

# LINKSYS®

A Division of Cisco Systems, Inc.



2.4GHz

## Wireless-N

### Gigabit Gaming Router

# User Guide



Model No. **WRT330N**

CISCO SYSTEMS



## Copyright and Trademarks

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

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

## How to Use This User Guide

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



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



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



This question mark provides you with a reminder about something you might need to do while using the Wireless-N Gigabit Gaming 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

<b>Chapter 1: Introduction</b>	<b>1</b>
Welcome	1
What's in this User Guide?	2
<b>Chapter 2: Planning Your Wireless Network</b>	<b>4</b>
Network Topology	4
Ad-Hoc versus Infrastructure Mode	4
Network Layout	4
<b>Chapter 3: Getting to Know the Wireless-N Gigabit Gaming Router</b>	<b>6</b>
The Back Panel	6
The Front Panel	7
The Top Panel	7
<b>Chapter 4: Connecting the Wireless-N Gigabit Gaming Router</b>	<b>8</b>
Hardware Installation	8
<b>Chapter 5: Configuring the Wireless-N Gigabit Gaming Router</b>	<b>9</b>
Overview	9
How to Access the Web-based Utility	11
The SETUP Tab - BASIC SETUP	12
The SETUP Tab - Dynamic DNS	20
The SETUP Tab - MAC ADDRESS CLONE	21
The SETUP Tab - ADVANCED ROUTING	22
The WIRELESS Tab - BASIC WIRELESS SETTINGS	23
The WIRELESS Tab - WIRELESS SECURITY	24
The WIRELESS Tab - WIRELESS MAC FILTER	27
The WIRELESS Tab - ADVANCED WIRELESS SETTINGS	28
The WIRELESS Tab - WISH	29
The SECURITY Tab - FIREWALL	30
The SECURITY Tab - VPN PASSTHROUGH	31
The ACCESS RESTRICTIONS Tab - INTERNET ACCESSS POLICY	32
The APPLICATIONS & GAMING Tab - SINGLE PORT FORWARDING	33
The APPLICATIONS & GAMING Tab - PORT RANGE FORWARDING	34
The APPLICATIONS & GAMING Tab - PORT RANGE TRIGGERING	35
The APPLICATIONS & GAMING Tab - DMZ	36

The APPLICATIONS & GAMING Tab - QOS	37
The ADMINISTRATION Tab- MANAGEMENT	39
The ADMINISTRATION Tab - LOG	41
The ADMINISTRATION Tab - DIAGNOSTICS	42
The ADMINISTRATION Tab - FACTORY DEFAULT	43
The ADMINISTRATION Tab - FIRMWARE UPGRADE	44
The STATUS Tab - ROUTER	45
The STATUS Tab - LOCAL NETWORK	46
<b>Appendix A: Troubleshooting</b>	<b>50</b>
Common Problems and Solutions	50
Frequently Asked Questions	58
<b>Appendix B: Wireless Security</b>	<b>64</b>
Security Precautions	64
Security Threats Facing Wireless Networks	64
<b>Appendix C: Upgrading Firmware</b>	<b>67</b>
<b>Appendix D: Windows Help</b>	<b>68</b>
<b>Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter</b>	<b>69</b>
Windows 2000 or XP Instructions	69
For the Router's Web-based Utility	70
<b>Appendix F: Glossary</b>	<b>72</b>
<b>Appendix G: Specifications</b>	<b>77</b>
<b>Appendix H: Warranty Information</b>	<b>79</b>
<b>Appendix I: Regulatory Information</b>	<b>80</b>
<b>Appendix J: Contact Information</b>	<b>86</b>

# List of Figures

Figure 3-1: The Router's Back Panel	6
Figure 3-2: The Router's Front Panel	7
Figure 3-3: The Router's Top Panel	7
Figure 4-1: Connect the Modem	8
Figure 4-2: Connect a PC	8
Figure 4-3: Connect the Power	8
Figure 5-1: Router Login	11
Figure 5-2: SETUP Tab - BASIC SETUP Static IP	12
Figure 5-3: Static IP: Internet Connection Type	14
Figure 5-4: Static IP: Network Address Server Settings (DHCP)	14
Figure 5-5: PPOE: Internet Connection Type	15
Figure 5-6: PPOE: Network Address Server Settings (DHCP)	15
Figure 5-7: PPTP: Internet Connection Type	17
Figure 5-8: PPTP: Network Address Server Settings (DHCP)	17
Figure 5-9: Telstra Cable: Internet Connection Type	18
Figure 5-10: Telstra Cable: Network Address Server Settings (DHCP)	18
Figure 5-11: SETUP Tab -DDNS-DynDNS.org	20
Figure 5-12: SETUP Tab -DDNS-tzo.com	20
Figure 5-13: SETUP Tab- MAC ADDRESS CLONE	21
Figure 5-14: SETUP Tab - ADVANCED ROUTING	22
Figure 5-15: Show Routing Table - Routing Table	22
Figure 5-16: WIRELESS Tab- BASIC WIRELESS SETTINGS	23
Figure 5-17: WIRELESS Tab - WIRELESS SECURITY - PSK Personal	24
Figure 5-18: WIRELESS Tab - WIRELESS SECURITY - PSK2 Personal	24
Figure 5-19: WIRELESS Tab - WIRELESS SECURITY - PSK Enterprise	25
Figure 5-20: WIRELESS Tab - WIRELESS SECURITY - PSK2 Enterprise	25
Figure 5-21: WIRELESS Tab - WIRELESS SECURITY - WEP	26
Figure 5-22: WIRELESS Tab - WIRELESS MAC FILTER	27
Figure 5-23: WIRELESS Tab - ADVANCED WIRELESS SETTINGS	28
Figure 5-24: WIRELESS Tab - WISH	29
Figure 5-25: SECURITY Tab - FIREWALL	30

Figure 5-26: SECURITY Tab - VPN PASSTHROUGH	31
Figure 5-27: ACCESS RESTRICTION Tab - INTERNET ACCESS POLICY	32
Figure 5-28: APPLICATIONS & GAMING Tab - SINGLE PORT FORWARDING	33
Figure 5-29: APPLICATIONS & GAMING Tab - PORT RANGE FORWARDING	34
Figure 5-30: APPLICATIONS & GAMING Tab - PORT RANGE TRIGGERING	35
Figure 5-31: APPLICATIONS & GAMING Tab - DMZ	36
Figure 5-32: APPLICATIONS & GAMING Tab - QOS	37
Figure 5-33: ADMINISTRATION Tab - MANAGEMENT	39
Figure 5-34: ADMINISTRATION Tab - LOG	41
Figure 5-35: ADMINISTRATION Tab - DIAGNOSTICS	42
Figure 5-36: ADMINISTRATION Tab - FACTORY DEFAULT	43
Figure 5-37: ADMINISTRATION Tab -FIRMWARE UPGRADE	44
Figure 5-38: STATUS Tab - ROUTER	45
Figure 5-39: STATUS Tab - LOCAL NETWORK	46
Figure 5-40: DHCP Client Table - Routing Table	46
Figure 5-41: STATUS Tab - WIRELESS NETWORK	47
Figure 5-42: Administration Log	47
Figure 5-43: Administration Diagnostics	47
Figure 5-44: Administration Tab - Factory Defaults	47
Figure 5-45: Administration Tab - Firmware Upgrade	47
Figure 5-46: Status Tab - Router	47
Figure 5-47: Status Tab - Local Network	47
Figure 5-48: DHCP Client Table- Routing Table	47
Figure 5-49: Status Tab - Wireless	47
Figure C-1: Firmware Upgrade	67
Figure E-1: IP Configuration Screen	69
Figure E-2: MAC Address/Adapter Address	70
Figure E-3: MAC Address/Physical Address	71
Figure E-4: Wireless MAC Filter	71
Figure E-5: MAC Address Cloning	71
Figure E-6: Wireless MAC Filter	71
Figure E-7: MAC Address Cloning	71

# Chapter 1: Introduction

## Welcome

Thank you for choosing the Linksys Wireless-N Gigabit Gaming Router. The Wireless-N Gigabit Gaming Router will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely and with a greater range of up to three times farther than standard Wireless-G.

How does the Wireless-N Gigabit Gaming Router do all of this? A router is a device that allows access to an Internet connection over a network. With the Wireless-N Gigabit Gaming Router, this access can be shared over the four switched ports or via the wireless broadcast.

Use the WPA2 standard to secure your wireless network while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology. The Router also offers VPN passthrough and other features, which can be configured through the easy-to-use, browser-based utility.

The incredible speed of Wireless-N makes it ideal for media-centric applications like streaming video and Voice over IP (VoIP) telephony, so your network can handle multiple data streams at the same time, with no degradation in performance.

But what does all of this mean?

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

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

PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. The Wireless-N Gigabit Gaming Router bridges wireless and wired networks, allowing them to communicate with each other.

Linksys recommends using the Setup Wizard on the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard, then use the instructions in this Guide to help you connect the Router and configure it. These instructions should be all you need to get the most out of the Wireless-N Gigabit Gaming Router.

