LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz
802.11g

WIRELESS

Wireless-G
Broadband Router
with SRX400

User Guide

CISCO SYSTEMS

Model No. **WRT54GX4**

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 © 2005 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-G Broadband 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-G Broadband Router.

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

This question mark provides you with a reminder about something you might need to do while using the Wireless-G Broadband 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".

WRT54GX4-UG-51018NC JL

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Linksys Wireless-G Broadband Router with SRX400. The Router will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely.

How does the Router do all of this? A router is a device that allows access to an Internet connection over a network. When you use the Router, this access can be shared over the four switched ports or via the wireless network.

The Wireless-G Broadband Router with SRX400 combines smart antenna technology with standards-based Wireless-G (802.11g) networking. By overlaying the signals of two Wireless-G compatible radios, the "Multiple In, Multiple Out" (MIMO) technology effectively doubles the data rate. Unlike ordinary wireless networking technologies that are confused by signal reflections, MIMO actually uses these reflections to increase the range and reduce "dead spots" in the wireless coverage area. The robust signal travels farther, maintaining wireless connections up to 3 times farther than standard Wireless-G.

With SRX, the farther away you are, the more speed advantage you get, and SRX400 works great with standard Wireless-G and -B equipment, and other flavors of Linksys SRX. But when both ends of the wireless link are SRX400, the router can increase the throughput even more by using twice as much radio band, yielding speeds up to 10 times as fast as standard Wireless-G. But unlike other speed-enhanced technologies, SRX400 can dynamically enable this double-speed mode for SRX400 devices, while still connecting to non-SRX400 wireless devices at their respective fastest speeds. And SRX400 is a "good neighbor", always checking for other wireless devices in the area before gobbling up the radio band.

In addition, the Router can encode all wireless transmissions with industrial-strength WPA encryption to help protect your data and privacy. The whole network is protected by a Stateful Packet Inspection (SPI) firewall and NAT technology. All of these security features, as well as full configurability, are accessed through the easy-to-use, browser-based utility.

But what does all of this mean?

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

mbps: one million bits per second; a unit of measurement for data transmission

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

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

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

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

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

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

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

You should always use the Setup CD-ROM when you first install the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then use the instructions in this Guide to help you connect the Router, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-G Broadband Router with SRX400.

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G Broadband Router with SRX400.

- 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-G Broadband Router with SRX400
  This chapter describes the Router's physical features.

- Chapter 4: Connecting the Wireless-G Broadband Router with SRX400
  This chapter instructs you on how to connect the Router to your network.

- Chapter 5: Configuring the Wireless-G Broadband Router with SRX400
  This chapter explains how to use the Router's Web-Based Utility.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G Broadband 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 Router's firmware 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 Router's MAC filtering and/or MAC address cloning feature.

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

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

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

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

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

Ad-Hoc versus Infrastructure Mode

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

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

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

Network Layout

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

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

ssid: your wireless network's name.

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

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

adapter: a device that adds network functionality to your PC

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

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

The Wireless-G Broadband Router is compatible with all 802.11b and 802.11g adapters, such as the notebook adapters for your laptop computers, PCI adapters for your desktop PCs, and USB adapters when you want to enjoy USB connectivity. The Router will also communicate with the Wireless-G PrintServer, as well as 802.11b and 802.11g wireless Ethernet bridges.

When you wish to connect your wireless network with your wired network, you can use the Wireless-G Broadband Router's four Ethernet ports. To add more ports, any of the Wireless-G Broadband Router's Ethernet ports can be connected to any of Linksys's switches.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at *www.linksys.com* for more information about products that work with the Wireless-G Broadband Router with SRX400.

Chapter 3: Getting to Know the Wireless-G Broadband Router with SRX400

The Router's Ports and Reset Button

The Router's ports and Reset button are located on one of the side panels.

port: the connection point on a computer or networking device used for plugging in cables or adapters
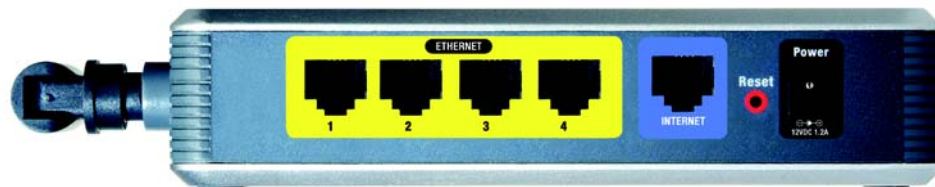
Figure 3-1: The Router's Side Panel

**ETHERNET
1, 2, 3, 4**   Color-coded yellow, these ports connect the Router to PCs and other Ethernet devices on your network.

INTERNET   Color-coded blue, the **INTERNET** port is where you will connect your broadband Internet connection.

broadband: an always-on, fast Internet connection

Reset   There are two ways to reset the Router's factory defaults. Either press the **Reset** button, which is color-coded red, for approximately five seconds, using a object with a sharp point, such as a ball-point pen, or restore the default settings from the Administration tab - Factory Defaults in the Router's Web-based Utility.

