructions:

1. In the *Private Range Begin* field, enter the beginning IP address of the private address range being mapped. This will be the IP address of the first machine that will be accessible from the Internet.
2. In the *Public Range Begin* field, enter the beginning IP address of the public address range being mapped. (This will be assigned by the ISP.) The Router's WAN IP (NAT public) address cannot be included in this range.
3. Enter the number of IP addresses in the *Range Length* field. This number may not exceed the number of valid external IP addresses. To map a single address, use a Range Length of 1.
4. Click the **Add to list** button, and configure as many ranges as you would like, up to a maximum of 64. To delete an entry, select it and click the **Delete selected range** button.

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



Figure 6-20: One-to-One NAT

Setup Tab - MAC Clone

Some ISPs require that you register a MAC address, which is a 12-digit code assigned to a unique piece of hardware for identification. The MAC Clone feature “clones” your network adapter’s MAC address onto the Router, so you don’t have to call your ISP to change the registered MAC address to the Router’s MAC address.

The MAC Clone table displays the number of WAN ports you have configured on the *Network* or *Port Management* screen. Their MAC addresses are shown in the MAC Address column. Click the **Edit** in the Config. column to edit the MAC Clone setting of the selected WAN port. A new screen will appear.

In the *Interface* field, the WAN port number is displayed. To manually clone a MAC address, select **User Defined WAN MAC Address**, and then enter the 12 digits of your adapter’s MAC address. If you want to clone the MAC address of the PC you are currently using to configure the Router, then select **MAC Address from this PC**.

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. Click the **Back** button to return to the previous page if you want to configure the other WAN ports.



Figure 6-21: MAC Clone



Figure 6-22: Edit MAC Clone

Setup Tab - DDNS

DDNS (Dynamic Domain Name System) service allows you to assign a fixed domain name to a dynamic WAN IP address, so you can host your own web, FTP or other type of TCP/IP server in your LAN. The DDNS feature is disabled by default.

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

The DDNS table displays the number of WAN ports you have configured on the *Network* or *Port Management* screen. The status of each port's DDNS setting is shown in the DDNS Service column. Click the **Edit** in the Config. column to edit the DDNS setting of the selected WAN port. A new screen will appear.

In the *Interface* field, the WAN port number is displayed. Select **DynDNS.org** from the *DDNS Service* drop-down menu. Enter your DynDNS.org account information in the *User name* and *Password* fields. Enter your host name in the three *Host Name* fields. For example, if your host name were *myhouse.dyndns.org*, then *myhouse* would go into the first field, *dyndns* would go into the second field, and *org* would go into the last field.

Then click the **Save Settings** button, and the status of the DDNS function will be updated.

In the Internet IP Address section, the Router's current Internet IP address is displayed. Because it is dynamic, this will change.

In the Status section, the status of the DDNS function is displayed. If the status information indicates an error, make sure you have correctly entered the information for your account with DynDNS.org.

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. Click the **Back** button to return to the *DDNS* screen.



Figure 6-23: DDNS



Figure 6-24: Edit DDNS

Setup Tab - Advanced Routing

Dynamic Routing

The Router's dynamic routing feature can be used, so the Router will automatically adjust to physical changes in the network's layout. Using the dynamic RIP protocol, the Router calculates the most efficient route for the network's data packets to travel between the source and the destination, based upon the shortest paths. The RIP protocol regularly broadcasts routing information to other routers on the network. It determines the route that the network packets take based on the fewest number of hops between the source and the destination.

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. In Router Mode, any computer connected to the Router will not be able to connect to the Internet unless you have another router function as the gateway.

RIP (Routing Information Protocol). To use dynamic routing for communication of network data, click the **Enabled** radio button. Otherwise, keep the default, **Disabled**.

Receive RIP versions. To use dynamic routing for reception of network data, select the protocol you want: **None**, **RIPv1**, **RIPv2**, or **Both RIP v1 and v2**.

Transmit RIP versions. To use dynamic routing for transmission of network data, select the protocol you want: **None**, **RIPv1**, **RIPv2 - Broadcast**, or **RIPv2 - Multicast**.

Static Routing

If the Router is connected to more than one network or there are multiple routers installed on your network, it may be necessary to set up static routes. The static routing function determines the path that data follows over your network before and after it passes through the Router. You can use static routing to allow different IP domain users to access the Internet through the Router.

Static routing is a powerful feature that should be used by advanced users only. In many cases, it is better to use dynamic routing because it enables the Router to automatically adjust to physical changes in the network's layout.

If you want to use static routing, the Router's DHCP settings must be disabled. Then add routing entries to the Static Routing table. These entries tell the Router where to send all incoming packets. All of your network routers should direct the default route entry to the 10/100 16-Port VPN Router.

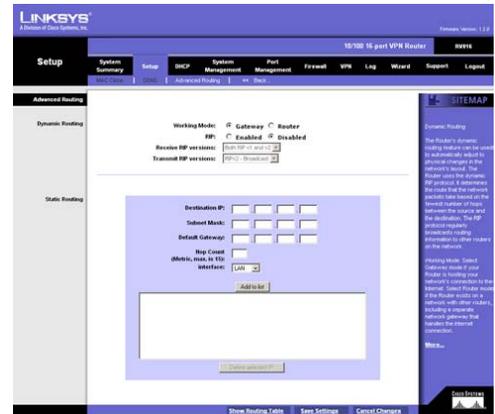


Figure 6-25: Advanced Routing

10/100 16-Port VPN Router

To create a static route entry, enter the following information:

1. In the *Destination IP* field, 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. In the *Subnet Mask* field, 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. In the *Default Gateway* field, enter the IP address of your network's gateway. If this Router is used to connect your network to the Internet, then the gateway IP is the Router's Internet IP address. If you have another router handling your network's Internet connection, enter the IP address of that router instead.
4. In the *Hop Count* field, enter the appropriate value (maximum is 15). This indicates the number of nodes that a data packet passes through before reaching its destination. A node is any device on the network, such as a switch, PC, or router.
5. From the *Interface* drop-down menu, select the appropriate interface. The Interface tells you whether your network is on the LAN or the WAN (the Internet). If you're connecting to a sub-network, select **LAN**. If you're connecting to another network through the Internet, select the appropriate WAN port option.
6. Click the **Add to list** button, and configure as many static routing entries as you would like, up to a maximum of 30. To delete an entry, select it and click the **Delete selected IP** button.

Click the **Save Settings** button to save your changes or click the **Cancel Changes** button to undo your changes. Click the **Show Routing Table** button to view the current routes and their settings.

DHCP Tab - Setup

Setup

The Router can be used as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server automatically assigns available IP addresses to computers on your network. If you choose to enable the DHCP server option, all of the PCs on your LAN must be set to obtain an IP address automatically from a DHCP server. (By default, Windows computers are set to obtain an IP automatically.)

If the Router's DHCP server function is disabled, you have to carefully configure the IP address, subnet mask, and DNS settings of every computer on your network. Be careful not to assign the same IP address to different computers.

You can also set up to 30 static IP entries on this screen.

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

Dynamic IP

Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. The range is 5-43,200 minutes.

Range Start/End. Enter a starting IP address and ending IP address to create a range of available IP addresses. The default range is 100-149. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1.2 or greater, because the default IP address for the Router is 192.168.1.1.

Static IP

Static IP Address. If necessary, you can assign a static IP address to a specific computer based on its MAC address. Complete the *Static IP Address* field.

MAC Address. Enter the MAC address of the specific computer to which you will assign a static IP address.

To add a static IP entry, click the **Add to list** button. To delete a static IP entry, select the listed entry, and click the **Delete selected Entry** button.

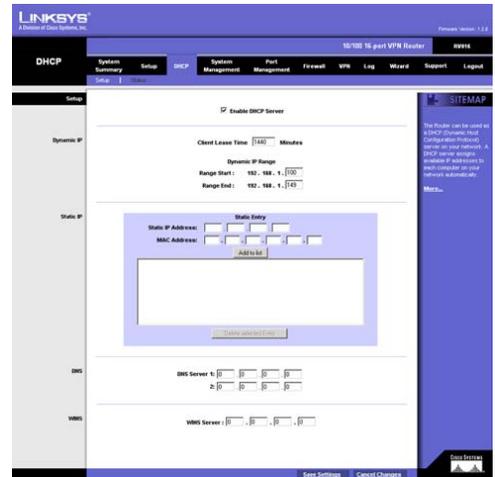


Figure 6-26: DHCP Setup

DNS

You can assign DNS server(s) to the DHCP clients so the Router will use the DNS server(s) for faster access to functioning DNS server(s). You do not need to complete either of these *DNS Server* fields; it is an optional feature.

WINS

Windows Internet Naming Service (WINS) is a service that resolves NetBIOS names to IP addresses. WINS is assigned if the computer (DHCP client) requests one. If you do not know the IP address of the WINS server, keep the default, **0.0.0.0**.

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

DHCP Tab - Status

A Status page is available so you can view the status information for the DHCP server and its clients.

Status

For the DHCP server, the following information is shown:

- DHCP Server. This is the IP address of the DHCP server.
- Dynamic IP Used. It shows the number of dynamic IP addresses used.
- Static IP Used. It shows the number of static IP addresses used.
- DHCP Available. This indicates the number of dynamic IP addresses available.
- Total. It shows the total number of dynamic IP addresses that can be assigned by the DHCP server.

Client Table

For all network clients using the DHCP server, the Client Table shows the current DHCP Client information:

- Client Host Name. This is the name assigned to a client host.
- IP Address. It is the dynamic IP address assigned to a client.
- MAC Address. This indicates the MAC address of a client.
- Leased Time. It displays the amount of time a network user will be allowed connection to the Router with their current dynamic IP address.

Click the **Trash Can** icon to delete a DHCP client, and the client host's IP address will be released. Click the **Refresh** button to refresh the on-screen information.



Figure 6-27: DHCP Status

System Management Tab - Multi-WAN

Load Balance

For the Load Balance feature, you have a choice of Intelligent Balancer (Auto Mode) and IP Group (By Users), except for WAN1. The Router reserves at least one WAN port for non-IP Group users, so WAN1 will always be set to Intelligent Balancer (Auto Mode).

If you change the Router's Load Balance Mode, a confirmation message will appear. You have to save this change before you can change the settings of any WAN ports.

Intelligent Balancer (Auto Mode)

Select the **Intelligent Balancer (Auto Mode)** setting if you want all WAN ports to be in Auto Mode. The Router will automatically compute the maximum bandwidth of all WAN ports by using Weighted Round Robin to balance the loading.

In the Interface Setting table, the number of each WAN port is shown in the Interface column. Its Load Balance Mode is displayed in the Mode column. Click the **Edit** in the Config. column to edit the Load Balance setting of the selected WAN port. The *Edit Load Balance* screen will appear.

In the *Interface* field, the WAN port number is displayed. For the Max. Bandwidth provided by ISP setting, select **64K, 128K, 256K, 384K, 512K, 1024K, 1.5M, 2M, or 2.5M or above** from the *Upstream* drop-down menu. From the *Downstream* drop-down menu, select **512K, 1024K, 1.5M, 2M, or 2.5M or above**.

You can enable the Router to check the network service layer using DNS lookup. This tool can detect the network connection status of the ISP if you have set up the DNS server in the Network section of the Setup page. If you did not set up the DNS server, the checkbox will be grayed out, and then you cannot use the DNS lookup tool. The default is unchecked. To use this tool, enter the host name and select the appropriate option from the *When Fail* drop-down menu. Using DNS lookup, the Router will check the network service layer every 15 minutes to see if the network connection to your ISP is active.

The *When Fail* drop-down menu offers two options. If the connection is not active, the Router will generate a system log or suspend this WAN interface. For the *Generate System Log* setting, the Router will generate a system log when DNS lookup fails to inform you that the ISP connection may be disconnected. For the *Suspend this WAN Interface* setting, the Router will suspend this WAN interface when the network connection to your ISP is not active. The traffic on this WAN will be dispatched to the other WAN ports in Auto Mode. When the ISP connection is re-established, traffic will return to this WAN interface.



Figure 6-28: Multi-WAN Load Balance

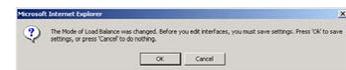


Figure 6-29: Save New Mode



Figure 6-30: Intelligent Balancer - Edit Load Balance

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. To return to the *Load Balance* screen, click the **Back** button.

IP Group (By Users)

IP Group (By Users) mode enables you to group traffic by different priority levels or classes of service (CoS). It can ensure bandwidth and higher priority for the specific IP addresses of important users, and the IP Group users don't need to share bandwidth with lower classification users who use Intelligent Balancer mode.

In the Interface Setting table, the number of each WAN port is shown in the Interface column. If you have set the IP Group for a selected WAN port, it will show the message, "Dispatched by user" in the Mode column. If you did not set the IP Group for a selected WAN port, it will show the message, "Dispatched by system" in the Mode column.