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

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

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

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

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

## What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-N Gigabit Gaming Router.

- **Chapter 1: Introduction**  
This chapter describes the Router's applications and this User Guide.
- **Chapter 2: Planning Your Wireless Network**  
This chapter describes the basics of wireless networking.
- **Chapter 3: Getting to Know the Wireless-N Gigabit Gaming Router**  
This chapter describes the physical features of the Router.
- **Chapter 4: Connecting the Wireless-N Gigabit Gaming Router**  
This chapter instructs you on how to connect the Router to your network.
- **Chapter 5: Configuring the Wireless-N Gigabit Gaming Router**  
This chapter explains how to use the Web-based Utility to configure the settings on the Wireless-N Gigabit Gaming Router.
- **Appendix A: Troubleshooting**  
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-N Gigabit Gaming Router.
- **Appendix B: Wireless Security**  
This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- **Appendix C: Upgrading Firmware**  
This appendix instructs you on how to upgrade the firmware on the Router should you need to do so.
- **Appendix D: Windows Help**  
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- **Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter**  
This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router.
- **Appendix F: Glossary**  
This appendix gives a brief glossary of terms frequently used in networking.



## Wireless-N Gigabit Gaming Router

- **Appendix G: Specifications**  
This appendix provides the technical specifications for the Router.
- **Appendix H: Warranty Information**  
This appendix supplies the warranty information for the Router.
- **Appendix I: Regulatory Information**  
This appendix supplies the regulatory information regarding the Router.
- **Appendix J: Contact Information**  
This appendix provides contact information for a variety of Linksys resources, including Technical Support.

# Chapter 2: Planning Your Wireless Network

## Network Topology

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

*ssid (service set identifier): your wireless network's name.*

## Ad-Hoc versus Infrastructure Mode

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

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

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

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

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

## Network Layout

The Wireless-N Gigabit Gaming Router has been specifically designed for use with your Wireless-N, Wireless-G, and Wireless-B products. It will work with notebook adapters for your laptop computers, PCI adapters for your

## Wireless-N Gigabit Gaming Router

desktop computers, and USB adapters for your USB connectivity needs. The Router can also communicate with other devices, such as wireless print servers and bridges.

When you wish to connect your wireless network to your wired network, you can use the Router's four local Ethernet ports. To add more ports, connect one of the Router's local ports to any Linksys switch.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at [www.linksys.com](http://www.linksys.com) for more information about products that work with the Wireless-N Gigabit Gaming Router.

# Chapter 3: Getting to Know the Wireless-N Gigabit Gaming Router

## The Back Panel

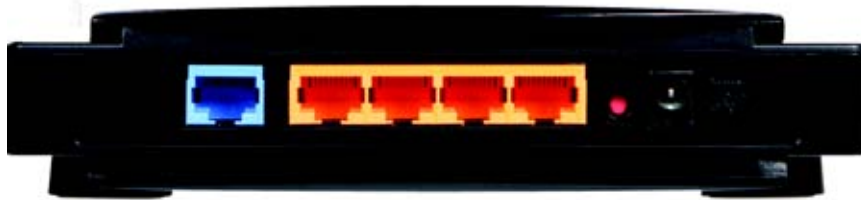


Figure 3-1: The Router's Back Panel

The Router's ports, where the cables are connected, and Reset button are located on the back panel.

- INTERNET** The Internet port is where you will connect your broadband modem.
- ETHERNET 1, 2, 3, 4** These ports (1, 2, 3, 4) connect the Router to your wired PCs and other Ethernet network devices.
- Reset Button** There are two ways to reset the Router's factory defaults. Either press the **Reset** button, for approximately five seconds, or restore the defaults from the Administration - Factory Defaults tab of the Router's Web-based Utility.
- Power** The **Power** port is where you will connect the power adapter.



**IMPORTANT:** Resetting the Router will erase all of your settings (Internet connection, wireless security, and other settings) and replace them with the factory defaults. Do not reset the Router if you want to retain these settings.

## The Front Panel



Figure 3-2: The Router's Front Panel

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

<b>POWER</b>	Green. The <b>POWER</b> LED lights up and will stay on while the Router is powered on.
<b>ETHERNET 1, 2, 3, 4</b>	Green/Orange. The numbered LEDs, correspond with the numbered ports on the Router's back panel and light up when the Router is connected to a device through the corresponding port. If the LED is flashing, the Router is sending or receiving data over that port. The light will be orange when there is a 1000 Mbps gigabit connection.
<b>INTERNET</b>	Green. The <b>INTERNET</b> LED lights up when there is a connection through the Internet port.
<b>WIRELESS</b>	Green. The <b>WIRELESS</b> LED lights up when there is a wireless connection. If the LED is flashing, the Router is sending or receiving data over the wireless network.
<b>SECURITY</b>	Green. The <b>SECURITY</b> LED is green when PSK/PSK2 is enabled.  Orange. The <b>SECURITY</b> LED is orange when WEP is enabled or no security is enabled.  Off. The <b>SECURITY</b> LED is off when the security button on the top of the unit is disabled.

## The Top Panel

The Router has a button reserved for a future function.



Figure 3-3: The Router's Top Panel

# Chapter 4: Connecting the Wireless-N Gigabit Gaming Router

## Hardware Installation

1. Make sure that all of your hardware is powered off, including the broadband modem and PCs.
2. Connect your broadband modem's Ethernet cable to the Router's Internet port.
3. Connect one end of an Ethernet network cable to one of the numbered ports on the back of the Router. Connect the other end to an Ethernet port on a network device, e.g., a PC, print server, or switch.

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

4. Power on the broadband modem.
5. Connect the included power adapter to the Router's Power port, and then plug the power adapter into an electrical outlet. The Power LED on the front panel will light up when the adapter is connected properly.
6. Power on your PC(s).
7. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your wireless devices.

Proceed to "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router".



Figure 4-1: Connect the Modem



Figure 4-2: Connect a PC



Figure 4-3: Connect the Power



**IMPORTANT:** Make sure you use the power adapter that is supplied with the Router. Use of a different power adapter could damage the Router.

# Chapter 5: Configuring the Wireless-N Gigabit Gaming Router

## Overview

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

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

- **BASIC SETUP.** On the *BASIC SETUP* screen, enter the Internet connection settings provided by your Internet Service Provider (ISP). If you do not have this information, you can call your ISP to request the settings. When you have the setup information, then you can configure the Router.
- **MANAGEMENT.** Click the **ADMINISTRATION** tab and then the **MANAGEMENT** tab. The Router's default password is **admin**. To secure the Router, change the password from its default.
- **WIRELESS.** On the *BASIC WIRELESS SETTINGS* screen, set the basic configuration for your wireless network.

There are seven main tabs: **SETUP**, **WIRELESS**, **SECURITY**, **ACCESS RESTRICTIONS**, **APPLICATIONS & GAMING**, **ADMINISTRATION**, and **STATUS**. Additional tabs will be available after you click one of the main tabs.

## SETUP

- **BASIC SETUP.** Enter the Internet connection and network settings on this screen.
- **DDNS.** Enable the Router's Dynamic Domain Name System (DDNS) feature on this screen.
- **MAC ADDRESS CLONE.** If you need to clone a MAC address onto the Router, use this screen.
- **ADVANCED ROUTING.** Use this screen to alter dynamic and static routing configurations.

## WIRELESS

- **BASIC WIRELESS SETTINGS.** Enter the basic settings for your wireless network on this screen.
- **WIRELESS SECURITY.** Enable and configure the security settings for your wireless network.
- **WIRELESS MAC FILTER.** Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.
- **ADVANCED WIRELESS SETTINGS.** For advanced users, you can alter data transmission settings on this screen.
- **WIRELESS QoS.** Allows you to prioritize the traffic of various wireless applications.

## SECURITY

- **FIREWALL.** You can enable or disable the Router's firewall, as well as various filters.
- **VPN PASSTHROUGH.** To enable or disable IPSec, L2TP, and/or PPTP Passthrough, use this screen.

## ACCESS RESTRICTIONS

**INTERNET ACCESS POLICY.** Create policies to control Internet access for your local network users.

## APPLICATIONS & GAMING

- **SINGLE PORT FORWARDING.** This allows you to do port mapping and forwarding for a single service port.
- **PORT RANGE FORWARDING.** Set up public services or other specialized Internet applications on your network.
- **PORT Range Triggering.** Configure the Router to watch outgoing data for specific port numbers.
- **DMZ.** Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services.
- **QoS.** QUALITY of SERVICE (QoS) ensures better service to high-priority types of network traffic.

## ADMINISTRATION

- **MANAGEMENT.** On this screen, alter the Router's password, access privileges, and UPnP settings. You can also use this screen to back up and restore the Router's configuration file.
- **LOG.** If you want to view activity logs, click this tab.