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

Power   Color-coded black, the **Power** port is where you will connect the power adapter.

The Router's LEDs

The Router's LEDs, which displays information about network activity, are located on another side panel.
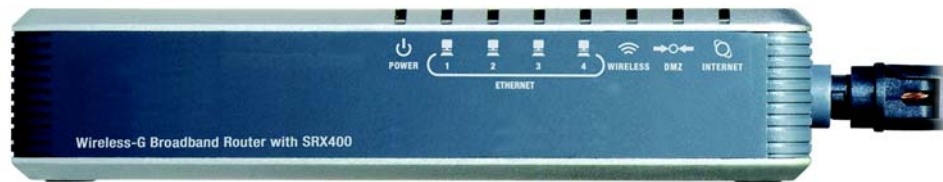
Figure 3-2: The Router's LEDs

POWER
Green. The **POWER** LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit.

ETHERNET 1, 2, 3, 4
Green. These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. If the LED is flashing, that port is actively transmitting or receiving data.

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

DMZ
Green. The **DMZ** LED indicates when the DMZ function is being used. This LED will remain lit as long as DMZ is enabled.

INTERNET
Green. The **INTERNET** LED lights up when there is a connection made through the Internet port. If the LED is flashing, that port is actively transmitting or receiving data.

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

Chapter 4: Connecting the Wireless-G Broadband Router with SRX400

Overview

Linksys recommends using the Setup Wizard on the Setup CD-ROM for first-time installation of the Router. For advanced users, you may follow the instructions in this chapter, and then configure the Router through its Web-based Utility (refer to "Chapter 5: Configuring the Wireless-G Broadband Router").

Hardware Installation for Connection to Your Broadband Modem

1. Power down your network devices.

2. 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 mobile stations.

3. Fix the direction of the antennas. Try to place the Router in a position that will best cover your wireless network. Normally, the higher you place the antennas, the better the performance will be.

4. Connect your network PCs or Ethernet devices to the Router's yellow Ethernet ports using standard Ethernet network cabling.

5. Connect a standard Ethernet network cable to the Router's blue Internet port. Then, connect the other end of the Ethernet cable to your cable or DSL broadband modem.

6. Connect the AC power adapter to the Router's Power port and the other end to an electrical outlet.

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

Proceed to the next section, "Placement Options."

Figure 4-1: Connect a PC
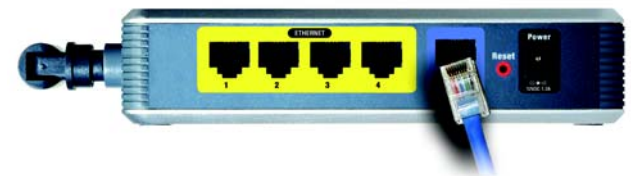
Figure 4-2: Connect the Modem
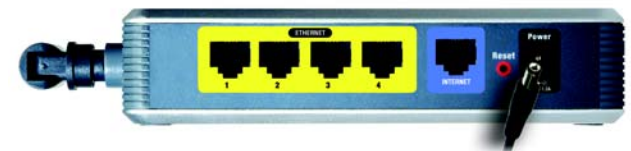
Figure 4-3: Connect the Power

Placement Options

There are three ways to place the Router. The first way is to place it horizontally on a surface, so it sits on its four rubber feet. The second way is to stand the Router vertically on a surface (this uses a stand). The third way is to mount it on a wall. The second and third options are explained in further detail below.

Stand Option

1. Line up the center of the Router's stand with the center of the Router's labeled edge.

2. Insert the Router into the stand.

Proceed to "Chapter 5: Configuring the Wireless-G Broadband Router."

There are three ways to place the Router. The first way is to place it horizontally on a surface, so it sits on its four rubber feet. The second way is to stand the Router vertically on a surface (this uses an optional stand). The third way is to mount it on a wall. The second and third options are explained in further detail below.

Wall-Mount Option

The Router has two wall-mount slots on its back panel.

1. Determine where you want to mount the Router.

2. Drill two holes into the wall. Make sure the holes are 60 mm (2.36 inches) apart.

3. Insert a screw into each hole, and leave 5 mm (0.2 inches) of its head exposed.

4. Maneuver the Router so the wall-mount slots line up with the two screws.

5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.

Proceed to "Chapter 5: Configuring the Wireless-G Broadband Router."

Figure 4-4: Router's Stand

Figure 4-5: Wall-Mount Measurements

Chapter 5: Configuring the Wireless-G Broadband Router

Overview

You should always use the Setup CD-ROM when first installing the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, 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 will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users will use these two screens of the Utility:

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

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

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

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

A password request page will appear. (Non-Windows XP users will see a similar screen.) Leave the *User Name* field blank. The first time you open the Web-based Utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Click the **OK** button to continue.

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

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

isp: your internet provider

Figure 5-1: Password Screen

The Setup Tab - Basic Setup

The first screen that appears displays the Setup tab. This allows you to change the Router's general settings. Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Internet Setup

The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained through your ISP.