After you have selected IP Group (By Users), then click the **Edit** in the Config. column to edit the Mode setting of the selected WAN port. The *Edit Load Balance* screen will appear.

In the *Interface* field, the WAN port number is displayed. For the Max. Bandwidth provided by ISP setting, select **64K, 128K, 256K, 384K, 512K, 1024K, 1.5M, 2M, or 2.5M or above** from the *Upstream* drop-down menu. From the *Downstream* drop-down menu, select **512K, 1024K, 1.5M, 2M, or 2.5M or above**.

You can enable the Router to check the network service layer using DNS lookup. This tool can detect the network connection status of the ISP if you have set up the DNS server in the Network section of the Setup page. If you did not set up the DNS server, the checkbox will be grayed out, and then you cannot use the DNS lookup tool. The default is unchecked. To use this tool, enter the host name and select the appropriate option from the *When Fail* drop-down menu. Using DNS lookup, the Router will check the network service layer every 15 minutes to see if the network connection to your ISP is active.

The *When Fail* drop-down menu offers two options. If the connection is not active, the Router will generate a system log or suspend this WAN interface. For the *Generate System Log* setting, the Router will generate a system log when DNS lookup fails to inform you that the ISP connection may be disconnected. For the *Suspend this WAN Interface* setting, the Router will suspend this WAN interface when the network connection to your ISP is not active. The traffic on this WAN will be dispatched to the other WAN ports in Auto Mode. When the ISP connection is re-established, traffic will return to this WAN interface.

To add an IP range, follow these instructions:

1. Enter the beginning IP address of the range in the *Address* field.
2. Enter the number of users in the *Range* field.



Figure 6-31: IP Group (By Users)



Figure 6-32: IP Group (By Users) - Edit Load Balance

10/100 16-Port VPN Router

3. Check the **IP user will be redirected when link fail** box. When checked, the IP users' traffic will be redirected to the backup link when the initial link fails. When unchecked, the IP users' traffic will not be redirected. The default is a checkmark.
4. Click the **Add to list** button, and configure as many IP range entries as you would like, up to a maximum of 30. To delete an entry, select it and click the **Delete selected range** button.

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. To return to the *Load Balance* screen, click the **Back** button.

System Management Tab - SNMP

SNMP, Simple Network Management Protocol, is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network. The Router supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups. The Router replies to SNMP Get commands for MIBII via any LAN (local) interface and supports a custom MIB for generating trap messages.

To enable SNMP, keep the *Enable* box checked. To disable the SNMP agent, remove the checkmark.

To configure SNMP, complete all fields on this screen.

System Name. Enter the hostname of the Router.

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

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

Get Community Name. Create a name for the group or community of administrators who can view the Router's SNMP data. The default name is **public**.

Set Community Name. Create a name for the group or community of administrators who can receive the Router's SNMP traps. The default name is **private**. A name must be entered in this field.

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

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

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



Figure 6-33: SNMP

System Management Tab - Diagnostic

The Router has two built-in tools, DNS Name Lookup and Ping, which are used for troubleshooting network problems.

The Internet has a service called the Domain Name Service (DNS), which allows users to enter an easily remembered host name, such as `www.linksys.com`, instead of numerical TCP/IP addresses to access Internet resources. The Router's DNS Name Lookup tool will return the numerical TCP/IP address of a host name.

The ping test bounces a packet off a machine on the Internet back to the sender. This test shows if the Router is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try ping the DNS server or other machine at the ISP's location. If this test is successful, try ping devices outside the ISP. This will show if the problem lies with the ISP's connection.

Select which tool you want to use, **DNS Name Lookup** or **Ping**.

DNS Name Lookup

Before using this tool, make sure the IP address of the DNS server is entered on the Network page of the Setup tab; otherwise, this tool will not work.

Enter the host name in the *Look up the name* field, and click the **Go** button. (Do not add the prefix `http://` or else you will get an error message.) The Router will then query the DNS server and display the result at the bottom of the screen.

Ping

Before using this tool make sure you know the device or host's IP address. If you do not know it, use the Router's DNS Name Lookup tool to find the IP address.

In the *Ping host or IP address* field, enter the IP address of the device being pinged, and click the **Go** button. The test will take a few seconds to complete. When completed, the Router will display the results at the bottom of the screen. The results include this information: number of packets transmitted, received, or lost, as well as round trip time (minimum, maximum, and average).



Figure 6-34: DNS Name Lookup

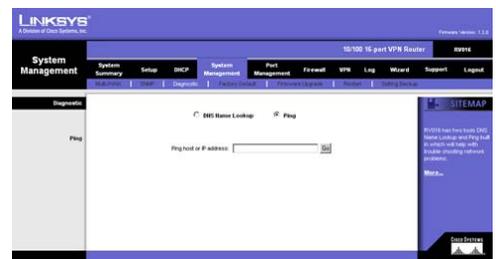


Figure 6-35: Ping

System Management Tab - Factory Default

Use this screen 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 the settings and preferences that you have configured.

Click the **Return to Factory Default Setting** button if you want to restore the Router to the factory default settings. After clicking the button, a confirmation screen will appear. Click the **OK** button to continue.

System Management Tab - Firmware Upgrade

Firmware Upgrade

You can use this feature to upgrade the Router's firmware to the latest version. To download the firmware, refer to the Firmware Download section. If you have already downloaded the firmware onto your computer, then click the **Browse** button to look for the file. Then click the **Firmware Upgrade Right Now** button.

Firmware Download

If you need to download the latest version of the Router's firmware, click the **Firmware Download from Linksys Web Site** button. You will see the Support page of the Linksys website. Select the 10/100 16-Port VPN Router from the pull-down menu, and choose the firmware from the available options. After downloading the firmware, follow the Firmware Upgrade instructions.



Figure 6-36: Factory Default



Figure 6-37: Confirm Return to Factory Default Settings



Figure 6-38: Firmware Upgrade

System Management Tab - Restart

If you need to restart the Router, it is highly recommended that you use the Restart tool on this screen. When you restart from the *Restart* screen, then the Router will send out your log file before it is reset.

Before restarting the Router, decide which firmware version you want the Router to use. The Active Firmware Version is the one currently used by the Router. The Backup Firmware Version may be the same as the active one, or it may be an older version if you have upgraded the Router's firmware. Select which firmware version you want the Router to use, the **Active Firmware Version** or **Backup Firmware Version**. Then click the **Restart Router** button to restart the Router.



Figure 6-39: Restart

System Management Tab - Setting Backup

This screen allows you to make a backup file of your preferences file for the Router. To save the backup file, you need to export the configuration file. To use the preferences file, you need to import the configuration file.

Import Configuration File

To import a configuration file, first specify where your preferences file is located. Click the **Browse** button, and a dialog box will appear and ask you to select the appropriate configuration file. After you select the file, click the **Import** button. This process may take up to a minute. Then you will need to restart the Router so the changes will take effect.

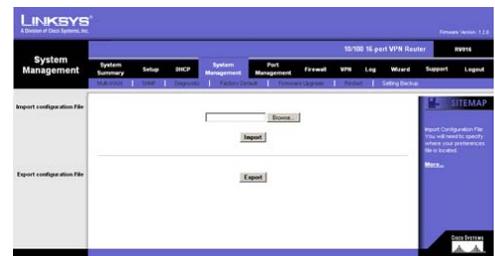


Figure 6-40: Setting Backup

Export Configuration File

To export the Router's current configuration file, click the **Export** button, and a dialog box will appear and ask you to select a location where you would like to store your preferences file. This file will be called *RV016.exp* by default, but you may rename it if you wish. This process may take up to a minute.

Port Management Tab - Port Setup

On this screen you can choose the number of WAN ports the Router will provide and configure the connection settings for each port, such as priority, speed, and duplex. You can also enable or disable the auto-negotiation feature for all ports.

From the drop-down menu, select how many WAN ports you prefer to use. The default is 2, while the maximum is 7. You can also change the number of WAN ports using the Network page of the Setup tab. If you change the number on this screen, then the number on the *Network* screen will change accordingly. Make sure the network configuration matches the number of WAN port settings on this screen.

If you change the number of WAN ports, a confirmation message will appear. Make sure your network configuration matches the new WAN settings. Then click the **OK** button to save the new setting.

The Basic Per Port Config. table will display the WAN port numbers in the Port ID column and their respective settings in the Interface, Disable, Priority, Speed, and Duplex columns. Click **Enable** in the Auto Negotiation column if you want the Router's ports to auto-negotiate connection speeds and duplex mode; then you will not need to set up speed and duplex settings separately.

Basic Per Port Config. Table

Port ID. The port number or name is displayed.

Interface. The port's interface type is shown here.

Disable. You can select specific ports to disable. Click the checkbox to disable a specific port.

Priority. From the drop-down menu, select **High** or **Normal** for port-based QoS (Quality of Service). QoS is used to maximize network performance, and this setting allows you to prioritize performance on all ports.

Speed. You can manually configure each port's speed as 10Mbps or 100Mbps.

Duplex. You can manually configure each port's duplex mode as half-duplex or full-duplex.

Auto Negotiation. You can set each port to auto-negotiation mode, so you will not need to set up speed and duplex settings separately.

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

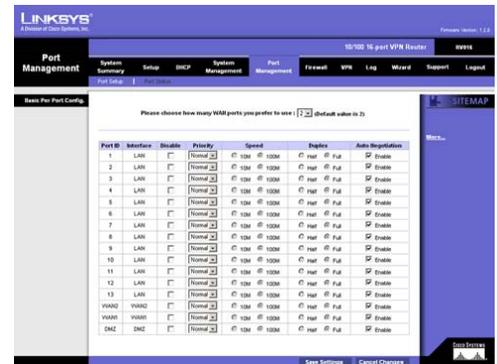


Figure 6-41: Port Setup

Port Management Tab - Port Status

To see the status information and settings for a specific port, select its ID number or name from the *Port ID* drop-down menu.

For the selected port, the Summary table will show these settings: Type, Interface, Link Status, Port Activity, Priority, Speed Status, Duplex Status, and Auto negotiation.

For the selected port, the Statistics table will show these statistics: number of packets received, number of packet bytes received, number of packets transmitted, number of packet bytes transmitted, and number of packet errors.

Click the **Refresh** button to retrieve the most recent settings and statistics.



Figure 6-42: Port Status

Firewall Tab - General

Using the screens of the Firewall tab, you can configure the Router to block or allow Internet access for specific internal users. You can also configure the Router to block or allow access to internal servers for specific Internet users. On the *Access Rules* screen, you can set up different packet filters for various users located on the internal network (LAN) or external network (WAN or Internet) based on their IP addresses or their network port numbers.

Firewall. The firewall is enabled by default. If you disable the firewall, then the SPI, DoS, and Block WAN Request features as well as the Access Rules and Content Filters will also be disabled, and the Remote Management feature will be enabled.

SPI (Stateful Packet Inspection). The SPI feature is enabled by default. The Router's firewall uses Stateful Packet Inspection to review the 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). The DoS feature is enabled by default. It protects 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 enabled by default and is designed to prevent attacks through the Internet. When it is enabled, the Router will drop both unaccepted TCP request and ICMP packets from the WAN side. Hackers will not find the Router by pinging the WAN IP address. If the Router's DMZ feature is enabled, then the Block WAN Request feature will be disabled.

Remote Management. The Router supports remote management. This feature is disabled by default. If you want to manage this Router through a WAN connection, click **Enable**. Then select the port number you want to use (port 80 or port 8080 is usually used for remote management).

Multicast Pass Through. IP Multicasting occurs when a single data transmission is sent to multiple recipients at the same time. This feature is disabled by default. If it is enabled, then the Router allows IP multicast packets to be forwarded to the appropriate computers.

MTU (Maximum Transmission Unit). This feature specifies the largest packet size permitted for network transmission. It is recommended that you use the Auto option; however, you may manually set the MTU value. The default MTU size is **1500** bytes.

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



Figure 6-43: General Firewall

Firewall Tab - Access Rules

Access Rules evaluate network traffic to decide whether or not it is allowed to pass through the Router's firewall. Access Rules look specifically at a data transmission's source IP address, destination IP address, and IP protocol type, and you can apply each Access Rule according to a different schedule.

With the use of custom rules, it is possible to disable all firewall protection or block all access to the Internet, so use extreme caution when creating or deleting Access Rules.

The Router has the following Default Rules:

- All traffic from the LAN to the WAN is allowed.
- All traffic from the WAN to the LAN is denied.
- All traffic from the LAN to the DMZ is allowed.
- All traffic from the DMZ to the LAN is denied.
- All traffic from the WAN to the DMZ is allowed.
- All traffic from the DMZ to the WAN is allowed.