- **DIAGNOSTICS.** If you want to run a ping or traceroute test, then use this screen.
- **FACTORY DEFAULTS.** If you want to restore the Router's factory defaults, then use this screen.
- **FIRMWARE UPGRADE.** Click this tab if you want to upgrade the Router's firmware.

## STATUS

- **ROUTER.** This screen provides status information about the Router.
- **LOCAL NETWORK.** This provides status information about the local network.
- **WIRELESS NETWORK.** This provides status information about the wireless network.

## 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. Press the **Enter** key.

A screen will appear asking you for your User name and Password. Leave the *User Name* field blank. Enter **admin** in the *Password* field. Then click the **OK** button.



Figure 5-1: Router Login

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

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

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

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

## The SETUP Tab - BASIC SETUP

The *BASIC SETUP* screen is the first screen you see when you access the Web-based Utility. An overview of the screens is presented here. Screen variations are described in detail under each Internet Connection Type.

### Internet Connection Type

The Internet Setup section configures the Router for your Internet connection type. This information can be obtained from your ISP. The Router supports four connection types: Static IP, PPPoE, PPTP and Telstra BigPond.



**NOTE:** Some of the Internet Connection Types may not be available in your area.

### Optional Settings (Required by some ISPs)

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

**Router Name.** You can customize the Router's name. The default is WRT330N.

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

**MTU and Size.** The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. To manually set a value, select **Manual** and enter the value desired in the *Size* field. You should leave this value in the 1200 to 1500 range. Most DSL users should use the value 1492. The default is **Auto**, which allows the Router to select the best MTU for your Internet connection.

### Router IP

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

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

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

### Network Address Server Settings (DHCP)

The Network Address Server Settings section allows you to change the Router's local network settings. Detailed information is listed under each Internet Connection Type.

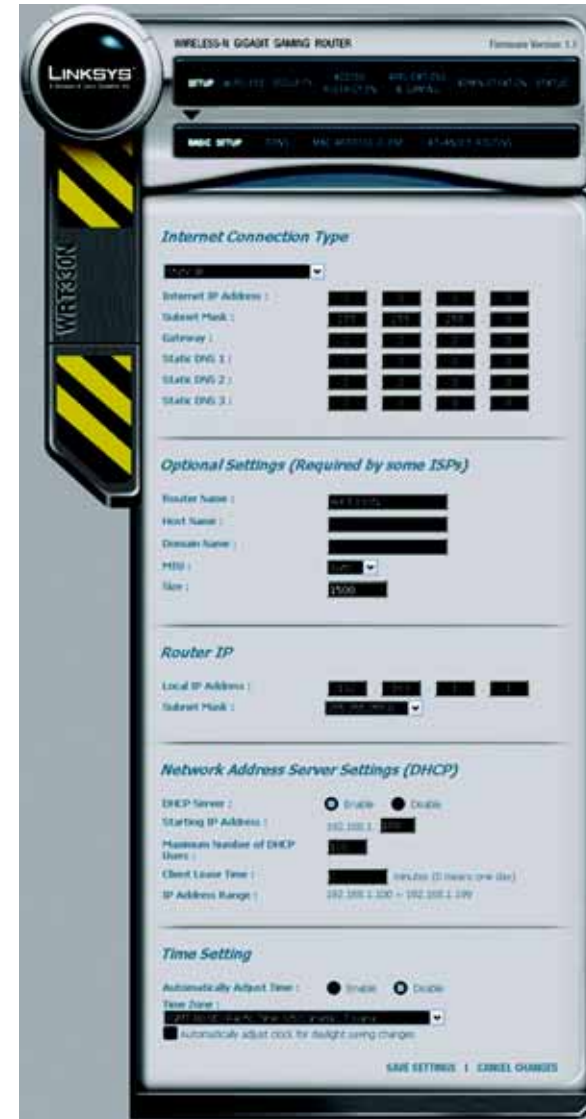


Figure 5-2: SETUP Tab - BASIC SETUP Static IP

## Time Setting

**Automatically Adjust Time.** You can choose to **Enable** or **Disable** the automatic time adjustment. If you select **Enable**, you will need to select the correct Time Zone for your Router.

**Time Zone.** Select the time zone in which your network functions. If you want the Router to automatically adjust the clock for daylight savings, then select the checkbox.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

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

## The SETUP Tab - BASIC SETUP - Static IP

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

### Internet Connection Type

**Internet IP Address.** This is the IP address that the Router has when seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

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

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

**Static DNS 1-3.** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

### Network Address Server Settings (DHCP)

**DHCP Server.** The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server. DHCP is enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**.

**Starting IP Address.** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the Start IP Address must be 192.168.1. 2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

**Maximum Number of DHCP Users (Optional).** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

**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. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

**IP Address Range.** The IP Address Range is Static and cannot be changed.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

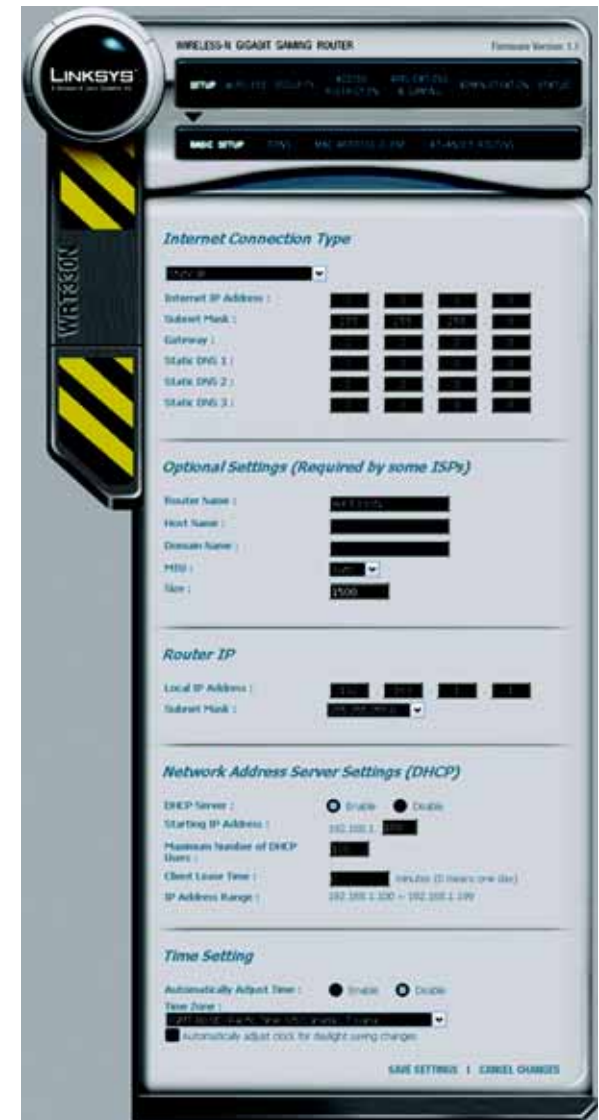


Figure 5-3: SETUP: BASIC SETUP: Static IP

## The SETUP Tab - BASIC SETUP - PPPoE

### Internet Connection Type

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.

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

**Service Name.** If provided by your ISP, enter the Service Name.

**Connect on Demand and Max Idle Time.** You can configure the Router to cut the Internet connection after it has been inactive for a specific period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter 0 in the *Max Idle Time* field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

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

### Network Address Server Settings (DHCP)

**DHCP Server.** The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server. DHCP is enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**.

**Starting IP Address.** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

**Maximum Number of DHCP Users (Optional).** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 50.

**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"



Figure 5-4: SETUP: BASIC SETUP: PPoE Settings

this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

**IP Address Range.** The IP Address Range is Static and cannot be changed.

**Static DNS 1-3.** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

**WINS.** The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



**IMPORTANT:** For DSL users, if you need to enable PPPoE support, remember to remove any PPPoE applications that are installed on your PCs.

***dynamic ip address:** a temporary IP address assigned by a DHCP server.*

## The SETUP Tab - BASIC SETUP - PPTP

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

### Internet Connection Type

**Internet IP Address.** This is the IP address that the Router has, when seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

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

**Service IP Address:** If provided by your ISP, enter the Service IP Address.

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

**Connect on Demand and Max Idle Time Min. and Sec.** You can configure the Router to cut the Internet connection after it has been inactive for a specific period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter 0 in the *Max Idle Time* field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

### Network Address Server Settings (DHCP)

**DHCP Server.** The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server. DHCP is enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**. DHCP is enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**. If you disable DHCP, remember to assign a static IP address to the Router.