Internet Connection Type

Choose the type of Internet connection your ISP provides from the drop-down menu.

- **Automatic Configuration - DHCP**. By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.
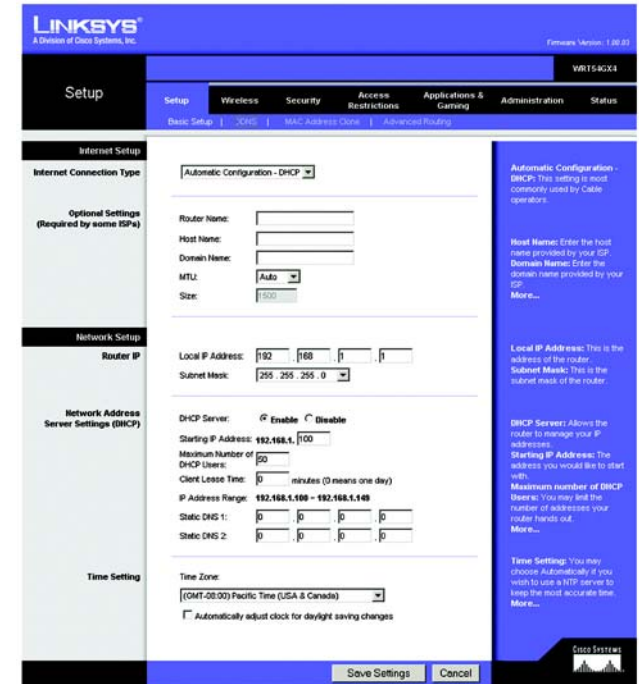
Figure 5-2: Setup Tab - Basic Setup

Figure 5-3: DHCP Connection Type
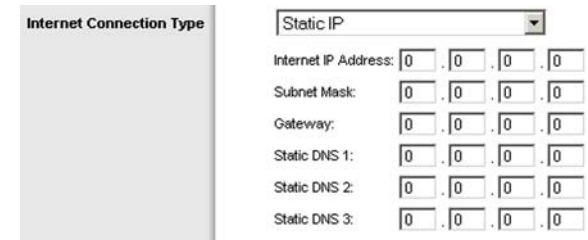
- **Static IP**. If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.

  Internet IP Address. This is the Router's IP address, 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 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, which is the ISP server's IP address.

  Static DNS 1-3. Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

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

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

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

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

Figure 5-4: Static IP Connection Type

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

Figure 5-5: PPPoE Connection Type

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

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

  Specify Internet IP Address. This is the Router's IP address, as 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 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.

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

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

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

- **Telstra BigPond**. Telstra BigPond is a service that applies to connections in Australia only.

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

  Heart Beat Server. 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.

Figure 5-6: PPTP Connection Type

Figure 5-7: Telstra BigPond Connection Type

Optional Settings

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

Router Name. In this field, you can type a name of up to 39 characters to represent the Router.

Host Name and Domain Name. These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable 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.
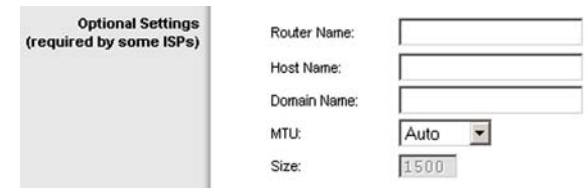
MTU. MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The default setting, **Manual**, allows you to enter the largest packet size that will be transmitted. The recommended size, entered in the *Size* field, is 1492. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, select **Auto**.

Network Setup

The Network Setup section changes the settings on the network connected to the Router's Ethernet ports. Wireless setup is performed through the Wireless tab.

Router IP
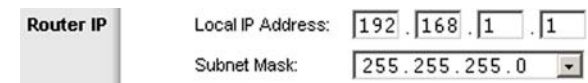
This presents both the Router's IP Address and Subnet Mask as seen by your local network.

Figure 5-8: Optional Settings

packet: a unit of data sent over a network

Figure 5-9: Router IP

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, you must configure all of your network PCs to connect to a DHCP server (the Router), and make sure there is no other DHCP server on your network.

DHCP Server. DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then click the **Disable** radio button (no other DHCP features will be available).

Starting IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

Maximum Number of DHCP Users. Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. 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 time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.

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

Static DNS 1-2. 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. If you wish to use another, type that IP Address in one of these fields.

Time Setting

Change the time zone in which your network functions from this pull-down menu. (You can even automatically adjust for daylight savings time.) Then, check **Automatically adjust clock for daylight saving changes**.

Figure 5-10: Network Address Server Settings

Figure 5-11: Time Setting

The Setup Tab - DDNS

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

DDNS

DDNS Service. To use DDNS, select **DynDNS.org**. If you do not want to use DDNS, keep the default, **Disable**.

User Name. Enter the User Name for your DDNS account

Password. Enter the Password for your DDNS account.

Host Name. This is the DDNS URL assigned by the DDNS service.

Internet IP Address. This displays the Router's current IP Address as seen on the Internet.