Custom rules can be created to override the above Default Rules, but there are four additional default rules that will be always active and cannot be overridden by any custom rules.

- HTTP service from the LAN to the Router is always allowed.
- DHCP service from the LAN is always allowed.
- DNS service from the LAN is always allowed.
- Ping service from the LAN to the Router is always allowed.

Except for the Default Rules, all configured Access Rules are listed in the Access Rules table, and you can set the priority for each custom rule. The Access Rules table lists the following information for each Access Rule: Priority, Enable status, Action, Service, Source Interface, Source, Destination, Time, and Day. Click the **Edit** button to edit an Access Rule, and click the **Trash Can** icon to delete an Access Rule. If the Access Rules table has multiple pages, select a different page to view from the *Jump to* drop-down menu. If you want more or fewer entries listed per page, select a different number from the *entries per page* drop-down menu.

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

Click **Add New Rule** button to add new Access Rules, and the *Add a New Access Rule* screen will appear. Click the **Restore to Default Rules** button to restore the Default Rules and delete the custom Access Rules.



Figure 6-44: Access Rules

Add a New Rule

Services. If you need help to set up the Access Rules, click the **Wizard** button. For more details, see the Wizard Tab section. Otherwise, follow these instructions:

1. For the Action setting, select **Allow** or **Deny** from the pull-down menu, depending on the purpose of the Access Rule.
2. Select the service you want from the *Service* pull-down menu. If the Service you need is not listed in the menu, click the **Service Management** button to add the new service. A new screen will appear. Enter a name in the *Service Name* field. From the *Protocol* drop-down menu, select the protocol it uses. Enter its range in the *Port Range* fields. Click the **Add to List** button. Then, click the **Save Setting** button to save your changes. Click the **Cancel Changes** button to cancel your changes. Click the **Exit** button to return to the *Add a New Access Rule* screen.

If you want to modify a service you have created, select it and click the **Update this service** button. Then, click the **Save Setting** button to save your changes. Click the **Exit** button to return to the *Add a New Access Rule* screen.

If you want to delete a service you have created, select it and click the **Delete selected service** button. Then, click the **Save Setting** button to save your changes. Click the **Exit** button to return to the *Add a New Access Rule* screen.

If you want to add another service, click the **Add New** button. Enter a name in the *Service Name* field. From the *Protocol* drop-down menu, select the protocol it uses. Enter its range in the *Port Range* fields. Click the **Add to List** button. Then, click the **Save Setting** button to save your changes. Click the **Cancel Changes** button to cancel your changes. Click the **Exit** button to return to the *Add a New Access Rule* screen.

3. For this service, you can decide whether or not you want the Router to keep a log tracking this type of activity. To keep a log, select **Log packets matching this access rule**. If you don't want a log, select **Do not log packets matching this access rule**.
4. Select the appropriate Source Interface (LAN, DMZ, Any, WAN1, WAN2...) from the pull-down menu. (The WAN ports available depend on the number of WAN ports set on the *Network* or *Port Management* screen.)
5. Select the Source IP address(es) for this Access Rule. If it can be any IP address, select **Any**. If it is one IP address, select **Single** and enter the IP address in the *Source IP* fields. If it is a range of IP addresses, select **Range**, and enter the IP addresses in the *Source IP* fields.

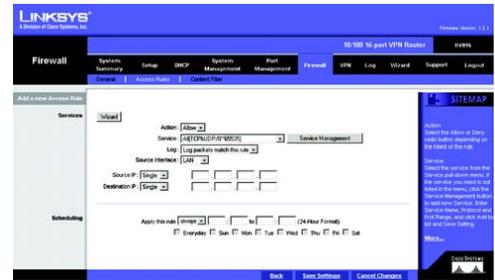


Figure 6-45: Add a New Access Rule

10/100 16-Port VPN Router

6. Select the Destination IP address(es) for this Access Rule. If it can be any IP address, select **Any**. If it is one IP address, select **Single** and enter the IP address in the *Destination IP* fields. If it is a range of IP addresses, select **Range**, and enter the IP addresses in the *Destination IP* fields.
7. Decide when you want this Access Rule to be enforced, and enter the hours and minutes in 24-hour format. The default condition for any new rule is to always enforce it.

Decide which days of the week you want the Access Rule to be enforced, and select the appropriate days.

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. Click the **Back** button to return to the *Access Rules* screen.

Firewall Tab - Content Filter

Use this screen to block specific domains during the designated days and times.

When the *Block Forbidden Domains* checkbox is selected, the Router will forbid access to websites on the Forbidden Domains list. To add a domain to the list, enter the address of the domain in the *Add* field, and then click the **Add to list** button. To remove a domain from the list, select the domain, and click the **Delete selected domain** button.

When will this content filter be in effect? If you want the content filter enforced 24 hours a day, keep the default, **always**, or enter a range of hours and minutes to designate the enforcement period. Then select the day(s) of the week you want the content filter enforced. If you want the content filter enforced daily, then keep the default, **Everyday**. For example, you could configure the Router to filter employee Internet access during normal business hours, but allow unrestricted access at night and on weekends. The default condition is to always enforce it.

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

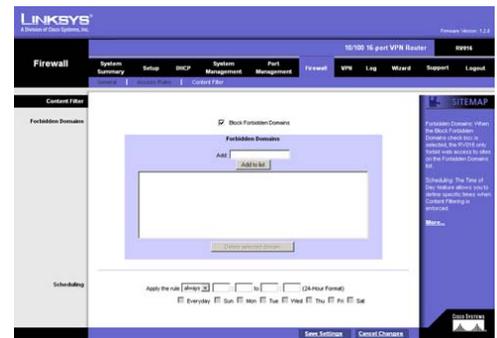


Figure 6-46: Content Filter

VPN Tab - Summary

This screen displays general information about the VPN tunnels and GroupVPNs.

Summary. This shows the number of VPN Tunnel(s) Used and Tunnel(s) Available. The Router supports up to 50 tunnels.

Detail. Click the **Detail** button to see additional information about the VPN tunnels. For each tunnel, you can view its Name, Status, Phase 2 Encryption/Authentication/Group, Local Group, Remote Group, and Remote Gateway. You can save or print this screen. Click the **Close** button to exit this screen.

Tunnel Status

Add New Tunnel. Click the **Add New Tunnel** button to add a Gateway-to-Gateway tunnel or a Client-to-Gateway tunnel. A new screen will appear and show the two types of VPN tunnels you can create.

Select the kind of tunnel you want to add.

Gateway to Gateway. The Gateway-to-Gateway tunnel is a tunnel created between two VPN Routers or other VPN devices. Click the **Add Now** button to see the *Gateway to Gateway* screen. Proceed to the Gateway to Gateway section for further instructions.

Client to Gateway. The Client to Gateway tunnel is a tunnel created between the VPN Router and the client host who is using VPN client software that supports IPSec. Click the **Add Now** button to see the *Client to Gateway* screen. Proceed to the Client to Gateway section for further instructions.

After you have added the VPN tunnels, you will see them listed in the Tunnel table, which describes all VPN tunnels, including the tunnels defined under GroupVPN. If the Tunnel table has multiple pages, you can click *Previous page* or *Next page* to jump to the page that you want to see. You can also select a different page to view from the *Jump to* drop-down menu. If you want more or fewer entries listed per page, select a different number from the *entries per page* drop-down menu.

Tunnel No. It shows the number of the VPN tunnel.

Tunnel Name. It shows the Tunnel Name that you gave the VPN tunnel or group VPN.

Status. This indicates the status of the VPN tunnel.

If you selected Manual Keying Mode in the IPSec Setup section, then the status will display the message, "Manual," and there will be no Tunnel Test function available.



Figure 6-47: VPN Summary



Figure 6-48: VPN Tunnel Details

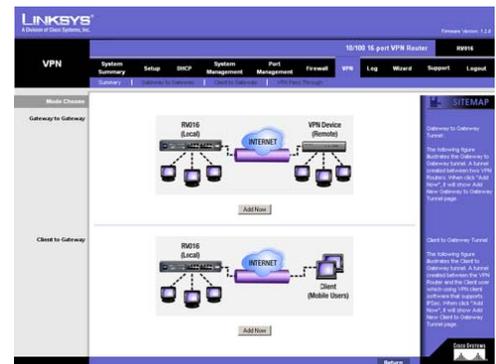


Figure 6-49: Types of VPN Tunnels

10/100 16-Port VPN Router

Phase2 Enc/Auth/Grp. This shows the Phase 2 Encryption type (DES/3DES), Authentication method (MD5/SHA1), and DH Group number (1/2/5) that you chose in the IPsec Setup section.

If you selected Manual Keying Mode in the IPsec Setup section, then there is no Phase 2 DH Group, so only the Encryption type and Authentication method will be displayed.

Local Group. This shows the IP address and subnet mask of the Local Group.

Remote Group. The IP address and subnet mask of the Remote Group are displayed here.

Remote Gateway. It shows the IP address of the Remote Gateway.

Tunnel Test. Click the **Connect** button to verify the status of the VPN tunnel. The test result will be updated in the Status column. If the tunnel is connected, a **Disconnect** button will be available so you can terminate the VPN connection. (If you selected Manual Keying Mode in the IPsec Setup section, the Tunnel Test will not be available.)

Config. Click the **Edit** button to open a new screen where you can change the tunnel's settings. Refer to the Gateway to Gateway or Gateway to Client section for more information. Click the **Trash Can** icon to delete all of your tunnel settings for each individual tunnel.

Tunnel(s) Enabled and Tunnel(s) Defined. These read-only fields show the number of VPN tunnels that are enabled and number of VPN tunnels that are defined. The number of tunnels enabled may be fewer than the number of tunnels defined because you can disable any of the tunnels that you have defined.

GroupVPN Status

If you did not enable any Group VPN connections, then none will be listed in the GroupVPN table.

Group Name. It shows the name you gave the Group VPN on the *Client to Gateway* screen.

Connected Tunnels. This shows the number of connected tunnels.

Phase2 Enc/Auth/Grp. This shows the Phase 2 Encryption type (DES/3DES), Authentication method (MD5/SHA1), and DH Group number (1/2/5) that you chose in the IPsec Setup section.

Local Group. This shows the IP address and subnet mask of the Local Group.

Remote Client. The remote client setup that you've chosen will be displayed here.

Remote Client Status. If you click the **Detail List** button, you will see information about this Group VPN. You can view its Group Name, IP address, and Connection Time. Click the **Refresh** button to update the status information. Click the **Close** button to exit this screen.

Chapter 6: Setting up and Configuring the Router
VPN Tab - Summary



Figure 6-50: GroupVPN List

10/100 16-Port VPN Router

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

Config. Click the **Edit** button to open a new screen where you can change the tunnel's settings. Click the **Trash Can** icon to delete all of your tunnel settings.

VPN Tab - Gateway to Gateway

Use this screen to create a new tunnel between two VPN devices.

Add a New Tunnel

Tunnel No. A tunnel number between 1-50 will be automatically generated.

Tunnel Name. Enter a name for this VPN tunnel, such as Los Angeles Office, Chicago Branch, or New York Division. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

Interface. Select the appropriate Interface (WAN1, WAN2...) from the pull-down menu. If you designate more than two WAN ports on the Network or Port Management page, then additional WAN ports will be available.

Enable. Check this box to enable a VPN tunnel. (When creating a VPN tunnel, this checkbox will be disabled.)

Local Group Setup

Local Security Gateway Type

Select one of these five available types: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**.

(If you want to use a Fully Qualified Domain Name (FQDN) for authentication but you do not have one, visit www.dyndns.org to set up a Dynamic Domain Name System (DDNS) account. Then enable and configure the 10/100 16-Port VPN Router's DDNS settings on the **DDNS** screen.)

The Local Security Gateway Type you select should match the Remote Security Gateway Type selected on the VPN device at the other end of the tunnel.

After you have selected the Local Security Gateway Type, the settings available on this screen may change, depending on which selection you have made.

Chapter 6: Setting up and Configuring the Router
VPN Tab - Gateway to Gateway

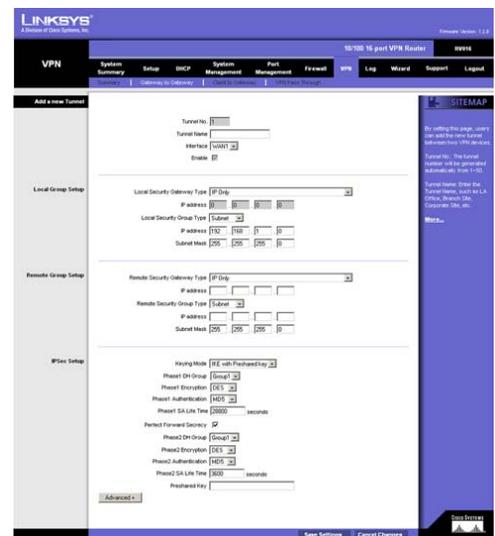


Figure 6-51: Gateway to Gateway

IP Only. If you select IP Only, then only the computer with a specific IP address will be able to access the tunnel. The WAN (or Internet) IP address of the Router will automatically appear in the *IP address* field.