**Starting IP Address.** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the Start IP Address must be 192.168.1. 2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

**Maximum Number of DHCP Users (Optional).** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 50.

**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"

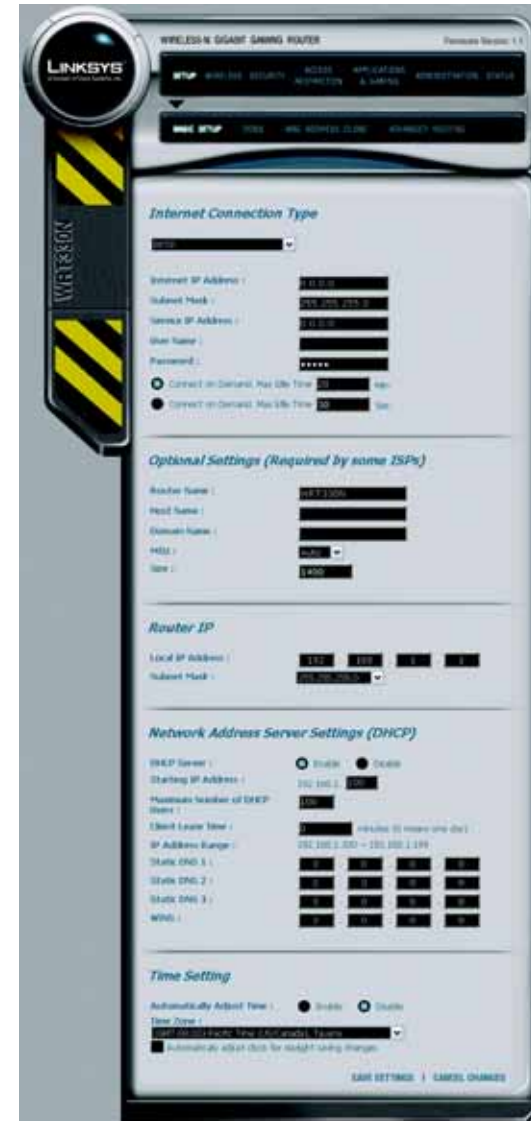


Figure 5-5: SETUP: BASIC SETUP:PPTP

this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

**IP Address Range.** The IP Address Range is Static and cannot be changed.

**Static DNS 1-3.** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

**WINS.** The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



## The SETUP Tab - BASIC SETUP - Telstra BigPond

Telstra BigPond is a service used in Australia only. Check with your ISP for the necessary setup information.

### Internet Connection Type

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

**Heart Beat Server:** Enter the Heart Beat Server information.

### Network Address Server Settings (DHCP)

**DHCP Server.** The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server. DHCP is enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**.

**Starting IP Address.** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the Start IP Address must be 192.168.1. 2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

**Maximum Number of DHCP Users (Optional).** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

**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. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

**IP Address Range.** The IP Address Range is Static and cannot be changed.

**Static DNS 1-3.** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

**WINS.** The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

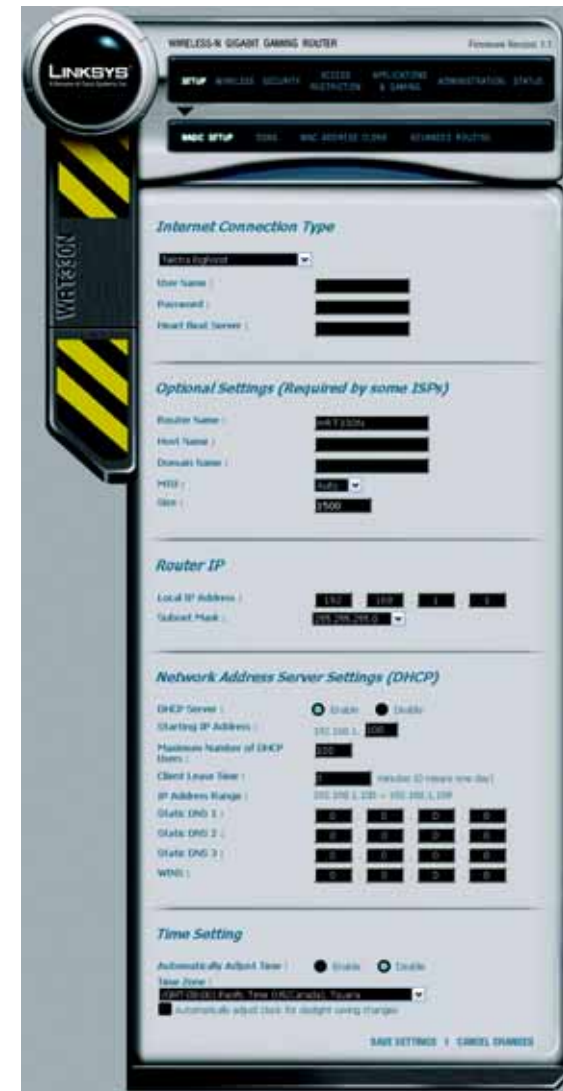


Figure 5-6: SETUP:BASIC SETUP: Telstra BigPond



**NOTE:** To test your settings, connect to the Internet now.

## The SETUP Tab - Dynamic DNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com.

### Dynamic DNS

#### DDNS Service

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

#### DynDNS.org

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

**System.** Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**.

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

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

**Update.** To manually trigger an update, click this button.

#### TZO.com

**E-mail Address, TZO Password, and Domain Name.** Enter the settings of the account you set up with TZO.

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

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

**Update.** To manually trigger an update, click this button.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-7: SETUP Tab -DDNS-DynDNS.org



Figure 5-8: SETUP Tab -DDNS-tzo.com

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

## The SETUP Tab - MAC ADDRESS CLONE

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

### Mac Cloning

To use MAC address cloning, select **Enable**. Otherwise, keep the default, **Disable**.

**MAC Address.** Enter the MAC Address registered with your ISP.

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

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-9: SETUP Tab- MAC ADDRESS CLONE

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

## The SETUP Tab - ADVANCED ROUTING

### NAT

If this Router is hosting your network's connection to the Internet, select **Enabled**. If another Router exists on your network, select **Disabled**. When the NAT setting is disabled, dynamic routing will be enabled.

### Dynamic Routing

This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. To use dynamic routing, select **Enabled**. Otherwise, select **Disabled**. When the NAT setting is disabled, dynamic routing will be enabled.

### Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Use this feature to set up a static route between the Router and another network (you can have up to 20 static routes). To create a static route, alter the following settings:

**Routing Entries.** Select the number of the static route from the drop-down menu.

**Enter Route Name.** Enter a name for the static route, using a maximum of 25 alphanumeric characters.

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

**Subnet Mask.** The Subnet Mask determines which portion of a Destination IP address is the network portion, and which portion is the host portion.

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

**Interface.** Select **LAN & Wireless** or **WAN (Internet)**, depending on the location of the final destination.

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

When you have finished making changes to the Advanced Routing screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-10: SETUP Tab - ADVANCED ROUTING



Figure 5-11: Show Routing Table - Routing Table

## The WIRELESS Tab - BASIC WIRELESS SETTINGS

### Wireless Setting

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

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

**Radio Band.** For best performance in a network using Wireless-N, Wireless-G and Wireless-B devices, keep the default, **Wide - 40MHz Channel**. For Wireless-G and Wireless-B networking only, select **Standard - 20MHz Channel**. If you are not sure which radio band to select, keep the default, **Auto**.

**Wide Channel.** If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu.

**Standard Channel.** Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. If you are not sure which channel to select, keep the default, **Auto**.

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

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-12: WIRELESS Tab- BASIC WIRELESS SETTINGS



**NOTE:** If you select Wide - 40MHz Channel for the Radio Band setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary one (Standard Channel). This will enhance Wireless-N performance.

## The WIRELESS Tab - WIRELESS SECURITY

These settings configure the security of your wireless network. There are six wireless security modes supported by the Router: PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK-2 Enterprise, RADIUS, and WEP. PSK (Pre-Shared Key), is a security standard stronger than WEP (Wired Equivalent Privacy), while RADIUS stands for Remote Authentication Dial-In User Service.) For details on configuring wireless security for the Router, turn to "Appendix B: Wireless Security." If you do not want to use wireless security, select **Disabled** in the Security Mode.

### Wireless Security

**Security Mode.** Select the mode you want to use: **PSK-Personal**, **PSK2-Personal**, **PSK-Enterprise**, **PSK2-Enterprise**, **RADIUS**, or **WEP**. PSK2 is a more advanced, more secure version of PSK.

#### PSK Personal

**Encryption.** Select the algorithm you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**Pre-shared Key.** Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

**Key Renewal.** Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

#### PSK2 Personal

**Encryption.** Select the algorithm(s) you want to use, **AES** or **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**Pre-shared Key.** Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

**Key Renewal.** Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-13: WIRELESS Tab - WIRELESS SECURITY - PSK Personal



Figure 5-14: WIRELESS Tab - WIRELESS SECURITY - PSK2 Personal

## PSK Enterprise

This option features PSK used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

**Encryption.** Select the algorithm(s) you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**RADIUS Server.** Enter the IP address of your RADIUS server.

**RADIUS Port.** Enter the port number of your RADIUS server.

**Shared Key.** Enter the key shared by the Router and RADIUS server.

**Key Renewal.** Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

## PSK2 Enterprise

This option features PSK2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

**Encryption.** Select the algorithm(s) you want to use, **AES** or **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**RADIUS Server.** Enter the IP address of your RADIUS server.