Status. This displays the status of the DDNS connection.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
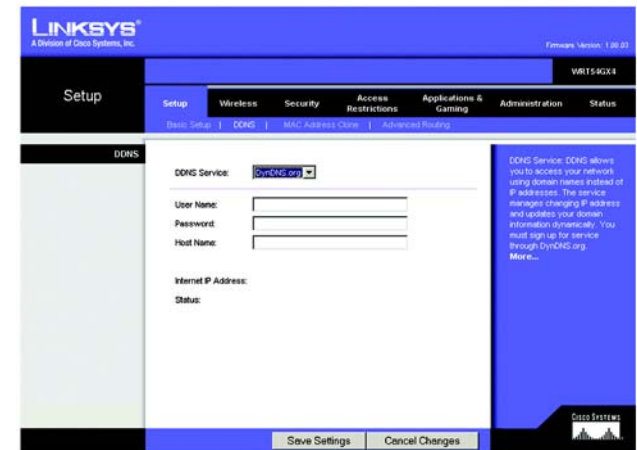
Figure 5-12: Setup Tab - DDNS

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

The Setup Tab - MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. 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

Enable/Disable. To have the MAC Address cloned, click the radio button beside *Enable*.

User Defined Entry. Enter the MAC Address registered with your ISP here.

Clone Your PC's MAC. Clicking this button will clone the MAC address of your registered PC.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
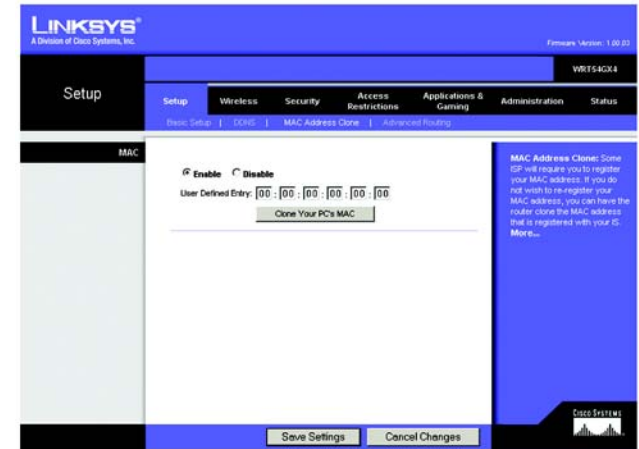
Figure 5-13: Setup Tab - MAC Address Clone

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

The Setup Tab - Advanced Routing

This tab is used to set up the Router's advanced functions. NAT Mode allows you to select the type(s) of advanced functions you use. Static Routing sets up a fixed route to another network destination.

Advanced Routing

NAT Mode

Select the mode in which this Router will function. If this Router is hosting your network's connection to the Internet, select **Enable**. If another Router exists on your network, select **Disable**, which will disable the DHCP server on this Router.

Dynamic Routing

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

RIP. To use dynamic routing, click the **Enable** radio button.

Receive RIP Version. To use dynamic routing for reception of network data, select the protocol you want: **Both RIP v1 and v2**, **RIPv1**, or **RIPv2**. If you do not want to use this feature, select **None**.

Transmit RIP Version. To use dynamic routing for transmission of network data, select the protocol you want: **Both RIP v1 and v2**, **RIPv1**, or **RIPv2**. If you do not want to use this feature, select **None**.

Static Routing

To set up a static route between the Router and another network, select a number from the *Select set number* drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click the **Delete This Entry** button to delete a static route.)

Enter Route Name. Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

Destination LAN IP. The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.
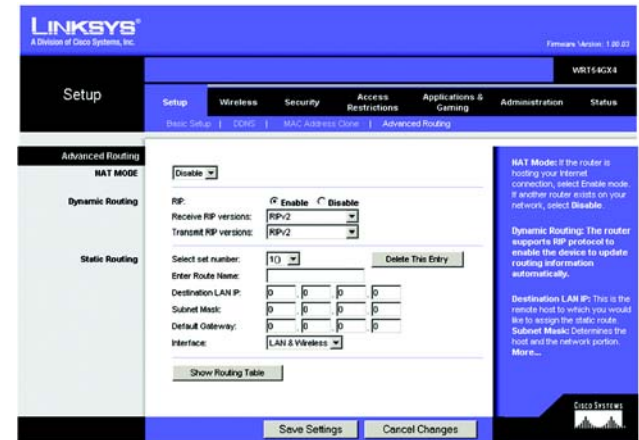
Figure 5-14: Setup Tab - Advanced Routing

default gateway: a device that forwards Internet traffic from your local area network
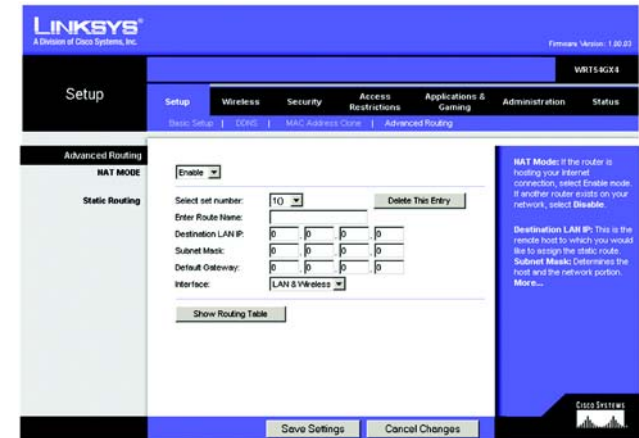
Figure 5-15: Setup Tab - Advanced Routing - NAT Mode

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

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

Interface. This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks), the **WAN** (Internet), or **Loopback** (a dummy network in which one PC acts like a network—necessary for certain software programs).