IP + Domain Name(FQDN) Authentication. If you select this type, enter the FQDN (Fully Qualified Domain Name) in the *Domain Name* field, and an IP address will automatically appear in the *IP address* field. The FQDN is the host name and domain name for a specific computer on the Internet. An example of a FQDN is *vpn.mypnserver.com*. The FQDN and IP address must match the FQDN and IP address of the Remote Security Gateway type selected on the remote VPN device at the other end of the tunnel. The FQDN and IP can be used for only one tunnel connection.

IP + E-mail Addr.(USER FQDN) Authentication. If you select this type, enter the appropriate e-mail address in the *E-mail address* fields, and an IP address will automatically appear in the *IP address* field.

Dynamic IP + Domain Name(FQDN) Authentication. If the Local Security Gateway has a dynamic IP and you want to use the Domain Name for authentication, then select this type. When the Remote Security Gateway asks to create a tunnel with the Router, the Router will work as a responder. For authentication, complete the *Domain Name* field, and make sure it matches the Domain Name set on the Remote Security Gateway of the remote VPN device. The Domain Name can be used for only one tunnel connection, so you can't use the same Domain Name to create another new tunnel connection.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication. If the Local Security Gateway has a dynamic IP and you want to use the e-mail address for authentication, then select this type. When the Remote Security Gateway asks to create a tunnel with the Router, the Router will work as a responder. For authentication, enter the appropriate e-mail address in the *E-mail address* fields.

Local Security Group Type

Select the local LAN user(s) behind the Router that can use this VPN tunnel. Select one of these three available types: **IP**, **Subnet**, or **IP Range**. The Local Security Group Type you select should match the Remote Security Group Type selected on the VPN device at the other end of the tunnel.

After you have selected the Local Security Group Type, the settings available on this screen may change, depending on which selection you have made.

IP. If you select IP, then only the computer with a specific IP address will be able to access the tunnel. Enter the appropriate IP address. The default IP is **192.168.1.0**.

Subnet. If you select Subnet, which is the default, then all computers on the local subnet will be able to access the tunnel. Complete the *IP address* and *Subnet Mask* fields. The default IP is **192.168.1.0**, and the default Subnet Mask is **255.255.255.0**.

Figure 6-52: Local Security Gateway Type - IP Only

Figure 6-53: Local Security Gateway Type - IP + Domain Name (FQDN) Authentication

Figure 6-54: Local Security Gateway Type - IP + E-mail Addr. (USER FQDN) Authentication

Figure 6-55: Local Security Gateway Type - Dynamic IP + Domain Name (FQDN) Authentication

Figure 6-56: Local Security Gateway Type - Dynamic IP + E-mail Addr. (USER FQDN) Authentication

Figure 6-57: Local Security Group Type - IP

Figure 6-58: Local Security Group Type - Subnet

IP Range. If you select IP Range, then you can specify a range of IP addresses within the subnet that will be able to access the tunnel. Complete the *IP range* fields. The default IP range is **192.168.1.0~254**.

Remote Group Setup

Before you configure the Remote Group Setup, make sure your VPN tunnel will have two different IP subnets. For example, if the local 10/100 16-Port VPN Router has an IP scheme of 192.168.1.x (x being a number from 1 to 254), then the remote VPN router should have a different IP scheme, such as 192.168.2.y (y being a number from 1 to 254). Otherwise, the IP addresses will conflict, and the VPN tunnel cannot be created.

Remote Security Gateway Type

Select one of these five available types: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**.

(If you want the remote VPN router to use a Fully Qualified Domain Name (FQDN) for authentication but it does not have one, visit www.dyndns.org to set up a Dynamic Domain Name System (DDNS) account. Then enable and configure the remote VPN router's DDNS feature.)

The Remote Security Gateway Type you select should match the Local Security Gateway Type selected on the VPN device at the other end of the tunnel.

After you have selected the Remote Security Gateway Type, the settings available on this screen may change, depending on which selection you have made.

IP Only. If you select IP Only, then only the computer with a specific IP address will be able to access the tunnel. In the *IP address* field, enter the IP address of the remote VPN device at the other end of the tunnel. (This must be a static or fixed IP address only.)

IP + Domain Name(FQDN) Authentication. If you select this type, enter the FQDN (Fully Qualified Domain Name) and IP address of the remote VPN device at the other end of the tunnel. (Enter the FQDN in the *Domain Name* field, and enter the IP address in the *IP address* field.) The FQDN is the host name and domain name for a specific computer on the Internet. An example of a FQDN is `vpn.remotevpnserver.com`. The FQDN and IP address must match the FQDN and IP address of the Local Security Gateway type selected on the remote VPN device at the other end of the tunnel. The FQDN and IP can be used for only one tunnel connection.

IP + E-mail Addr.(USER FQDN) Authentication. If you select this type, enter the e-mail address and IP address of the remote VPN device at the other end of the tunnel.

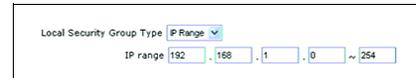


Figure 6-59: Local Security Group Type - IP Range



Figure 6-60: Remote Security Gateway Type - IP Only

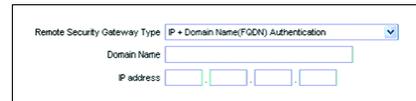


Figure 6-61: Remote Security Gateway Type - IP + Domain Name (FQDN) Authentication



Figure 6-62: Remote Security Gateway Type - IP + E-mail Addr. (USER FQDN) Authentication

Dynamic IP + Domain Name(FQDN) Authentication. If the Remote Security Gateway has a dynamic IP and you want to use the Domain Name for authentication, then select this type. When the Remote Security Gateway asks to create a tunnel with the Router, the Router will work as a responder. For authentication, complete the *Domain Name* field, and make sure it matches the Domain Name set on the Local Gateway of the remote VPN device. (The Remote Security Gateway has a dynamic IP, so you do not need to enter an IP address.) The Domain Name can be used for only one tunnel connection, so you can't use the same Domain Name to create another new tunnel connection.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication. If the Remote Security Gateway has a dynamic IP and you want to use the e-mail address for authentication, then select this type. When the Remote Security Gateway asks to create a tunnel with the Router, the Router will work as a responder. For authentication, enter the appropriate e-mail address in the *E-mail address* fields. (The Remote Security Gateway has a dynamic IP, so you do not need to enter an IP address.)

Remote Security Group Type

Select the Remote Security Group behind the Remote Gateway that can use this VPN tunnel. Select one of these three available types: **IP**, **Subnet**, or **IP Range**. The Remote Security Group Type you select should match the Local Security Group Type selected on the VPN device at the other end of the tunnel.

After you have selected the Remote Security Group Type, the settings available on this screen may change, depending on which selection you have made.

IP. If you select IP, then only the computer with a specific IP address will be able to access the tunnel. Enter the appropriate IP address.

Subnet. If you select Subnet, which is the default, then all computers on the remote subnet will be able to access the tunnel. Complete the *IP address* and *Subnet Mask* fields. The default Subnet Mask is **255.255.255.0**.

IP Range. If you select IP Range, then you can specify a range of IP addresses within the subnet that will be able to access the tunnel. Complete the *IP range* fields.

IPSec Setup

In order for any encryption to occur, the two ends of a VPN tunnel must agree on the methods of encryption, decryption, and authentication. This is done by sharing a key to the encryption code. For key management, there are two modes available; select **IKE with Preshared Key** or **Manual**. Both ends of a VPN tunnel must use the same mode of key management.

Figure 6-63: Remote Security Gateway Type - Dynamic IP + Domain Name (FQDN) Authentication

Figure 6-64: Remote Security Gateway Type - Dynamic IP + E-mail Addr. (USER FQDN) Authentication

Figure 6-65: Remote Security Group Type - IP

Figure 6-66: Remote Security Group Type - Subnet

Figure 6-67: Remote Security Group Type - IP Range

After you have selected the Keying Mode, the settings available on this screen may change, depending on the selection you have made.

IKE with Preshared Key

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

Phase 1 DH Group. Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol 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, and Group 2 is 1,024 bits. 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. Select a method of encryption, **DES** or **3DES**. The encryption method determines the length of the key used to encrypt or decrypt ESP packets. DES uses 56-bit encryption, and 3DES uses 168-bit encryption. 3DES is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

Phase 1 Authentication. Select a method of authentication, **MD5** or **SHA**. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

Phase 1 SA Life Time. Configure the length of time a VPN tunnel is active in Phase 1. The default value is **28800** seconds.

Perfect Forward Secrecy. If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys.

Phase 2 DH Group. If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group (the key for Phase 2 will match the key in Phase 1).

There are three groups of different prime key lengths. Group 1 is 768 bits, and Group 2 is 1,024 bits. Group 5 is 1,536 bits. If network speed is preferred, select **Group 1**. If network security is preferred, select **Group 5**. You do not have to use the same DH Group that you used for Phase 1.

Phase 2 Encryption. Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption, **DES** or **3DES**. The encryption method determines the length of the key used to encrypt or decrypt ESP packets. DES uses 56-bit encryption, and 3DES uses 168-bit encryption. 3DES is recommended because it is more secure. If you enable the AH Hash Algorithm on the *Advanced*

The screenshot shows the configuration interface for IKE with a Preshared Key. The settings are as follows:

- Keying Mode: IKE with Preshared key
- Phase1 DH Group: Group1
- Phase1 Encryption: DES
- Phase1 Authentication: MD5
- Phase1 SA Life Time: 28800 seconds
- Perfect Forward Secrecy:
- Phase2 DH Group: Group1
- Phase2 Encryption: DES
- Phase2 Authentication: MD5
- Phase2 SA Life Time: 3600 seconds
- Preshared Key: [Empty text field]

An "Advanced +" button is located at the bottom left of the configuration area.

Figure 6-68: IPSec Setup - IKE with Preshared Key

screen, then it is recommended to select **Null** to disable the encryption and decryption of ESP packets in Phase 2 (make sure the remote VPN device also has the AH Hash Algorithm enabled). Both ends of the VPN tunnel must use the same Phase 2 Encryption setting: DES, 3DES, or Null.

Phase 2 Authentication. Select a method of authentication, **MD5** or **SHA**. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. If you enable the AH Hash Algorithm on the *Advanced* screen, then it is recommended to select **Null** to disable the authentication of ESP packets in Phase 2 (make sure the remote VPN device also has the AH Hash Algorithm enabled). Both ends of the VPN tunnel must use the same Phase 2 Authentication setting: MD5, SHA, or Null.

Phase 2 SA Life Time. Configure the length of time a VPN tunnel is active in Phase 2. The default value is **3600** seconds.

Preshared Key. This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., My_@123 or 4d795f40313233. This field allows a maximum of 30 characters and/or hexadecimal values. Both ends of the VPN tunnel must use the same Preshared Key. It is strongly recommended that you change the Preshared Key periodically to maximize VPN security.

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

Manual

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

Incoming SPI (Security Parameter Index). SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to send the Security Association (SA), under which a packet should be processed. Hexadecimal values are acceptable, and the valid range of hexadecimal values is from 100 to ffffffff. Each tunnel must have a unique Inbound SPI and Outbound SPI. The Incoming SPI of the Router must match the Outgoing SPI set on the remote VPN device at the other end of the tunnel. For example, if the Incoming SPI is 20123, then the Outgoing SPI would be 32102.

Outgoing SPI (Security Parameter Index). SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to send the SA, under which a packet should be processed. Hexadecimal values are acceptable, and the valid range of hexadecimal values is from 100 to ffffffff. Each tunnel must have a unique Inbound SPI and Outbound SPI. The Outgoing SPI of the Router must match the Incoming SPI set on the remote VPN device at the other end of the tunnel. For example, if the Outgoing SPI is 32102, then the Incoming SPI would be 20123.

The screenshot shows the 'IPSec Setup - Manual' configuration interface. It contains the following elements:

- Keying Mode:** A dropdown menu set to 'Manual'.
- Incoming SPI:** An empty text input field.
- Outgoing SPI:** An empty text input field.
- Encryption:** A dropdown menu set to 'DES'.
- Authentication:** A dropdown menu set to 'MD5'.
- Encryption Key:** An empty text input field.
- Authentication Key:** An empty text input field.

Figure 6-69: IPSec Setup - Manual

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

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

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

Authentication Key. This field specifies a key used to authenticate IP traffic. Enter a key of hexadecimal values in the *Authentication Key* field. If you selected MD5 as the authentication method, then the Authentication Key must be 32-bit, which requires 32 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Authentication Key will be 32-bit. If you selected SHA1 as the authentication method, then the Authentication Key must be 40-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes, so the Authentication Key will be 40-bit. Make sure both ends of the VPN tunnel use the same Authentication Key.