**RADIUS Port.** Enter the port number of your RADIUS server.

**Shared Key.** Enter the key shared by the Router and RADIUS server.

**Key Renewal.** Enter the Key Renewal period, which tells the Router how often it should change encryption keys.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-15: WIRELESS Tab - WIRELESS SECURITY - PSK Enterprise



Figure 5-16: WIRELESS Tab - WIRELESS SECURITY - PSK2 Enterprise

## WEP

WEP is a basic encryption method offering two levels of encryption; 128-bit is stronger than 40/64-bit encryption.

**Encryption.** Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **128-bit (26 hex digits)**.

**Passphrase.** To automatically generate keys, enter your passphrase. Then click the **Generate** button.

**Key 1-4.** If you want to manually enter the WEP keys, then enter them in the *Key 1-4* fields.

**TX Key.** To indicate which WEP key to use, select a transmit key number.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-17: WIRELESS Tab - WIRELESS SECURITY - WEP



## The WIRELESS Tab - WIRELESS MAC FILTER

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.

### Wireless MAC Filter

To filter wireless users by MAC Address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC Address, select **Disable**.

### Access Restrictions

**Prevent.** Click this button to block wireless access from the devices listed on this screen.

**Permit.** Click this button to allow wireless access by the devices listed on this screen.

### MAC Address Filter List

Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. The list is shown by MAC Address. Enter the MAC addresses of the devices whose wireless access you want to block or allow. When you have finished making changes to the *Wireless Client List*, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-18: WIRELESS Tab - WIRELESS MAC FILTER

## The WIRELESS Tab - ADVANCED WIRELESS SETTINGS

These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

### Advanced Wireless Setting

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

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

**Beacon Interval.** This value indicates the frequency interval of the beacon which is a packet broadcast by the Router to synchronize the wireless network. Enter a value between a-65535 mscs. The default value is **100 msc**.

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

**Fragmentation Threshold.** This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, a slight increase should help. Too low a setting may result in poor network performance. Only minor reduction of the default value is recommended. The value can be between 256 and 2346. In most cases, it should remain at its default value of **2346**.

**RTS Threshold.** Should you encounter inconsistent data flow, only minor reduction of the default value, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. In most cases, keep its default value of **2346**.

**Network Density.** Adjust the density allowed on the network. The default is **Low**.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over



Figure 5-19: WIRELESS Tab - ADVANCED WIRELESS SETTINGS

## The WIRELESS Tab - QoS

Wireless QoS allows the router to give priority to certain types of wireless network traffic.

### QoS

To enable Wireless QoS, click **Enable**. If you do not wish to use Wireless QoS, select **Disabled**.

### Priority Classifiers

**HTTP:** Allows the router to recognize HTTP traffic that contains common audio and video types. The router will give higher priority to these types of traffic when they are detected. To enable HTTP classification, select **Enable**.

**Windows Media Center:** Allows the router to recognize audio and video traffic generated by Windows Media Center PC. The router will give higher priority to these types of traffic when they are detected. To enable Windows Media Center classification, select **Enable**.

**Automatic:** Allows the router to automatically classify and prioritize all other types of wireless traffic. It will give lower priority to traffic it detects as bulk (i.e., printing, email send/receive, etc.), and give higher priority to real-time traffic (i.e., VoIP, streaming video, etc.).

### Add/Edit Wireless QoS Rules

**Name:** Enter a name for the Wireless QoS rule. You should choose a name that identifies with the rule created, i.e. Online Game, VoIP, Video, etc.

**Priority:** Choose the priority you would like to apply to your rule. The available options from lowest priority to highest priority are:

**Background (BK):** These are bulk traffic such as a print job, email send/receive, etc.

**Best Effort (BE):** These are regular Internet traffic, such as web surfing, FTP downloads, etc.

**Video (VI):** Streaming video traffic that needs higher priority to ensure a smooth video.

**Voice (VO):** Voice traffic that will be given the highest priority.

**Host Internal IP Range:** Select the IP range of the devices this rule will apply to. If the rule only applies to one device, enter the same IP for both the **From** and **To** field.



Figure 5-20: WIRELESS Tab - QoS

**Host Internal Port Range:** Select the application port range that will apply the QoS rule. If the rule will only apply to one application port, enter the same port number in both the **From** and the **To** field.

**Host External IP Range:** Enter the IP address range of the device that will receive traffic on the remote end of the connection. If there's only one device on the remote end, enter the same IP address in the **From** and **To** field.

**Host External Port Range:** Enter the port range of the device that will receive traffic on the remote end of the connection. If there's only one device on the remote end, enter the same port number in the **From** and **To** field.

### Wireless QoS Rule List

This field will display the current custom rules that are applied by the router. To edit the rule, click the **pencil** icon next to the rule. To delete the rule, click the **red circle** icon next to the rule.

Click **SAVE SETTINGS** when you have finished editing the Wireless QoS settings. Click **CANCEL CHANGES** to clear all fields and start over.

## The SECURITY Tab - FIREWALL

The *FIREWALL* screen offers a firewall and filters that block specific Internet data types.

### Firewall

**Firewall Protection.** A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network. Select **Enable** to use a firewall, or **Disable** to disable it.

### Block WAN Request

**Block WAN Requests.** When enabled, this feature keeps your network from being “pinged,” or detected, by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network. Click in the box to block anonymous internet requests.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-21: SECURITY Tab - FIREWALL

## The SECURITY Tab - VPN PASSTHROUGH

The *VPN PASSTHROUGH* screen allows you to allow VPN tunnels using PPPoE, IPSec, PPTP or L2TP protocols to pass through the Router.

### VPN Passthrough

**PPPoE Passthrough.** PPPoe (Point-to-Point Protocol over Ethernet) allows a PPP session to be initiated on a simple bridging Ethernet connected client. To allow PPPoE Passthrough, click the **Enable** button. To disable PPPoE Passthrough, click the **Disable** button.

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

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

**L2TP Passthrough.** L2TP (Layer 2 Tunneling Protocol) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, click the **Enable** button. To disable L2TP Passthrough, click the **Disable** button.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-22: SECURITY Tab - VPN PASSTHROUGH

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

*pppoe:* a signaling protocol defined within PPPoE as well as the encapsulation method.

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

*pptp:* 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.

## The ACCESS RESTRICTIONS Tab - INTERNET ACCESS POLICY

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

### Internet Access

**Access Policy.** Select an access policy to see a summary of, or delete. Select a policy from the drop-down menu. Click the **Delete This Entry** button or the **Summary** button. On the *Summary* screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled).

### Apply Policy

**Enter Policy Name.** Enter the Policy Name in the field provided and to enable.

**Status.** Click for **Enabled** or **Disabled**.

**Edit List.** Click this button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of PCs. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.

### Access Restrictions

**Deny or Allow.** Choose to have your policy block or allow internet access. Select specific days and times in the Schedule section.

### Schedule

Decide which days and what times you want this policy to be enforced.

**Days.** Select **Everyday** or the individual days during which the policy will be in effect.

**Times.** Select the times in which deny or allow internet access. Select **24 Hours** or enter the hours, minutes and AM or PM during which the policy will be in effect.

### Web Blocking by URL Address

You can block up to four websites by specific URL addresses. Enter each URL in a separate field.



Figure 5-23: ACCESS RESTRICTION Tab - INTERNET ACCESS POLICY

## Blocked Applications

Three applications can be blocked per Policy.

**Applications/Blocked List.** You can filter access to various services accessed over the Internet, such as FTP or telnet. From the Applications list, select the application you want to block. Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button.

**Application Name.** If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field.

**Port Range.** For the named application, enter its range in the *Port Range* fields.

**Protocol.** For the named application, select its protocol from the *Protocol* drop-down menu.

Once you have entered the applications, click the **Add** button. To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click the **Modify** button. To delete a service, select it from the Application list. Then click the **Delete** button.

Click **SAVE Settings** to save your changes, or click **CANCEL CHANGES** to clear all fields and start over.



## The APPLICATIONS & GAMING Tab - SINGLE PORT FORWARDING

When you click the APPLICATIONS & GAMING tab, you will see the *SINGLE PORT FORWARDING* screen. You can customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

### Single Port Forwarding

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Click the **Enable** checkbox to activate this entry.

For additional applications, complete the following fields:

**Application Name.** Enter the name of the application.

**External Port.** Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

**Internal Port.** Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

**Protocol.** Select the protocol **TCP** or **UDP**, or select **Both**.

**To IP Address.** Enter the IP address of the server that should receive the requests. To find the IP address, go to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter." If you assigned a static IP address to the server, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.

**Enable.** Click the **Enable** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-24: APPLICATIONS & GAMING Tab - SINGLE PORT FORWARDING

*tcp*: a network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

*udp*: a network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

## The APPLICATIONS & GAMING Tab - PORT RANGE FORWARDING

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

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

If you need to forward all ports to one PC, click the **DMZ** tab.

### Port Range Forwarding

To add an application, complete the following fields:

**Application Name.** Enter the name of the application.

**Start ~ End Port.** Enter the number or range of port(s) used by the server or Internet application. Check with the Internet application documentation for more information.