Click the **Show Routing Table** button to view the Static Routes you've already set up.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

Figure 5-16: Setup Tab - Advanced Routing - NAT Mode - Routing Table

The Wireless Tab - Basic Wireless Settings

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

Wireless Network

Wireless Network Mode. From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed**. If you have only 802.11g devices, select **G-Only**. If you do not have any 802.11g and 802.11b devices in your network, select **Disable**. SRX400 works automatically with Mixed or G-Only mode, providing the added bonus of increased speed across your entire network and even greater speed when using SRX-enabled products only.

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

Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly and to avoid interference with other wireless items in your home. In most cases, you should keep the default, **Auto**, so the Router will automatically use the channel that has the least activity.

Adaptive Channel Expansion. This feature increases the RF (radio frequency) bandwidth, so data rates are increased. The existing 20 MHz bandwidth is increased to up to 40 MHz by combining adjacent channels. In most cases, keep the default setting, **Auto**, so the Router automatically adjusts the increase depending on the channels available.

Wireless SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enable**. To be more secure and not broadcast the Router's SSID, then select **Disable**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
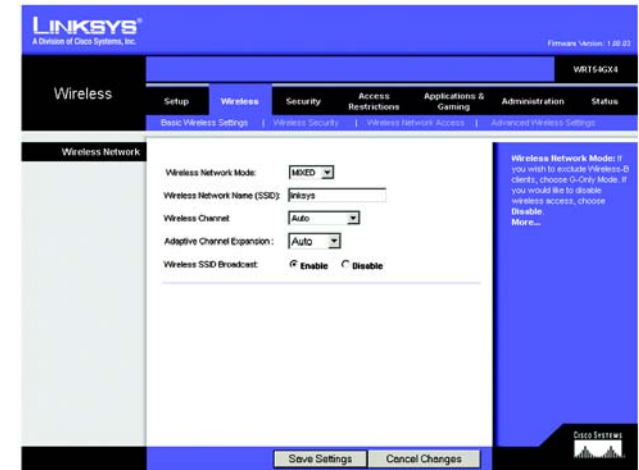

Figure 5-17: Wireless Tab - Basic Wireless Settings

The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are five wireless security mode options supported by the Router: WPA-Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, and WEP. (WPA stands for Wi-Fi Protected Access, WEP stands for Wired Equivalent Privacy, and WPA Enterprise uses a RADIUS (Remote Authentication Dial-In User Service) server. WPA is a security standard stronger than WEP encryption. WPA2 is stronger than WPA. These options are briefly discussed here. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

Wireless Security

Select **WPA/WPA2 Personal**, **WPA/WPA2 Enterprise**, or **WEP** from the *Security Mode* drop-down menu. Then proceed to the appropriate instructions. If you do not want to enable wireless security, select **Disable**.

> **IMPORTANT:** If you are using wireless security, always remember that each device in your wireless network MUST use the same wireless security method and shared key, or else the network will not function correctly. You may mix between WPA and WPA2 Personal or WPA and WPA2 Enterprise, but not between Personal and Enterprise, Personal and WEP, or Enterprise and WEP.

WPA/WPA2 Personal. Two WPA Personal options are available. To select WPA or WPA2 Personal, select **Enable** from the drop-down menu next to the desired option. WPA/WPA2 Personal gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. Enter a Personal Key of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

WPA/WPA2 Enterprise. This option features WPA/WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Two WPA Enterprise options are available. To select WPA or WPA2 Enterprise, select **Enable** from the drop-down menu next to the desired option. Then, select the type of WPA algorithm you want to use, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with an Enterprise Key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.
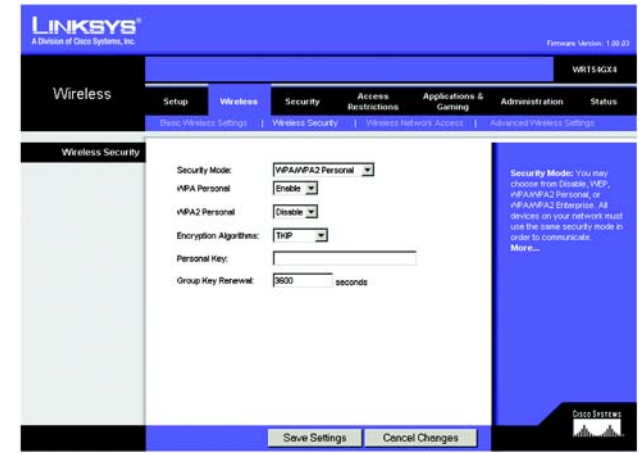
Figure 5-18: Wireless Tab - Wireless Security (WPA/WPA Personal)