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

Advanced

For most users, the settings on the VPN page should suffice; however, the Router provides advanced IPsec settings for advanced users. Click the **Advanced** button to view the Advanced settings, which are available only for VPN tunnels using the IKE with Preshared Key mode.

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, leave the *Aggressive Mode* checkbox unchecked. If network speed is preferred,

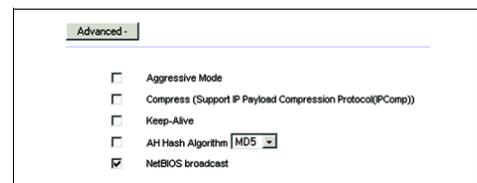


Figure 6-70: IKE with Preshared Key - Advanced

select **Aggressive Mode**. If you select one of the Dynamic IP types for the Remote Security Gateway Type setting, then Main Mode will be unavailable, so Aggressive Mode will be used.

Compress (Support IP Payload compression Protocol (IP Comp)). The Router supports IP Payload Compression Protocol, which is used to reduce the size of IP datagrams. If this feature is enabled, the Router will propose compression when initiating a connection. If the responders reject this proposal, then the Router will not implement compression. When the Router works as a responder, the Router will always accept compression even when the Compress feature has not been enabled. Select **Compress** to support this protocol.

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

AH Hash Algorithm. The AH (Authentication Header) protocol describes the packet format and default standards for packet structure. If AH is used as a security protocol, portions of the original IP header are used to verify the integrity of the entire packet during the hashing process, so protection is extended forward into the IP header. Select an algorithm, **MD5** or **SHA1**. MD5 produces a 128-bit digest to authenticate packet data, and SHA1 produces a 160-bit digest to authenticate packet data. Both ends of the VPN tunnel should use the same AH Hash Algorithm.

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

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

VPN Tab - Client to Gateway

Use this screen to create a new tunnel between a local VPN device and a mobile user.

Add a New Tunnel

You can select **Tunnel** to create a tunnel for a single mobile user, or select **Group VPN** to create tunnels for multiple VPN clients. The Group VPN feature facilitates the setup of tunnels for multiple VPN clients, so you do not need to individually configure multiple remote VPN clients. After you have selected Tunnel or Group VPN, the settings available on this screen may change, depending on which selection you have made.

Tunnel No. A tunnel number between 1-50 will be automatically generated.

Tunnel Name. Enter a name for this VPN tunnel, such as Home Office or New York Branch. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

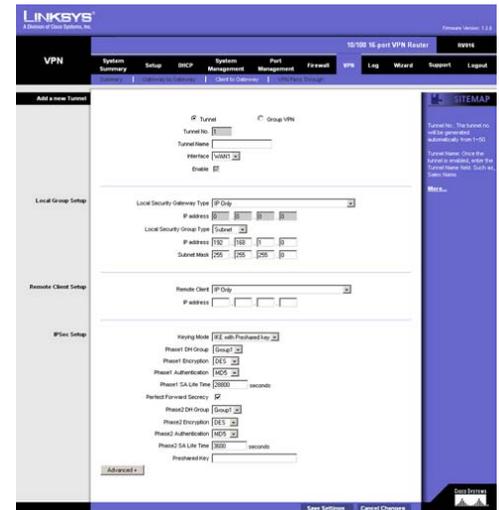


Figure 6-71: Client to Gateway

10/100 16-Port VPN Router

Interface. Select the appropriate Interface (WAN1, WAN2...) from the pull-down menu. If you designate more than two WAN ports on the Network or Port Management page, then additional WAN ports will be available.

Enable. Check this box to enable this VPN tunnel.

Group VPN

The Group VPN settings will appear only if you are adding a new Group VPN. Up to two Group VPNs are supported by the Router.

Group No. A group number will be automatically generated.

Group Name. Enter a name for this Group VPN, such as American Managers Group or West Coast Locations.

Interface. Select the appropriate Interface (WAN1, WAN2...) from the pull-down menu. If you designate more than two WAN ports on the Network or Port Management page, then additional WAN ports will be available.

Enable. Check the box to enable this Group VPN.

Local Group Setup

Local Security Gateway Type (not applicable to Group VPNs)

Select one of these five available types: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**.

(If you want to use a Fully Qualified Domain Name (FQDN) for authentication but you do not have one, visit www.dyndns.org to set up a Dynamic Domain Name System (DDNS) account. Then enable and configure the 10/100 16-Port VPN Router's DDNS settings on the *DDNS* screen.)

The Local Security Gateway Type you select should match the Remote Security Gateway Type selected on the remote VPN client(s) at the other end of the tunnel(s).

After you have selected the Local Security Gateway Type, the settings available on this screen may change, depending on which selection you have made.

IP Only. If you select IP Only, then only the computer with a specific IP address will be able to access the tunnel. The WAN (or Internet) IP address of the Router will automatically appear in the *IP address* field.

The screenshot shows a configuration window for the Local Security Gateway Type. A dropdown menu is set to 'IP Only'. Below it, the 'IP address' field is populated with the IP address 192.168.5.86, displayed in four separate input boxes.

Figure 6-72: Local Security Gateway Type - IP Only

The screenshot shows the same configuration window, but the dropdown menu is now set to 'IP + Domain Name(FQDN) Authentication'. A 'Domain Name' input field has appeared above the 'IP address' field. The 'IP address' field still shows 192.168.5.86.

Figure 6-73: Local Security Gateway Type - IP + Domain Name (FQDN) Authentication

IP + Domain Name(FQDN) Authentication. If you select this type, enter the FQDN (Fully Qualified Domain Name) in the *Domain Name* field, and an IP address will automatically appear in the *IP address* field. The FQDN is the host name and domain name for a specific computer on the Internet. An example of a FQDN is `vpn.myvpnsrv.com`. The FQDN and IP address must match the FQDN and IP address of the Remote Client at the other end of the tunnel. The FQDN and IP can be used for only one tunnel connection.

IP + E-mail Addr.(USER FQDN) Authentication. If you select this type, enter the appropriate e-mail address in the *E-mail address* fields, and an IP address will automatically appear in the *IP address* field.

Dynamic IP + Domain Name(FQDN) Authentication. If the Local Security Gateway has a dynamic IP and you want to use the Domain Name for authentication, then select this type. When the Remote Client asks to create a tunnel with the Router, the Router will work as a responder. For authentication, complete the *Domain Name* field, and make sure it matches the Domain Name set on the Remote Client. The Domain Name can be used for only one tunnel connection, so you can't use the same Domain Name to create another new tunnel connection.

Dynamic IP + E-mail Addr.(USER FQDN) Authentication. If the Local Security Gateway has a dynamic IP and you want to use the e-mail address for authentication, then select this type. When the Remote Client asks to create a tunnel with the Router, the Router will work as a responder. For authentication, enter the appropriate e-mail address in the *E-mail address* fields.

Local Security Group Type

Select the local LAN user(s) behind the Router that can use this VPN tunnel. Select one of these three available types: **IP**, **Subnet**, or **IP Range**. The Local Security Group Type you select should match the Remote Security Group Type selected on the remote VPN client(s) at the other end of the tunnel(s).

After you have selected the Local Security Group Type, the settings available on this screen may change, depending on which selection you have made.

IP. If you select IP Only, then only the computer with a specific IP address will be able to access the tunnel. Enter the appropriate IP address. The default IP is **192.168.1.0**.

Subnet. If you select Subnet, which is the default, then all computers on the local subnet will be able to access the tunnel. Complete the *IP address* and *Subnet Mask* fields. The default IP is **192.168.1.0**, and the default Subnet Mask is **255.255.255.0**.

IP Range. If you select IP Range, then you can specify a range of IP addresses within the subnet that will be able to access the tunnel. Complete the *IP range* fields. The default IP Range is **192.168.1.0~254**.

Figure 6-74: Local Security Gateway Type - IP + E-mail Addr. (USER FQDN) Authentication

Figure 6-75: Local Security Gateway Type - Dynamic IP + Domain Name (FQDN) Authentication

Figure 6-76: Local Security Gateway Type - Dynamic IP + E-mail Addr. (USER FQDN) Authentication

Figure 6-77: Local Security Group Type - IP

Figure 6-78: Local Security Group Type - Subnet

Figure 6-79: Local Security Group Type - IP Range

Remote Client Setup for a VPN Tunnel

You will have different Remote Client Setup settings depending on whether you are adding a new tunnel or a new Group VPN. If you are adding a new Group VPN, proceed to the "Remote Client Setup for a Group VPN" section.

Remote Client

Select one of these five available types: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**.

(If you want the remote client to use a Fully Qualified Domain Name (FQDN) for authentication but the remote client does not have one, visit www.dyndns.org to set up a Dynamic Domain Name System (DDNS) account.)

After you have selected the Remote Client, the settings available on this screen may change, depending on which selection you have made.

IP Only. If you know the fixed IP address of the Remote Client, select IP Only. Only the computer with this specific IP address will be able to access the tunnel. In the *IP address* field, enter the IP address of the Remote Client at the other end of the tunnel. (The Remote Client can be a computer with VPN client software that support IPsec.)

IP + Domain Name(FQDN) Authentication. If you select this type, enter the FQDN (Fully Qualified Domain Name) and IP address of the Remote Client, which can be a computer with VPN client software that supports IPsec. (Enter the FQDN in the *Domain Name* field, and enter the IP address in the *IP address* field.) The FQDN is the host name and domain name for a specific computer on the Internet. An example of a FQDN is `vpn.remotevpnserver.com`. The FQDN and IP address must match the FQDN and IP address of the Local Security Gateway type selected on the Remote Client. The FQDN and IP can be used for only one tunnel connection.

IP + E-mail Addr.(User FQDN) Authentication. If you select this type, enter the e-mail address and IP address of the Remote Client at the other end of the tunnel. (The Remote Client can be a computer with VPN client software that support IPsec.)

Dynamic IP + Domain Name(FQDN) Authentication. If the Remote Security Gateway has a dynamic IP and you want to use the Domain Name for authentication, then select this type. When the Remote Security Gateway asks to create a tunnel with the Router, the Router will work as a responder. For authentication, complete the *Domain Name* field, and make sure it matches the Domain Name set on the Local Gateway of the Remote Client. The Domain Name can be used for only one tunnel connection, so you can't use the same Domain Name to create another new tunnel connection.

The screenshot shows the 'Remote Client' dropdown menu set to 'IP Only'. Below it, the 'IP address' field is a four-part dotted box for entering an IP address.

Figure 6-80: Remote Client for VPN Tunnel - IP Only

The screenshot shows the 'Remote Client' dropdown menu set to 'IP + Domain Name(FQDN) Authentication'. Below it, there are two fields: 'Domain Name' and 'IP address' (a four-part dotted box).

Figure 6-81: Remote Client for VPN Tunnel - IP + Domain Name (FQDN) Authentication

The screenshot shows the 'Remote Client' dropdown menu set to 'IP + E-mail Addr. (User FQDN) Authentication'. Below it, there are two fields: 'E-mail address' (with an '@' icon) and 'IP address' (a four-part dotted box).

Figure 6-82: Remote Client for VPN Tunnel - IP + E-mail Addr. (User FQDN) Authentication

The screenshot shows the 'Remote Client' dropdown menu set to 'Dynamic IP + Domain Name(FQDN) Authentication'. Below it, there is a 'Domain Name' field.

Figure 6-83: Remote Client for VPN Tunnel - Dynamic IP + Domain Name (FQDN) Authentication

Dynamic IP + E-mail Addr.(User FQDN) Authentication. If the Remote Security Gateway has a dynamic IP and you want to use the e-mail address for authentication, then select this type. When the Remote Security Gateway asks to create a tunnel with the Router, the Router will work as a responder. For authentication, enter the appropriate e-mail address in the *E-mail address* fields.

Remote Client Setup for a Group VPN

Remote Client. There are three types of Remote Client: Domain Name (FQDN), E-mail Address (User FQDN), and Microsoft XP/2000 VPN Client.

Remote Client

Select one of these three types: **Domain Name(FQDN)**, **E-mail Address(USER FQDN)**, or **Microsoft XP/2000 VPN Client**.

(If you want to use an FQDN (Fully Qualified Domain Name) but you have not set it up, visit www.dyndns.org to set up a Dynamic Domain Name System (DDNS) account.)

After you have selected the Remote Client, the settings available on this screen may change, depending on which selection you have made.