**Protocol.** Select the protocol **TCP** or **UDP**, or select **Both**.

**To IP Address.** Enter the IP address of the server that you want the Internet users to be able to access. To find the IP address, go to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter." If you assigned a static IP address to the server, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.

**Enable.** Click the **Enable** checkbox to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

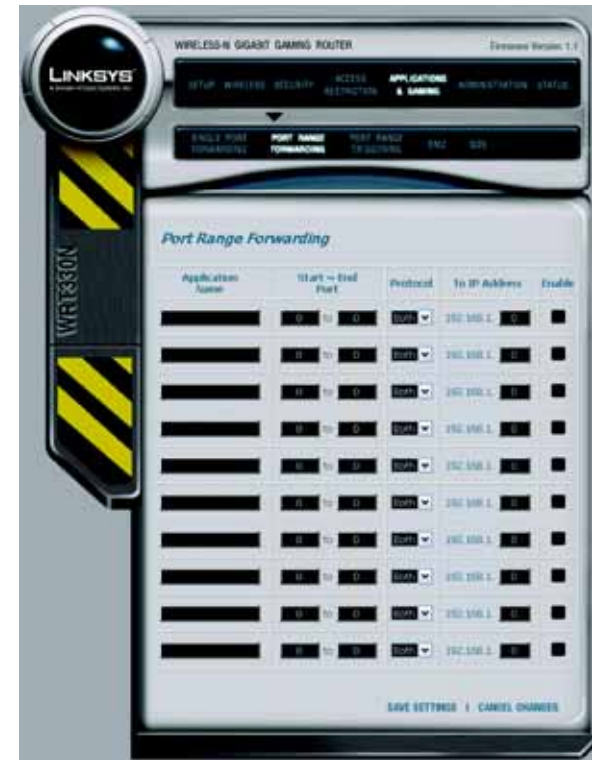


Figure 5-25: APPLICATIONS & GAMING Tab - PORT RANGE FORWARDING

## The APPLICATIONS & GAMING Tab - PORT RANGE TRIGGERING

This screen instructs 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 sent to the proper computer by way of IP address and port mapping rules.

### Port Range Triggering

To add an application, complete the following fields:

**Application Name.** Enter the name of the application.

**Triggered Range.** Enter the starting and ending port numbers of the triggered port range. Check with the Internet application documentation for the port number(s) needed.

**Forwarded Range.** Enter the starting and ending port numbers of the forwarded port range. Check with the Internet application documentation for the port number(s) needed.

**Enable.** Click the **Enable checkbox** to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.

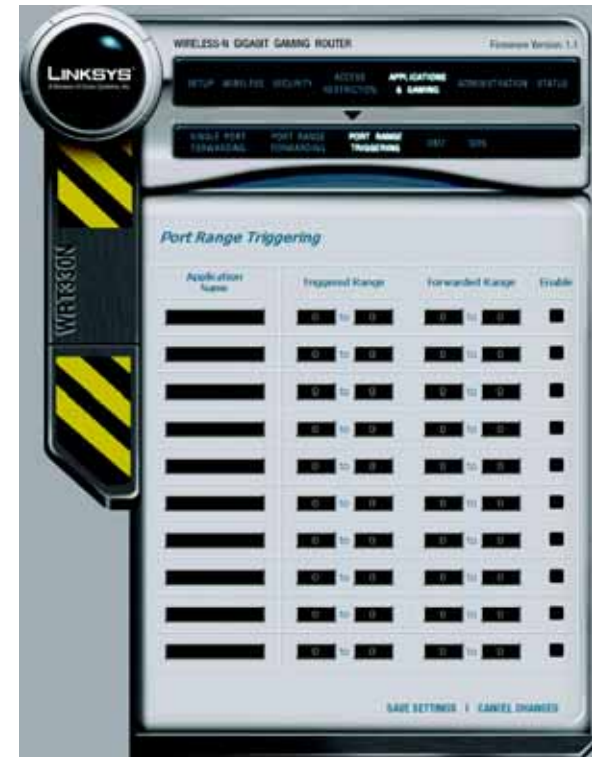


Figure 5-26: APPLICATIONS & GAMING Tab - PORT RANGE TRIGGERING

## The APPLICATIONS & GAMING Tab - DMZ

The *DMZ* screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

### DMZ

To use this feature, select **Enabled**. To disable DMZ hosting, select **Disabled**.

**DMZ Host IP Address.** If you want to specify the DMZ host by IP address, complete the IP address in the field provided.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-27: APPLICATIONS & GAMING Tab - DMZ

## The APPLICATIONS & GAMING Tab - QoS

Quality of Service (QoS) allows the router to give priority to certain types of network traffic.

### QoS (Quality of Service)

To enable QoS, click **Enable**. If you do not wish to use QoS, select **Disabled**.

**Automatic Classification:** The router can automatically classify the types of traffic on your network. To enable automatic classification, click **Enable**.

**Dynamic Fragmentation:** The router can dynamically break down data that is too large to transmit in one session. This can improve network traffic speeds. To enable dynamic fragmentation, click **Enable**.

**Automatic Uplink Speed:** The router can automatically detect the maximum uplink speed of your Internet connection and optimize network traffic accordingly. To enable automatic uplink speed detection, click **Enable**.

**Measured Uplink Speed:** If you have enabled Automatic Uplink Speed, this field will display the speed measured by the router.

**Manual Uplink Speed:** If you have chosen not to enable Automatic Uplink Speed, select your maximum uplink speed from the pull down list.

**Connection Type:** Select the type of Internet connection you have, **Cable** or **DSL**. If you wish to have the router detect the type of connection, select **Auto-detect**.

**Detected Network:** If you have chosen Auto-detect for Connection Type, the type of connection detected by the router will be displayed here.

### Add QoS Rule

The router has built-in QoS rules that gives priority to Voice, Video and Game traffic. If you wish to add your own rules in addition to the router's built-in rules, click **Enable**.

**Name:** Enter a name for the QoS rule. You should choose a name that identifies with the rule created, i.e. Online Game, VoIP, Video, etc.

**Priority:** The priority of the traffic can be selected here. Enter a number between **1** and **255**. Traffic with lower numbers will have higher priority than traffic with higher numbers. i.e. Traffic with priority of 1 will have higher priority than traffic with a priority of 2.



Figure 5-28: APPLICATIONS & GAMING Tab - QoS

**Protocol:** Select the protocols that will apply the QoS rule. You may choose from Any, TCP, UDP, Both (TCP and UDP), or ICMP.

**Local IP Range:** Select the IP range of the devices this rule will apply to. If the rule only applies to one device, enter the same IP for both the **From** and **To** field.

**Local Port Range:** Select the application port range that will apply the QoS rule. If the rule will only apply to one application port, enter the same port number in both the **From** and the **To** field.

**Remote IP Range:** Enter the IP address range of the device that will receive traffic on the remote end of the connection. If there's only one device on the remote end, enter the same IP address in the **From** and **To** field.

**Remote Port Range:** Enter the port range of the device that will receive traffic on the remote end of the connection. If there's only one device on the remote end, enter the same port number in the **From** and **To** field.

Click **Add** to add the new QoS rule you have just created into the router's rules list. Click **Clear** to clear all fields and start over.

### QoS Rule List

This field will display the current custom rules that are applied by the router. To edit the rule, click the **pencil** icon next to the rule. To delete the rule, click the **red circle** icon next to the rule.

Click **SAVE SETTINGS** when you have finished editing the QoS settings. Click **CANCEL CHANGES** to clear all fields and start over.

## The ADMINISTRATION Tab- MANAGEMENT

When you click the Administration tab, you can select the *MANAGEMENT* screen. This screen allows you to change the Router's access settings and configure the UPnP (Universal Plug and Play) features. You can also back up and restore the Router's configuration file.

### Local Router Access

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

**Router Password and Re-enter to Confirm.** It is recommended that you change the default password to one of your choice. Enter a new Router password and then enter it again in the *Re-enter to Confirm* field.

### HTTPS Web Access

**HTTPS Access Server.** If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's Web-based Utility. You will only be able to access the Utility via a wired connection if you disable the setting. Select **Enabled** to allow wireless access to the Utility, or select **Disabled** to block wireless access to the Utility.

### Remote Router Access

**Remote Management.** To permit remote access of the Router, from outside the local network, select **Enabled**. Otherwise, keep the default setting, **Disabled**. NOTE: You must change the default password (admin) to enable this feature.

**Management Port.** Enter the port number that will be open to outside access.

**Use HTTPS.** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. For more security when using the remote router, click on **HTTPS**.

### UPnP

Universal Plug and Play (UPnP) allows Windows Me and XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.

**UPnP.** If you want to use UPnP, keep the default setting, **Enabled**. Otherwise, select **Disabled**.



Figure 5-29: ADMINISTRATION Tab - MANAGEMENT

**Allow Users to Disable Internet Access.** Select **Enabled**, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default setting, **Disabled**.