encryption: encoding data transmitted in a network
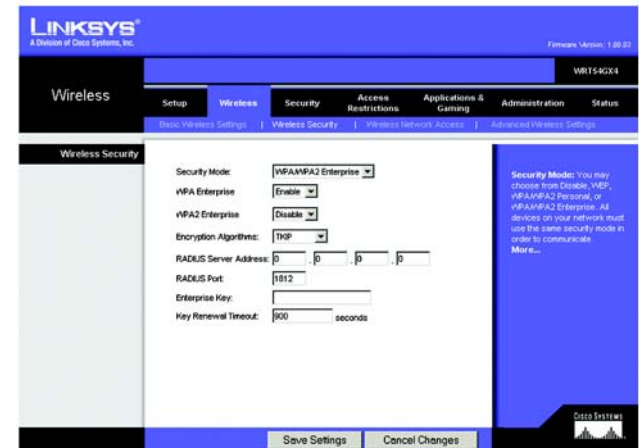
Figure 5-19: Wireless Tab - Wireless Security (WPA/WPA2 Enterprise)

WEP. WEP is a basic encryption method, which is not as secure as WPA or WPA2. To use WEP, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Then either generate a WEP key using the Passphrase or enter the WEP key manually.

> ⚠️ **IMPORTANT:** If you are using wireless security, always remember that each device in your wireless network MUST use the same wireless security method and shared key, or else the network will not function correctly. You may mix between WPA and WPA2 Personal or WPA and WPA2 Enterprise, but not between Personal and Enterprise, Personal and WEP, or Enterprise and WEP.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."
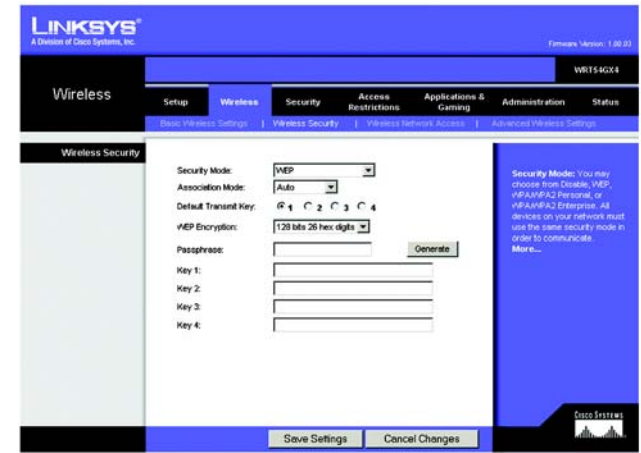
Figure 5-20: Wireless Tab - Wireless Security (WEP)

The Wireless Tab - Wireless MAC Filter

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

Wireless MAC Filter

Wireless MAC Filter. This screen lets you filter wireless users by MAC Address. If you do not wish to filter users by MAC Address, select **Disable**.

Permit Only. Clicking this button will allow wireless access by computers with specified MAC Addresses.

There are 50 fields provided in which you can list users, by MAC Address, whose access you wish to allow. Just enter the MAC Address for the PC whose access you want to allow in one of the fields. For a more convenient way to add MAC addresses, click the **Select MAC Address From Networked Computers** button. The *Networked Computers* screen will appear. Select the MAC Addresses you want. Then click the **Select** button. Click the **Refresh** button if you want to refresh the screen. Click the **Close Window** button to return to the previous screen.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
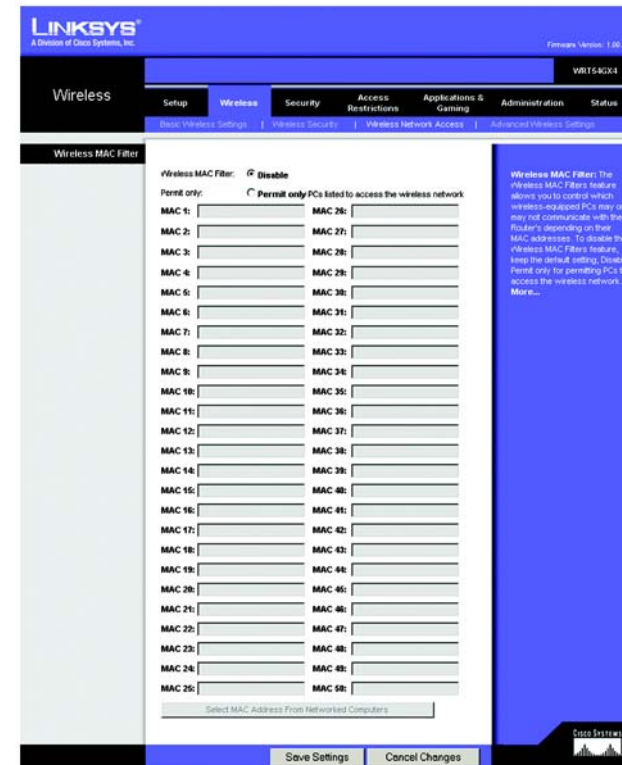