Domain Name(FQDN). If you select this type, enter the FQDN (Fully Qualified Domain Name) of the Remote Client in the *Domain Name* field. The FQDN is the host name and domain name for a specific computer on the Internet. An example of a FQDN is `vpn.remotevpnserver.com`. The FQDN must match the FQDN setting on the Remote Client. When the Remote Client asks to create a tunnel with the Router, the Router will work as a responder.

E-mail Address(USER FQDN). If you select this type, enter the e-mail address of the Remote Client at the other end of the tunnel.

Microsoft XP/2000 VPN Client. If the Remote Client has a dynamic IP address and is a Microsoft VPN client, select this type. The difference between Microsoft and other VPN clients is that the Microsoft VPN client does not support Aggressive Mode and the two Remote Client options, Domain Name(FQDN) and E-mail Address(USER FQDN).

IPSec Setup

In order for any encryption to occur, the two ends of a VPN tunnel must agree on the methods of encryption, decryption, and authentication. This is done by sharing a key to the encryption code. For key management, there are two modes available; select **Manual** or **IKE with Preshared Key**. Both ends of a VPN tunnel must use the same mode of key management.



Figure 6-84: Remote Client for VPN Tunnel - Dynamic IP + E-mail Addr. (User FQDN) Authentication

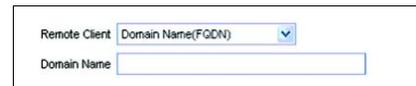


Figure 6-85: Remote Client for Group VPN - Domain Name (FQDN)



Figure 6-86: Remote Client for Group VPN - E-mail Address (USER FQDN)

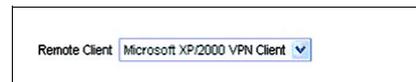


Figure 6-87: Remote Client for Group VPN - Microsoft XP/2000 VPN Client

After you have selected the Keying Mode, the settings available on this screen may change, depending on which selection you have made.

IKE with Preshared Key

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

Phase 1 DH Group. Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol 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, and Group 2 is 1,024 bits. 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. Select a method of encryption, **DES** or **3DES**. The encryption method determines the length of the key used to encrypt or decrypt ESP packets. DES uses 56-bit encryption, and 3DES uses 168-bit encryption. 3DES is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

Phase 1 Authentication. Select a method of authentication, **MD5** or **SHA**. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

Phase 1 SA Life Time. Configure the length of time a VPN tunnel is active in Phase 1. The default value is **28800** seconds.

Perfect Forward Secrecy. If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys.

Phase 2 DH Group. If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group (the key for Phase 2 will match the key in Phase 1). There are three groups of different prime key lengths. Group 1 is 768 bits, and Group 2 is 1,024 bits. Group 5 is 1,536 bits. If network speed is preferred, select **Group 1**. If network security is preferred, select **Group 5**. You do not have to use the same DH Group that you used for Phase 1.

Phase 2 Encryption. Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption, **DES** or **3DES**. The encryption method determines the length of the key used to encrypt or decrypt ESP packets. DES uses 56-bit encryption, and 3DES uses 168-bit encryption. 3DES is recommended because it is more secure. If you enable the AH Hash Algorithm on the *Advanced* screen, then it is recommended to select **Null** to disable the encryption and decryption of ESP packets in

The screenshot shows the configuration interface for IKE with a Preshared Key. The settings are as follows:

- Keying Mode: IKE with Preshared key
- Phase1 DH Group: Group1
- Phase1 Encryption: DES
- Phase1 Authentication: MD5
- Phase1 SA Life Time: 28800 seconds
- Perfect Forward Secrecy:
- Phase2 DH Group: Group1
- Phase2 Encryption: DES
- Phase2 Authentication: MD5
- Phase2 SA Life Time: 3600 seconds
- Preshared Key: [Empty text field]

An "Advanced +" button is located at the bottom left of the configuration area.

Figure 6-88: IPSec Setup - IKE with Preshared Key

Phase 2 (make sure the remote VPN device also has the AH Hash Algorithm enabled). Both ends of the VPN tunnel must use the same Phase 2 Encryption setting: DES, 3DES, or Null.

Phase 2 Authentication. Select a method of authentication, **MD5** or **SHA**. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. If you enable the AH Hash Algorithm on the *Advanced* screen, then it is recommended to select **Null** to disable the authentication of ESP packets in Phase 2 (make sure the remote VPN device also has the AH Hash Algorithm enabled). Both ends of the VPN tunnel must use the same Phase 2 Authentication setting: MD5, SHA, or Null.

Phase 2 SA Life Time. Configure the length of time a VPN tunnel is active in Phase 2. The default value is **3600** seconds.

Preshared Key. This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., My_@123 or 4d795f40313233. This field allows a maximum of 30 characters and/or hexadecimal values. Both ends of the VPN tunnel must use the same Preshared Key. It is strongly recommended that you change the Preshared Key periodically to maximize VPN security.

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

Manual (not applicable to Group VPNs)

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

Incoming SPI (Security Parameter Index). SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to send the Security Association (SA), under which a packet should be processed. Hexadecimal values are acceptable, and the valid range of hexadecimal values is from 100 to ffffffff. Each tunnel must have a unique Inbound SPI and Outbound SPI. The Incoming SPI of the Router must match the Outgoing SPI set on the remote VPN device at the other end of the tunnel. For example, if the Incoming SPI is 20123, then the Outgoing SPI would be 32102.

Outgoing SPI (Security Parameter Index). SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to send the SA, under which a packet should be processed. Hexadecimal values are acceptable, and the valid range of hexadecimal values is from 100 to ffffffff. Each tunnel must have a unique Inbound SPI and Outbound SPI. The Outgoing SPI of the Router must match the Incoming SPI set on the remote VPN device at the other end of the tunnel. For example, if the Outgoing SPI is 32102, then the Incoming SPI would be 20123.

The screenshot shows a configuration window for IPsec Setup - Manual. It contains the following fields:

- Keying Mode: Manual (dropdown menu)
- Incoming SPI: [Empty text box]
- Outgoing SPI: [Empty text box]
- Encryption: DES (dropdown menu)
- Authentication: MD5 (dropdown menu)
- Encryption Key: [Empty text box]
- Authentication Key: [Empty text box]

Figure 6-89: IPsec Setup - Manual

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

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

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

Authentication Key. This field specifies a key used to authenticate IP traffic. Enter a key of hexadecimal values in the *Authentication Key* field. If you selected MD5 as the authentication method, then the Authentication Key must be 32-bit, which requires 32 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Authentication Key will be 32-bit. If you selected SHA1 as the authentication method, then the Authentication Key must be 40-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes, so the Authentication Key will be 40-bit. Make sure both ends of the VPN tunnel use the same Authentication Key.

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

Advanced

For most users, the settings on the VPN page should suffice; however, the Router provides advanced IPsec settings for advanced users. Click the **Advanced** button to view the Advanced settings, which are available only for VPN tunnels using the IKE with Preshared Key mode.

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, leave the *Aggressive Mode* checkbox unchecked. If network speed is preferred, select **Aggressive Mode**. If you select one of the Dynamic IP types for the Remote Security Gateway Type

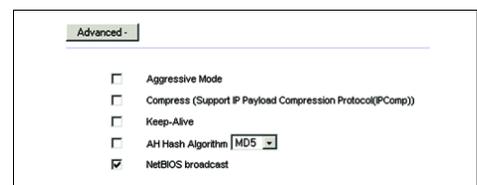


Figure 6-90: IKE with Preshared Key - Advanced

10/100 16-Port VPN Router

setting, then Main mode will be unavailable, so Aggressive Mode will be used—unless the Remote Client is Microsoft XP/2000 VPN client. For Microsoft XP/2000 VPN clients, then Aggressive Mode will be unavailable, so Main mode will be used.

Compress (Support IP Payload compression Protocol (IP Comp)). The Router supports IP Payload Compression Protocol, which is used to reduce the size of IP datagrams. If this feature is enabled, the Router will propose compression when initiating a connection. If the responders reject this proposal, then the Router will not implement compression. When the Router works as a responder, the Router will always accept compression even when the Compress feature has not been enabled. Select **Compress** to support this protocol.

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

AH Hash Algorithm. The AH (Authentication Header) protocol describes the packet format and default standards for packet structure. If AH is used as a security protocol, portions of the original IP header are used to verify the integrity of the entire packet during the hashing process, so protection is extended forward into the IP header. Select an algorithm, **MD5** or **SHA1**. MD5 produces a 128-bit digest to authenticate packet data, and SHA1 produces a 160-bit digest to authenticate packet data. Both ends of the VPN tunnel should use the same AH Hash Algorithm.

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

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

VPN Tab - VPN Pass Through

The *VPN Passthrough* screen allows you to enable or disable passthrough for a variety of VPN methods.

IPSec Pass Through

Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass Through is enabled by default to allow IPSec tunnels to pass through the Router.

PPTP Pass Through

Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass Through is enabled by default.

L2TP Pass Through

Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass Through is enabled by default.

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



Figure 6-91: VPN Pass Through

Log Tab - System Log

On this screen you will be able to configure the Router's log settings, so you can specify how you want its activity logs handled.

Syslog

Syslog is a standard protocol used to capture information about network activity. The Router supports this protocol and can send its activity logs to an external server.

Enable Syslog. If you check the box, the Router's Syslog feature will be enabled.

Syslog Server. In addition to the standard event log, the Router can send a detailed log to an external Syslog server. The Router's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP service, and number of bytes transferred. Enter the Syslog server name or IP address in the *Syslog Server* field. Click the **Save Settings** button to save your changes, and then restart the Router for the changes to take effect.

E-mail

You may want logs or alert messages to be e-mailed to you. If so, then configure the E-mail settings.

Enable E-Mail Alert. If you check the box, The Router's E-Mail Alert feature will be enabled.

Mail Server. If you want any log or alert information e-mailed to you, then enter the name or numerical IP address of your SMTP server. Your ISP can provide you with this information.

Send E-mail to. This is the e-mail address to which your log files will be sent. If you do not want copies of the log information e-mailed to you, then leave this field blank.

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

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

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

E-mail Log Now. Click the **E-mail Log Now** button to immediately send the log to the address in the *Send E-mail to* field.

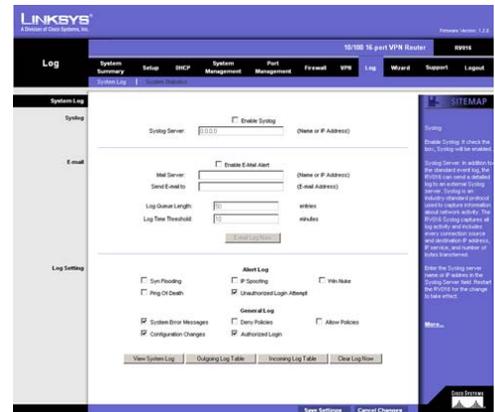


Figure 6-92: System Log

Log Setting

Alert Log

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

General Log

You can receive logs that track specific types of events: System Error Messages, Deny Policies, Allow Policies, Configuration Changes, and Authorized Login. To include an event in the log, click its checkbox.

View System Log. Click this button to display a log of all activities and to access a drop-down menu of the various logs available.

From the drop-down menu, select the log you wish to view: **ALL**, **System Log**, **Access Log**, **Firewall Log**, or **VPN Log**. When you select All, you will see a log of all activities. The System Log displays a list of cold and warm starts, web login successes and failures, and packet filtering policies, while the Access Log shows all activities involving local network or Internet access. The Firewall Log displays all activities regarding the Router's firewall, while the VPN Log shows information about VPN tunnel activity.

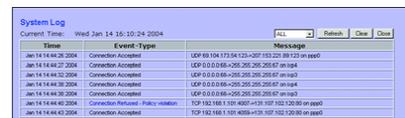
To clear a log, click the **Clear** button. To update a log, click the **Refresh** button. To exit this screen, click the **Close** button.

Outgoing Log Table. Click the **Outgoing Log Table** button to view a temporary log of all the URLs and IP addresses of Internet sites that users on your network have accessed. Each event is described, and the LAN IP address, Destination URL/IP, and Service/Port Number for each site are listed. Click the **Refresh** button to update the log. To exit this screen, click the **Close** button.

Incoming Log Table. Click the **Incoming Log Table** button to view a temporary log describing all the incoming Internet traffic. Each event is described, and the Source IP and Destination Port number for each event are listed. Click the **Refresh** button to update the log. To exit this screen, click the **Close** button.

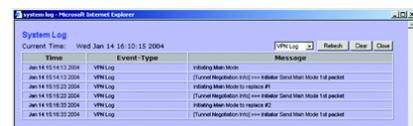
Clear Log Now. Click this button to clear your log without e-mailing it. Only use this button if you are willing to lose your log information.