**Allow Users to modify Virtual Server Mappings.** Select **Enabled**, if you want to allow manual changes to the Router while using the UPnP feature. Otherwise, keep the default setting, **Disabled**.

## Multicast

Multicast Passthrough. If you want to allow multicast passthrough, select **Enabled**. Otherwise, select **Disabled**.

## Reboot

**Reboot the Device.** Click this button to reboot the Router. You will temporarily lose network and internet access while the router is rebooting.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



## The ADMINISTRATION Tab - LOG

When you click the Administration tab, you can select the *Log* screen. It provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

### Log Options

**View.** Click in a box to view the log for **Firewall Security**, the **System**, or the **Router Status**. You can also select the level of the log you want to see, **Critical**, **Warning** or **Informational**.

The Firewall Security log displays the login information for the Web-based Utility. The System Log will display a the source IP addresses, destination port numbers for the incoming Internet traffic, the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. Router Status will display the LAN DHCP server status information.

### Log Details

Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.



**NOTE:** When you are in a remote location and wish to manage the Router, enter *http://<Internet IP Address>: port* or *https://<Internet IP Address>: port*, depending on whether you use HTTP or HTTPS. Enter the Router's specific Internet IP address in place of *<Internet IP Address>*, and enter the Administration Port number in place of the word *port*.

When you have finished making changes to this screen, click **SAVE SETTINGS** to save the changes, or click **CANCEL CHANGES** to clear all fields and start over.



Figure 5-30: ADMINISTRATION Tab - LOG

## The ADMINISTRATION Tab - DIAGNOSTICS

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network devices, including the connection to the Internet.

### Ping Test

The Ping test will check the status of a connection. Enter the IP address or Domain Name of the PC whose connection you wish to test, the packet size (default is 32 bytes), and how many times you wish to test it. Then, click the **start test** button. The screen will then display the test results. To stop the test before it is finished, click the **abort test** button. Click the **clear** button to clear the test results.

### Traceroute Test

To test the performance of a connect, enter the IP address or Domain Name of the PC whose connection you wish to test and click the **start test** button. The screen will then display the test results. To stop the test before it is finished, click the **abort test** button. Click the **clear** button to clear the test results.



Figure 5-31: ADMINISTRATION Tab - DIAGNOSTICS

## The ADMINISTRATION Tab - FACTORY DEFAULT

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

### Factory Defaults

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



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

Click on **SAVE SETTINGS** to confirm your choice. Click on **CANCEL CHANGES** if you do not want to reset the Router's settings to the Factory Defaults.



Figure 5-32: ADMINISTRATION Tab - FACTORY DEFAULT

## The ADMINISTRATION Tab - FIRMWARE UPGRADE

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

Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, [www.linksys.com](http://www.linksys.com). Then extract the file.



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

### Firmware Upgrade

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



Figure 5-33: ADMINISTRATION Tab -FIRMWARE UPGRADE

*firmware:* the programming code that runs a networking device.

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

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

## The STATUS Tab - ROUTER

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

### Router Status

**Firmware Version.** This is the version number of the Router's current firmware.

**NAT.** This shows whether the NAT is enabled or disabled.

**Current Time.** This shows the time set on the Router.

**System Up Time.** This displays the amount of time the system has been operating in this session.

### Internet Connections

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

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

**Subnet Mask.** The Router's Subnet Mask for DHCP and static IP connections is displayed here.

**Default Gateway.** The Default Gateway address is displayed here for DHCP and static IP connections.

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

**MAC Address.** This is the Router's MAC address, as seen by your ISP.

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

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

Click **REFRESH** to update the on-screen information.



Figure 5-34: STATUS Tab - ROUTER

## The STATUS Tab - LOCAL NETWORK

The *LOCAL NETWORK* screen displays information about the local network.

### Local Network Status

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

**IP Address.** This shows the Router's IP address, as it appears on your local network.

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

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

**Start IP Address.** For the range of IP addresses used by devices on your local network, the beginning IP address is shown here.

**End IP Address.** For the range of IP addresses used by devices on your local network, the ending IP address is shown here.

**DHCP Client Table.** Click the **DHCP Client Table** button to view the DHCP Routing Table. It lists computers and other devices that have been assigned IP addresses by the Router. The list displays each Hardware Address, Assigned IP Address, Host Name, and Expired Time (how many seconds are left for the current IP address). To retrieve the most up-to-date information, click **REFRESH**. To exit this screen and return to the *Local Network* screen, click **CLOSE WINDOW**.



Figure 5-35: STATUS Tab - LOCAL NETWORK

Hardware Address	Assigned IP	Hostname	Expires (seconds)
00:03:8a:fc:2c:34	192.168.1.129	lanace-w3	429463073
00:13:c0:57:25:74	192.168.1.128	seanach-143	429463073
00:03:8b:1e:64:52	192.168.1.127	lanace-w3	429463073
00:0e:8b:40:03:03	192.168.1.131	LDXO.891	429463073
00:0e:8b:43:8c:24	192.168.1.131	lanace-w3	429463073

REFRESH | CLOSE WINDOW

Figure 5-36: DHCP Client Table - Routing Table

## The STATUS Tab - WIRELESS NETWORK

The *WIRELESS NETWORK* screen displays the status information of your wireless network.

### Wireless Status

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

**Mode.** Displayed here is the wireless mode (Mixed, Wireless-N Only, Wireless-G Only, Wireless-B Only, or Disabled) used by the network.

**SSID (Network Name).** Displayed here is the name of the wireless network or SSID.

**Channel.** Displayed here is the Channel selected on the *Basic Wireless Settings* screen.

**Encryption Mode.** Displayed here is the Encryption Mode setting selected on the *Wireless Security* screen.

Click **REFRESH** to update the on-screen information.



Figure 5-37: STATUS Tab - WIRELESS NETWORK

# Appendix A: Troubleshooting

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

## Common Problems and Solutions

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

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

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

### 2. *I need to set a static IP address on a PC.*

You can assign a static IP address to a PC by performing the following steps:

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



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

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

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

**3. I want to test my Internet connection.**

A Check your TCP/IP settings.

For Windows 98SE, Me, 2000, and XP:

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

B Open a command prompt.

For Windows 98SE and Me:

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

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

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

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

- Refer to "Problem #3, I want to test my Internet connection" to verify that you have connectivity.
- If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix E: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router" for details.
- Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router" for details on Internet connection settings.
- Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
- 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.
- Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's web-based utility to see if you get an IP address.

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

- Refer to "Problem #3, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
- Refer to "Appendix E: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
- Set a static IP address on your system; refer to "Problem #2: I need to set a static IP address."
- Refer to "Problem #10: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window."

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

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

Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Application Name.
3. Enter the Start and End Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Select the protocol(s) you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enabled** option for the port services you want to use. Consider the example below:

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

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

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

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

1. Access the Router's web interface by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Application Name.
3. Enter the Start and End Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Select the protocol(s) you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enabled** option for the port services you want to use. Consider the example below:

Application Name	Start and End Port	Protocol	To IP Address	Enabled
UT	7777 to 27900	Both	192.168.1.100	X
Half-life	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

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

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

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

Follow these steps to set DMZ hosting:

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications & Gaming => Port Range Forwarding tab.
2. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
3. Go to the Applications & Gaming => DMZ tab.
4. Select **Enabled** next to DMZ. For the computer you want exposed to the Internet, specify it by IP address or MAC address. If you use its IP address, select **Destination IP Address**, and enter its IP address in the *Destination IP Address* field. If you use its MAC address, select **Destination MAC Address**, and enter its MAC address in the *Destination MAC Address* field. Please refer to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address. If you assigned a static IP address to the computer, then you can click the **DHCP Reservation** button on the *Basic Setup* screen to look up its static IP address.
5. Once completed with the configuration, click the **Save Settings** button.

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

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

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Enter the default password **admin**, and click the Administration => Management tab.
2. Enter a different password in the *Router Password* field, and enter the same password in the second field to confirm the password.
3. Click the **Save Settings** button.

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

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

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

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

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

**12. I need to upgrade the firmware.**

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at [www.linksys.com](http://www.linksys.com).

Follow these steps:

1. Go to the Linksys website at <http://www.linksys.com> and download the latest firmware.
2. To upgrade the firmware, follow the steps in "Appendix C: Upgrading Firmware."

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

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

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

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

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

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

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

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

- If you are having some difficulties, perform the following steps:
  1. To connect to the Router, go to the web browser, and enter `http://192.168.1.1` or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. On the *Basic Setup* screen, look for the MTU option, and select **Manual**. In the *Size* field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  - 1462
  - 1400
  - 1362
  - 1300

**16. The Power LED keeps flashing.**

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

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

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

## Frequently Asked Questions

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

The Router will support up to 253 IP addresses.

***Is IPSec Pass-Through supported by the Router?***

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

***Where is the Router installed on the network?***

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

***Does the Router support IPX or AppleTalk?***

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

***Does the Internet connection of the Router support 100Mbps Ethernet?***

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

***What is Network Address Translation and what is it used for?***

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

***Does the Router support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?***

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

***Does the Router support ICQ send file?***

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



***I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?***

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

***Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?***

It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

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

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

***How can I block corrupted FTP downloads?***

If you are get 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](http://www.linksys.com) for more information.