Figure 5-21: Wireless Tab - Wireless MAC Filter
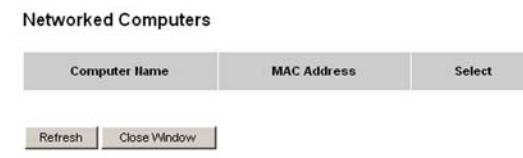
Figure 5-22: Wireless MAC Filter - Networked Computers

The Wireless Tab - Advanced Wireless Settings

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

Advanced Wireless

Basic Rate Set. The Basic Rate is not the actual rate of data transmission; it is a series of rates at which the Router can transmit. (If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.) The Router will advertise its Basic Rate Set to the other wireless devices in your network, so they know which rates will be supported. The Router will also advertise that it will automatically select the best rate for transmission. In most cases, you should keep the default setting, **Basic Rate Set #2**, which includes higher data rates for higher performance. If your wireless computers or other clients cannot associate with the Router, select **Basic Rate Set #1**, a set of data rates specified by the 802.11b standard.

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

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should remain set to its default, **Auto**, so when your Wireless-G products are not able to transmit to the Router in an environment with heavy 802.11b traffic, the CTS Protection Mode will be used. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance.

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

DTIM Interval. This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. 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, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.
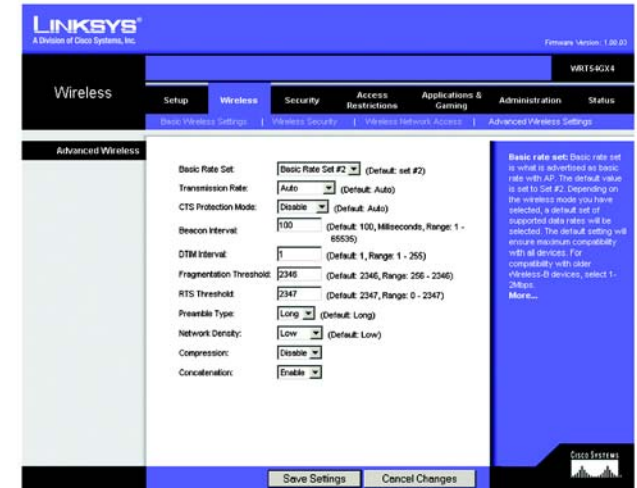
Figure 5-23: Wireless Tab - Advanced Wireless Settings

cts (clear to send): a signal sent by a wireless device, signifying that it is ready to receive data

beacon interval: data transmitted on your wireless network that keeps the network synchronized

dtim: a message included in data packets that can increase wireless efficiency.

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

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

Preamble Type. The preamble defines the length of the CRC block for communication between the Router and the roaming Network Card. (High network traffic areas should use the shorter preamble type.) Select the appropriate preamble type, **Long** (default) or **Short**.

Network Density. This setting is a reflection of the Router's range. Setting the density to **Low** provides you with a greater range. Setting the density to **High** gives you a lower range. The default setting is **Low**.

Compression. This feature provides real-time hardware data compression, so pre-compressed frames are used, with no impact on the Router's processor. Data throughput is thereby increased. To use compression, select **Enable**. The default setting is **Disable**.

Concatenation. This feature allows data from several packets to be merged into one. Overhead is removed, so data throughput is increased, particularly at higher data transmission rates. If you do not want to use concatenation, select **Disable**. The default setting is **Enable**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

rts (request to send): a networking method of coordinating large packets through the RTS Threshold setting.

The Security Tab - Firewall

Use this screen to configure the firewall and VPN pass through settings.

Firewall

Firewall Protection. Enable this feature to employ Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network environment.

Block WAN Request

Block WAN Ping. Enable the Block WAN Ping feature by checking the box beside *Block WAN Ping* and you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Ping feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Ping feature make it more difficult for outside users to work their way into your network. This feature is enabled by default.

VPN Pass Through

These settings allow VPN tunnels using PPTP, IPSec, or L2TP protocols to pass through the Router's firewall.

PPTP Pass through. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click **Enable**.

IPSec Pass through. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, click **Enable**.

L2TP Pass through. Layer 2 Tunneling Protocol (L2TP) 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 **Enable**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
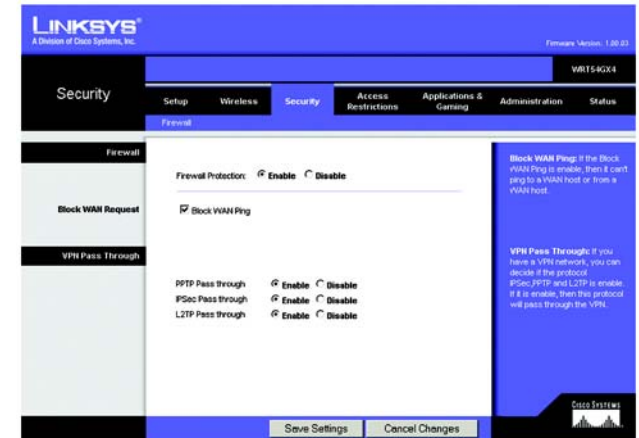

Figure 5-24: Security Tab - Firewall

firewall: a set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

The Access Restrictions Tab - Internet Access

The *Internet Access* 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

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

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

You can create a policy to manage Internet access.