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



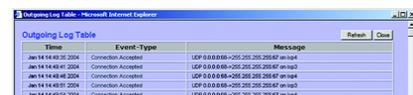
Time	Event-Type	Message
Jan 14 14:46:26 2004	Connection Accepted	UDP 69.104.173.54:125->207.170.220.86:123 on ppp0
Jan 14 14:46:27 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:28 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:29 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:30 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:40 2004	Connection Refused - Policy violation	TCP 192.168.1.101:4051->192.168.1.101:123 on ppp0
Jan 14 14:46:42 2004	Connection Accepted	TCP 192.168.1.101:4051->192.168.1.101:123 on ppp0

Figure 6-93: View All Logs



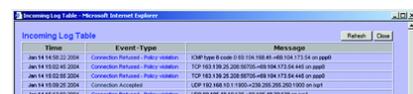
Time	Event-Type	Message
Jan 14 15:14:13 2004	VPN Log	Incoming Main Menu
Jan 14 15:14:13 2004	VPN Log	[Tunnel Negotiation Init] ->>> Main Menu Mode 1st packet
Jan 14 15:15:23 2004	VPN Log	Incoming Main Menu to remote #1
Jan 14 15:15:23 2004	VPN Log	[Tunnel Negotiation Init] ->>> Main Menu Mode 1st packet
Jan 14 15:15:30 2004	VPN Log	Incoming Main Menu to remote #2
Jan 14 15:15:30 2004	VPN Log	[Tunnel Negotiation Init] ->>> Main Menu Mode 1st packet

Figure 6-94: View VPN Log



Time	Event-Type	Message
Jan 14 14:46:26 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:27 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:28 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:29 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 14:46:30 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0

Figure 6-95: View Outgoing Log Table



Time	Event-Type	Message
Jan 14 14:46:26 2004	Connection Accepted	UDP 0.0.0.0:688->205.205.205.205:20587 on ppp0
Jan 14 15:02:22 2004	Connection Refused - Policy violation	ICMP Type 8 code 0: 69.104.173.54->192.168.1.101:123 on ppp0
Jan 14 15:02:23 2004	Connection Refused - Policy violation	TCP 192.168.1.101:1000->205.205.205.205:80 on ppp0
Jan 14 15:02:24 2004	Connection Refused - Policy violation	TCP 192.168.1.101:1000->205.205.205.205:80 on ppp0
Jan 14 15:02:25 2004	Connection Refused - Policy violation	UDP 69.104.173.54:125->192.168.1.101:123 on ppp0

Figure 6-96: View Incoming Log Table

Log Tab - System Statistics

This screen displays statistics about all of the Router's ports (LAN, DMZ, and all WAN ports). For each port, the following statistics are listed: Device Name, Status, IP Address, MAC Address, Subnet Mask, Default Gateway, number of Received Packets, number of Sent Packets, number of Total Packets, number of Received Bytes, number of Sent Bytes, number of Total Bytes, number of Error Packets Received, and number of Dropped Packets Received.

When there are more than two WAN ports, click **Next page** to see additional system statistics on the next page. Then click **Previous page** to see the system statistics on the previous page.

Click the **Refresh** button to update the statistics.

	LAN	DMZ	WAN1	WAN2
Device Name	100	100	100	100
Status	Up	Up	Up	Up
IP Address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
MAC Address	10:1F:0A:00:00:04	28:0E:00:00:00:00	36:06:00:00:00:04	0.0.0.0
Subnet mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Received Packets	0	0	0	0
Sent Packets	0	0	0	0
Total Packets	0	0	0	0
Received Bytes	0	0	0	0
Sent Bytes	0	0	0	0
Total Bytes	0	0	0	0
Error Packets Received	0	0	0	0
Dropped Packets Received	0	0	0	0

Figure 6-97: System Statistics

Wizard Tab

Use this tab to access two Setup Wizards, the Basic Setup Wizard and the Access Rule Setup Wizard. Run the Basic Setup Wizard to set up the Router for your Internet connection(s). Run the Access Rule Setup Wizard to set up the security policy for the Router.

Basic Setup

If you want to change the number of WAN ports, go to the Change Number of WAN Ports section. If you want to modify the Router's network settings, go to the Modify the Router's Network Settings section.

Change Number of WAN Ports

1. Click the **Launch Now** button to run the Basic Setup Wizard.
2. The screen shown in Figure 6-99 will appear. If you want to change the number of WAN ports, select **Set the total number of WAN ports**. Click the **Next** button to continue. Click the **Exit** button if you want to exit the Setup Wizard.
3. Select the number of WAN ports you want to use, up to a maximum of 7. Click the **Next** button to continue. Click the **Exit** button if you want to exit the Setup Wizard.



Figure 6-98: Wizard



Figure 6-99: Basic Setup Wizard - Change Number of WAN Ports



Figure 6-100: Change Number of WAN Ports

4. The screen shown in Figure 6-101 will appear. If you want to save your changes, click the Save Settings button. Click the Previous button if you want to return to the previous screen. Click the Exit button if you want to exit the Setup Wizard (your changes will not be saved).

Modify the Router's Network Settings

1. Click the **Launch Now** button to run the Basic Setup Wizard.
2. The screen shown in Figure 6-102 will appear. If you want to edit the Router's network settings, select **Edit Network Settings**. Click the **Next** button to continue. Click the **Exit** button if you want to exit the Setup Wizard.
3. Your Internet Service Provider (ISP) may require you to use a host and domain name for your Internet connection. If your ISP requires them, complete the *Host Name* and *Domain Name* fields; otherwise leave these blank. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.



Figure 6-101: Save Settings



Figure 6-102: Basic Setup Wizard - Edit Network Settings



Figure 6-103: Host and Domain Name

- On the screen shown in Figure 6-104, select the WAN (or Internet) Connection Type for the Interface listed (generally, the Setup Wizard will begin with WAN1). Select the appropriate connection type: **Obtain an IP automatically**, **Static IP**, or **PPPoE**. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.
- Depending on which connection type you have selected, the appropriate screen will appear. Follow the instructions for the appropriate connection type:

Obtain an IP automatically

If you chose Obtain an IP automatically, the screen shown in Figure 6-105 will appear. If you want to use the ISP's DNS server, select **Use DNS Server provided by ISP (default)**. If you want to designate a specific DNS server IP address, select **Use the Following DNS Server Addresses**, and enter the DNS server IP addresses you want to use (you must enter at least one).

Click the **Next** button to continue, and proceed to step 6. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.



Figure 6-104: WAN Connection Type

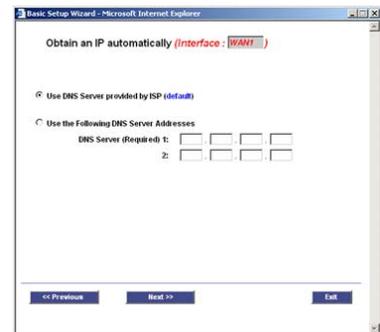


Figure 6-105: Obtain an IP Automatically

Static IP

If you chose Static IP, the screen shown in Figure 6-106 will appear. Complete the *Static IP*, *Subnet Mask*, and *Default Gateway* fields with the settings provided by your ISP. Click the **Next** button, and then the screen shown in Figure 6-107 will appear.

Enter the DNS server IP addresses you want to use (you must enter at least one). Click the **Next** button to continue, and proceed to step 6. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.



Figure 6-106: Static IP

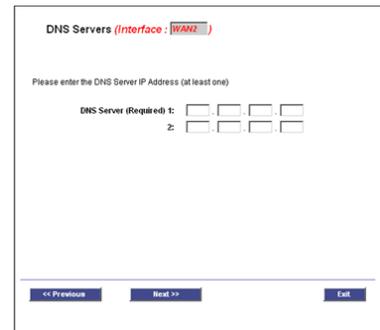


Figure 6-107: Static IP - DNS Servers

PPPoE

If you chose PPPoE, the screen shown in Figure 6-108 will appear. Complete the *User Name* and *Password* fields with the information provided by your ISP. Click the **Next** button, and then the screen shown in Figure 6-109 will appear.

Select **Connect on demand** or **Keep alive**. If you select the *Connect on demand* option, the PPPoE connection will be disconnected after a specified period of inactivity (*Max. Idle Time*). In the *Max. Idle Time* field, enter the number of minutes you want the Router to wait before your Internet access disconnects.

If you select the *Keep Alive* option, the Router will keep the connection alive by sending out a few data packets periodically, so your ISP thinks that the connection is still active. This option keeps your PPPoE-enabled connection active indefinitely, even when it sits idle. In the *Redial period* field, enter the number of seconds you want the Router to wait between data transmissions.

Click the **Next** button to continue, and proceed to step 6. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.

Figure 6-108: PPPoE

Figure 6-109: PPPoE - Connect on Demand or Keep Alive

6. Repeat step 5 for the rest of the Router's WAN ports. When it is time to configure the DMZ port, proceed to step 7.
7. On the screen shown in Figure 6-110, enter the DMZ IP address provided by the ISP in the *DMZ IP* fields. Then complete the *Subnet Mask* field. If you are not using the DMZ port, enter **0** in each of the *DMZ IP* fields. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.
8. The screen shown in Figure 6-111 will appear. If you want to save your changes, click the **Save Settings** button. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Setup Wizard.

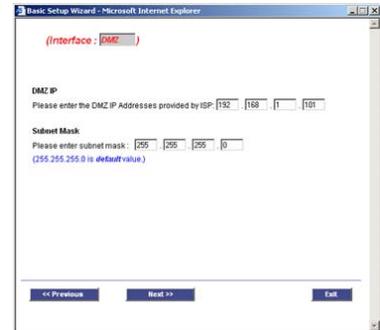


Figure 6-110: DMZ



Figure 6-111: Save Settings

Access Rule Setup

1. Click the **Launch Now** button to run the Access Rule Wizard.
2. The screen shown in Figure 6-112 will appear. This screen explains the Access Rules, including the Router's Default Rules. Click the **Next** button to continue. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.
3. The screen shown in Figure 6-113 will appear. From the drop-down menu, select **Allow** or **Deny** depending on the intent of the Access Rule. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.



Figure 6-112: Access Rules



Figure 6-113: Action

4. The screen shown in Figure 6-114 will appear. Select the service you want from the *Service* pull-down menu. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.
5. The screen shown in Figure 6-115 will appear. For this service, you can select whether or not you want the Router to keep a log tracking this type of activity. To keep a log, select **Log packets matching this access rule**. If you don't want a log, select **Do not log packets matching this access rule**. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.
6. The screen shown in Figure 6-116 will appear. Select the appropriate Source Interface (LAN, DMZ, Any, WAN1, WAN2...) from the *Ethernet* pull-down menu.

Select the Source IP address(es) for this Access Rule. If it can be any IP address, select **Any**. If it is one IP address, select **Single** and enter the IP address in the *Source IP* fields. If it is a range of IP addresses, select **Range**, and enter the IP addresses in the *Source IP* fields. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.



Figure 6-114: Service

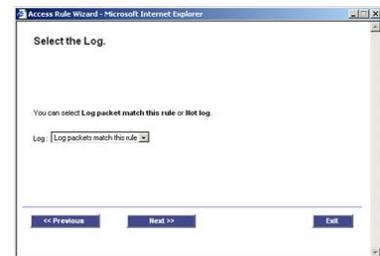


Figure 6-115: Log



Figure 6-116: Source

7. The screen shown in Figure 6-117 will appear. Select the Destination IP address(es) for this Access Rule. If it can be any IP address, select **Any**. If it is one IP address, select **Single** and enter the IP address in the *Destination IP* fields. If it is a range of IP addresses, select **Range**, and enter the IP addresses in the *Destination IP* fields. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.
8. The screen shown in Figure 6-118 will appear. Decide when you want this Access Rule to be enforced. Select **Always** if you want the Access Rule to be always enforced. Select **Scheduling** if you want to specify when the Access Rule should be in effect. Decide what times and which days of the week the Access Rule should be enforced. Then enter the hours and minutes in 24-hour format, and select the appropriate days of the week. Click the **Next** button to continue. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard.
9. The screen shown in Figure 6-119 will appear. If you want to save your changes, click the **Save Settings** button. Click the **Previous** button if you want to return to the previous screen. Click the **Exit** button if you want to exit the Access Rule Setup Wizard without saving the settings.
10. A screen will appear indicating that the settings have been saved. If you want to add another Access Rule, click the **OK** button, and the first screen of the Access Rule Setup Wizard will appear. If you want to exit the Access Rule Setup Wizard, click the **Cancel** button, and the *Access Rules* screen will appear.