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

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

***How will I be notified of new Router firmware upgrades?***

All Linksys firmware upgrades are posted on the Linksys website at [www.linksys.com](http://www.linksys.com), where they can be downloaded for free. To upgrade the Router's firmware, use the Administration - Firmware Upgrade tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a

more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

***Will the Router function in a Macintosh environment?***

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

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

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

***What is DMZ Hosting?***

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

***If DMZ Hosting is used, does the exposed user share the public IP with the Router?***

No.

***Does the Router pass PPTP packets or actively route PPTP sessions?***

The Router allows PPTP packets to pass through.

***Is the Router cross-platform compatible?***

Any platform that supports Ethernet and TCP/IP is compatible with the Router.

***How many ports can be simultaneously forwarded?***

Theoretically, the Router can establish 520 sessions at the same time, but it can only forward 10 ranges of ports.

***What are the advanced features of the Router?***

The Router's advanced features include advanced wireless settings, filters, access restriction policies, port forwarding, advanced routing, and DDNS.

***How do I get mIRC to work with the Router?***

Under the Port Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

***Can the Router act as my DHCP server?***

Yes. The Router has DHCP server software built-in.

***Can I run an application from a remote computer over the wireless network?***

This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

***What is the IEEE 802.11g standard?***

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

***What is the IEEE 802.11b standard?***

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

***What IEEE 802.11g features are supported?***

The product supports the following IEEE 802.11g functions:

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

***What IEEE 802.11b features are supported?***

The product supports the following IEEE 802.11b functions:

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

***What is ad-hoc mode?***

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

***What is infrastructure mode?***

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

***What is roaming?***

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

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

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

***What is ISM band?***

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

***What is Spread Spectrum?***

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

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

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

***What is a MAC Address?***

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

***How do I reset the Router?***

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

***How do I resolve issues with signal loss?***

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

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

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

Wireless security is probably enabled on the Router, but not on your wireless adapter (or vice versa). Verify that the same wireless security method and passphrase/keys are being used on all devices of your wireless network.

***How many channels/frequencies are available with the Router?***

There are eleven available channels, ranging from 1 to 11, in North America. There may be additional channels available in other regions, subject to the regulations of your region and/or country.

If your questions are not addressed here, refer to the Linksys website, [www.linksys.com](http://www.linksys.com).

# Appendix B: Wireless Security

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

## Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

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



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

## Security Threats Facing Wireless Networks

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

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

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

## Wireless-N Gigabit Gaming Router

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

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



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

## Wireless-N Gigabit Gaming Router

PSK. If you do not have a RADIUS server, Select the type of algorithm, TKIP or AES, and enter a password in the Passphrase field of 8-63 characters.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.)

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

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



# Appendix C: Upgrading Firmware

The Router's firmware is upgraded through the Web-based Utility's ADMINISTRATION tab. Follow these instructions:

1. Download the firmware from Linksys's website at [www.linksys.com](http://www.linksys.com).
2. Extract the firmware file on your computer.
3. Open the Router's Web-based Utility, and click the **ADMINISTRATION** tab.
4. Click the **FIRMWARE UPGRADE** tab, and the *FIRMWARE UPGRADE* screen will appear.
5. Enter the location of the firmware's file, or click the **Browse** button to find the file.
6. Click **UPGRADE**, and follow the on-screen instructions.



Figure C-1: Firmware Upgrade

# Appendix D: Windows Help

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

## TCP/IP

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

## Shared Resources

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

## Network Neighborhood/My Network Places

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

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

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

## Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.
2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
3. Write down the Physical Address as shown on your computer screen (Figure E-1); 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.

The example in Figure E-1 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

```

C:\>ipconfig /all

Windows 2000 IP Configuration

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

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : 
   Description . . . . . : Linksys (MCI08T345) Fast Ethernet B
   Adapter . . . . . : 
   Physical Address. . . . . : 88-01-20-00-00-00
   DHCP Enabled. . . . . : Yes
   Autotunneling 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 E-1: IP Configuration Screen



**NOTE:** The MAC address is also called the Adapter Address.

## For the Router's Web-based Utility

### WIRELESS MAC FILTER

To filter wireless users by MAC Address, select the WIRELESS tab, then select WIRELESS MAC FILTER. Use this screen to Enable or Disable the Wireless MAC Filter, Prevent or Permit access to the wireless network, view the MAC Address Filter List and access the Wireless Client List.

For more information, refer to "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router."



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



Figure E-2: MAC Address/Adapter Address

## Mac Cloning

To clone a PC's MAC Address, select the SETUP tab, then click on MAC ADDRESS CLONE. You can Enable or Disable MAC Cloning and enter the MAC Address registered with your ISP to clone.

For more information, refer to "Chapter 5: Configuring the Wireless-N Gigabit Gaming Router."



Figure E-3: MAC Address/Physical Address

# Appendix F: Glossary

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

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

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

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

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

**Bit** - A binary digit.

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

**Broadband** - An always-on, fast Internet connection.

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

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

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

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

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

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

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

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

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

**Domain** - A specific name for a network of computers.

**Download** - To receive a file transmitted over a network.

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

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

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

**Encryption** - Encoding data transmitted in a network.

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

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

**Firmware** - The programming code that runs a networking device.

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

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

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

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

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

**Infrastructure** - A wireless network that is bridged to a wired network via an access point.

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

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

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

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

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

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

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

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

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

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

**Packet** - A unit of data sent over a network.

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

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

**POP3 (Post Office Protocol 3)** - A standard mail server commonly used on the Internet.

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

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

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

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

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



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

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

**Router** - A networking device that connects multiple networks together.

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

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

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

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

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

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

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

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

**Switch** - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

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

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

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

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

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

## Wireless-N Gigabit Gaming Router

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

**Topology** - The physical layout of a network.

**TX Rate** - Transmission Rate.

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

**Upload** - To transmit a file over a network.

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

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

**WAN (Wide Area Network)**- The Internet.

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

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

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

# Appendix G: Specifications

Model	WRT330N
Standards	802.11b, 802.11g, 802.3, 802.3u, draft 802.11n
Ports	Power, Internet, Ethernet
Button	Reset
Cabling Type	CAT 5e
LEDs	Power, Internet, Ethernet (1-4), Wireless, Security
# of Antennas	3
RF Pwr (EIRP) in dBm	14
Antenna Gain in dBi	1.5 dBi
UPnP able/cert	able
Security Features	WEP, PSK, PSK2
WEP Key Bits	64, 128
Dimensions (W x H x D)	7.40" x 1.57" x 6.93" (188 x 40 x 176 mm)
Unit Weight	18.60 oz. (0.527 kg)
Power	12V, 1.0A
Certifications	FCC, IC-03

Wireless-N Gigabit Gaming Router

Operating Temp.	0° C to 50° C (32° F to 122° F)
Storage Temp.	-20° C to 75° C (-4° F to 167° F)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 95% Non-Condensing

# Appendix H: Warranty Information

## LIMITED WARRANTY

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

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

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

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

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

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

# Appendix I: Regulatory Information

## FCC Statement

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

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

## FCC Radiation Exposure Statement

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

## Safety Notices

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

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

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

## Industry Canada (Canada)

This device complies with Industry Canada ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB003 et RSS210 d'Industrie Canada.

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

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



**English**

**Environmental Information for Customers in the European Union**

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

**Ceština/Czech**

**Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie**

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

## Dansk/Danish

### Miljøinformation for kunder i EU

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

## Deutsch/German

### Umweltinformation für Kunden innerhalb der Europäischen Union

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

## Eesti/Estonian

### Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

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

## Español/Spanish

### Información medioambiental para clientes de la Unión Europea

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

## Ελληνικά/Greek

### Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

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



## Français/French

### Informations environnementales pour les clients de l'Union européenne

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

## Italiano/Italian

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

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

## Latviešu valoda/Latvian

### Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

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

## Lietuvškai/Lithuanian

### Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

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

## Malti/Maltese

### Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea

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

## Magyar/Hungarian

### Környezetvédelmi információ az európai uniós vásárlók számára

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

## Nederlands/Dutch

### Milieu-informatie voor klanten in de Europese Unie

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

## Norsk/Norwegian

### Miljøinformasjon for kunder i EU

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

## Polski/Polish

### Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

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

## Português/Portuguese

### Informação ambiental para clientes da União Europeia

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

## Slovenčina/Slovak

### Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

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

## Slovenčina/Slovene

### Okoljske informacije za stranke v Evropski uniji

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

## **Suomi/Finnish**

### **Ympäristöä koskevia tietoja EU-alueen asiakkaille**

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

## **Svenska/Swedish**

### **Miljöinformation för kunder i Europeiska unionen**

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

For more information, visit [www.linksys.com](http://www.linksys.com).

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

800-859-2379  
[support@linksys.com](mailto:support@linksys.com)

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

949-823-3000