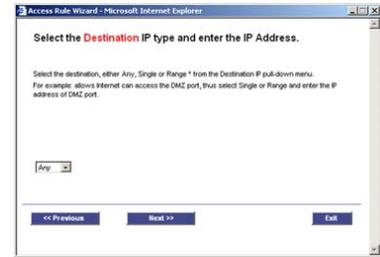


Figure 6-117: Destination

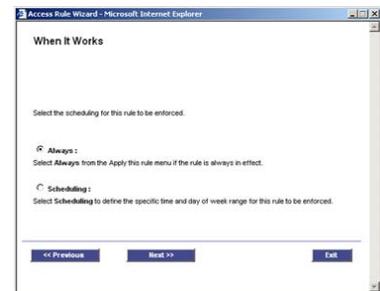


Figure 6-118: Scheduling



Figure 6-119: Save Settings

Support Tab

From this tab, you will be able to access the Support page of the Linksys website, which offers a variety of resources. You must have an active Internet connection before you can visit the Linksys website.

Manual

If you want the latest version of this User Guide, click the **On Line Manual** button. The Support page of the Linksys website will appear. Click the **Downloads** button from the Technical Support menu, and then select the RV016 - 10/100 16-Port VPN Router from the drop-down menu. Select your operating system, and then click **Downloads for this Product**. Click **User Guide**.

Linksys Web Site

Click the **Linksys Web Site** button, and the Support page of the Linksys Website, www.linksys.com, will appear.

Logout Tab

The Logout tab is located on the upper right-hand corner of the screen. Click this tab to end the management session. After you click the Logout tab, a screen will appear and ask you to confirm that you want to end the session. If you end the session, you will need to re-enter your User Name and Password to log in and then manage the Router.

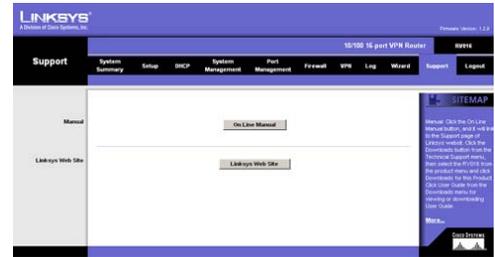


Figure 6-120: Support



Figure 6-121: Logout

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'm having trouble getting my VPN tunnel to connect. What should I do?*

Perform the following steps until the VPN tunnel connects:

- A. Double-check all of the settings. Make sure the IPsec Setup settings of the 10/100 16-Port VPN Router match the IPsec Setup settings of the remote VPN router or client, including the Preshared Key and Phase1 and Phase2 SA Life Time settings, which are used in the IKE with Preshared Key mode.
- B. Click the **Log** tab of the Router's Web-based Utility. Click the **View System Log** button. From the drop-down menu, select the **VPN Log**. The error message will indicate which setting is incorrect and needs to be changed on either the 10/100 16-Port VPN Router or the remote VPN router or client.
- C. Make sure the IP address of the Remote Secure Gateway or Client is correct. Click the **System Management** tab of the Router's Web-based Utility. Select the **Ping** radio button. Enter the IP address of the Remote Secure Gateway or Client in the *Ping host or IP address* field. Then click the **Go** button.

2. *My VPN tunnel connects properly, but it frequently drops the connection. What should I do?*

Through the Router's Web-based Utility, access the settings for your VPN tunnel. In the IPsec Setup section with IKE with Preshared Key mode selected, increase the Phase2 SA Life Time setting to **28800** seconds, which is eight hours. Then increase the Phase2 SA Life Time setting to **28800** seconds on the remote VPN router or client. If you need to check the status of your VPN tunnel, view the *VPN Summary* screen of the Router's Web-based Utility.

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

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

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

4. 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).

10/100 16-Port VPN Router

- 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.
5. ***I want to test my Internet connection.***
- A. Check your TCP/IP settings.

For Windows 98 and Millennium:

Refer to Windows Help and "Chapter 5: Configuring the PCs" 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.
- 6. 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 6: Setting up and Configuring the Router" for details.
- C. Make sure you are using the right Internet settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: Setting up and Configuring the Router" for details on Internet Connection Type settings.
- D. Make sure you use the right cable. Check to see if the Internet LED is solidly lit.
- E. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's Web-based Utility shows a valid IP address from your ISP.
- F. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's Web-based Utility to see if you get an IP address.
- 7. 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)."

8. I am using VPN client software on my computer, and I can't get my Virtual Private Network (VPN) tunnel to pass 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, PPTP, and/or L2TP passthrough enabled.

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

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

Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab of the Web-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 2 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.

9. 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.

- 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.

10.1 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:

- 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.
- 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.
- 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
Halfife	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.

11. 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:

- 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.
- 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.
- Click the **DMZ Host** tab.
- 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.

12. 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:

10/100 16-Port VPN Router

- A. Access the Router's web interface by going to <http://192.168.1.1> or the IP address of the Router. Enter **admin** (the default) in the *User Name* and *Password* fields, 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.

13. 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.

14. 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.

15. I need to upgrade the firmware.

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

- A. Go to the Linksys website at <http://www.linksys.com> and download the latest firmware, or use the Web-based Utility to be automatically redirected to the download webpage. Go to System Management - Firmware Upgrade, and click the **Firmware Download from Linksys Web Site** button. Select the Router from the pull-down menu and choose the firmware from the options.
- B. Extract the firmware file on your computer.

- C. To upgrade the firmware, follow the steps in the Upgrade section found in "Chapter 6: Setting up and Configuring the Router" or "Appendix B: Upgrading Firmware."

16. The firmware upgrade failed.

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

- A. 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

- B. 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.

17. 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 user name and password, if asked. (The default user name and password are admin.)
- C. On the *Setup - Network* tab, select **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.

18. 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 user name and password, if asked. (The default user name and password are **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

19. 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 user name and password, if asked. (The default user name and password are **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.

20. 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.

10/100 16-Port VPN Router

- 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). 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.

10/100 16-Port VPN Router

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



Figure B-1: Upgrade Firmware

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

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

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



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

Windows 2000 or XP Instructions

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

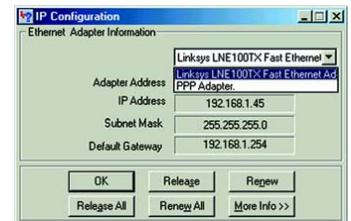


Figure C-1: IP Configuration Screen

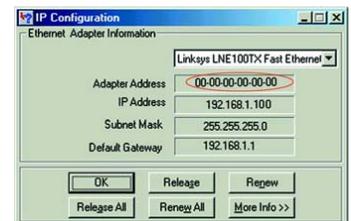


Figure C-2: MAC Address/Adapter Address

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

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



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

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

For the Router's Web-based Utility

The MAC Clone table displays the number of WAN ports you have configured on the *Network* or *Port Management* screen. Their MAC addresses are shown in the MAC Address column. Click the **Edit** in the Config. column to edit the MAC Clone setting of the selected WAN port. A new screen will appear.

In the *Interface* field, the WAN port number is displayed. To manually clone a MAC address, select **User Defined WAN MAC Address**, and then enter the 12 digits of your adapter's MAC address. If you want to clone the MAC address of the PC you are currently using to configure the Router, then select **MAC Address from this PC**.

Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to undo your changes. Click the **Back** button to return to the previous page if you want to configure the other WAN ports.

```

C:\>ipconfig /all

Windows 2000 IP Configuration

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  : 
   Description . . . . . : Linksys LNE100TX(G5) Fast Ethernet N
   adapter
   Physical Address. . . . . : 00-00-00-00-00-00
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address . . . . . : 192.168.1.100
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
   DHCP Server . . . . . : 192.168.1.1
   DNS Servers . . . . . : 192.168.1.1
   Primary WINS Server . . . . . : 192.168.1.1
   Secondary WINS Server . . . . . : 
   Lease Obtained. . . . . : Monday, February 11, 2002 2:31:47 PM
   Lease Expires . . . . . : Tuesday, February 12, 2002 2:31:47 PM
    
```

Figure C-3: MAC Address/Physical Address



Figure C-4: MAC Clone



Figure C-5: Edit MAC Clone

Appendix D: Physical Setup of the Router

This section describes the physical setup of the Router, including 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. The attached brackets are shown in Figure D-1.

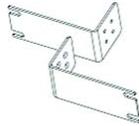


Figure D-1: Mounting Brackets

10/100 16-Port VPN Router

Line up the bracket holes with the holes located on the Router's sides. Attach the mounting brackets using the included screws, four on each side of the Router.

When the brackets are attached to the Router, you can rack-mount it. Attach the Router to the rack, using two screws on each side of the Router, as shown below in Figure D-2.

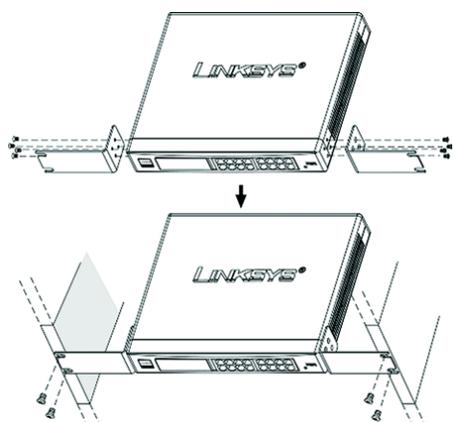


Figure D-2: Attaching the Brackets to the Router and Rack-Mounting the Router

Wall-Mounting the Router

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

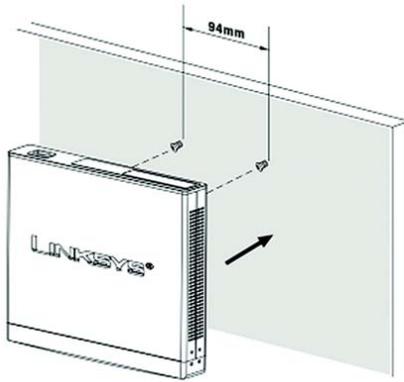


Figure D-3: Wall-Mounting the Router

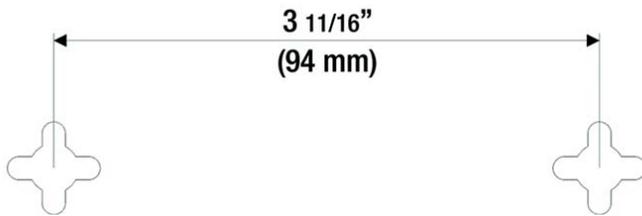
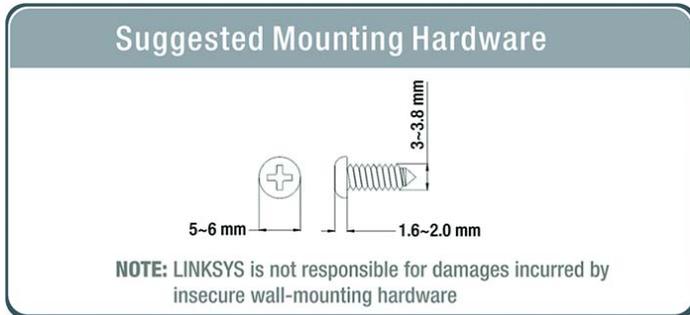


Figure D-4: Wall-Mounting Hardware

Appendix E: Battery Replacement

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 one to two 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: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix G: Glossary

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

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

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

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

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

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

AES (Advanced Encryption Standard) - A method that uses up to 256-bit key encryption to secure data.

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

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

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

Bit - A binary digit.

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

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

Broadband - An always-on, fast Internet connection.

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

10/100 16-Port VPN Router

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

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

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

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

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

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

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

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

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

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

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

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

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

EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) - A mutual authentication method that uses digital certificates.

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

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

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

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

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

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

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

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

Gateway - A system that interconnects networks.

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

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

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

10/100 16-Port VPN Router

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

Infrastructure - Currently installed computing and networking equipment.

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

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

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

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

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

ISM band - Radio band used in wireless networking transmissions.

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

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

LEAP (Lightweight Extensible Authentication Protocol) - A mutual authentication method that uses a username and password system.

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

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

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

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

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

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

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

10/100 16-Port VPN Router

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

Packet - A unit of data sent over a network.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10/100 16-Port VPN Router

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

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

10/100 16-Port VPN Router

Upload - To transmit a file over a network.

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

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

WAN (Wide Area Network) - The Internet.

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

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

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

Appendix H: Specifications

Model	RV016
Standards	IEEE 802.3, 802.3u
Ports	16 10/100 RJ-45 Ports, 2 10/100 RJ-45 Internet Port, 1 10/100 RJ-45 DMZ Port, Up to 7 10/100 RJ-45 Internet Ports
Button	Reset
Cabling Type	Category 5 Ethernet
LEDs	System, Internet 1-7, DMZ, Diag, LAN 1-13
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	52.03 oz. (1.475 kg)
Power	3.3 V, 5 Amps
Certifications	FCC Class B, CE Class B
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	0°C to 70°C (32°F to 158°F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix I: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix J: 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 K: Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at:

<http://www.linksys.com> or
[ftp.linksys.com](ftp://ftp.linksys.com)

Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:
Or fax your request in to:

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

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

800-326-7114
support@linksys.com

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

If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at:
(Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.

949-823-3000