Figure 5-25: Access Restrictions Tab - Internet Access

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.

2. To enable this policy, click the radio button beside *Enable*.

3. Enter a Policy Name in the field provided.

4. Click the **Edit List of PCs** 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. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.

Figure 5-26: Internet Policy Summary

5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen (shown in Figure 5-26).

6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. Then enter the range of ports you want to filter.

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

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

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

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

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

8. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.

9. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.

10. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.

Figure 5-27: List of PCs

Figure 5-28: Port Services

ftp: a protocol used to transfer files over a TCP/IP network

telnet: a user command and TCP/IP protocol used for accessing remote PCs

url: the address of a file located on the Internet

The Applications and Gaming Tab - Port Range Forward

The Applications and Gaming Tab allows you to set 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.)

Port Range Forward

To forward a port, enter the necessary information.

Port Range

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

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

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

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

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

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
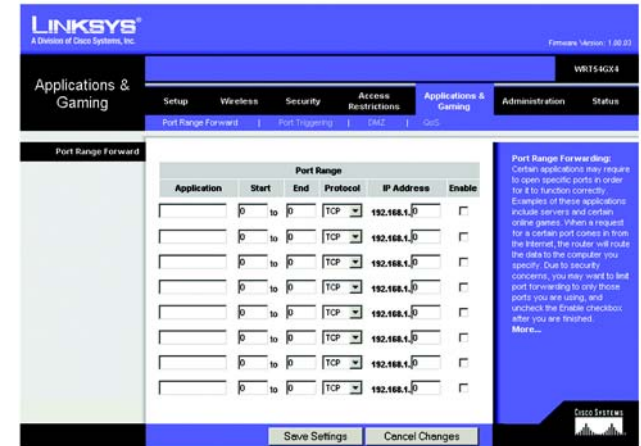

Figure 5-29: Applications and Gaming Tab - Port Range Forward

The Applications and Gaming Tab - Port Triggering

Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers. The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Port Triggering

Application. In this field, enter the name you wish to give the application.

Triggered Range and Forwarded Range

Start Port and End Port. Enter the starting and ending port numbers of the Triggered Range and Forwarded Range.

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

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The Applications and Gaming Tab - DMZ

The DMZ feature allows one network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forward feature 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 expose one PC, select **Enable**. Then, enter the computer's IP address in the *DMZ Host IP Address* field.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.
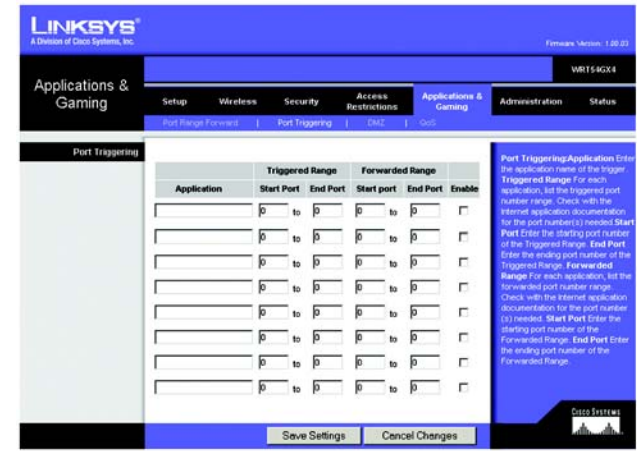
Figure 5-30: Applications and Gaming Tab - Port Triggering

Figure 5-31: Applications and Gaming Tab - DMZ

The Applications and Gaming Tab - QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

QoS (Quality of Service)

Wireless

ACK Mode. This setting prioritizes QoS for users who also have ACK Mode enabled. Users with Immediate ACK (the default setting) will experience reliable connectivity for normal network use. Burst ACK is faster but less reliable and may also affect long-range wireless performance. The No ACK setting disables the ACK feature. Clients utilizing ACK must have their wireless adapter on the same setting as the Router. This is normally used in a multicast broadcast like video. Do not use this unless you are an advanced user.

802.11e/QoS. QoS will be enabled by default to provide the best performance for your wireless connection. Select **Disable** to improve performance for a mixed wireless network.

Internet Access Priority

In this section, you can set priority based on Application, Port Range, or MAC Address. There are four priories you can set: High, Medium, Normal, or Low.

Enable/Disable. To limit outgoing bandwidth for the QoS policies in use, select **Enable**. Otherwise, select **Disable**.

Set Internet Bandwidth. This setting allows you to limit the outgoing bandwidth for the QoS policies in use, so you can control how much bandwidth a particular application is allowed to use. Enter the bandwidth in the field.

Application. With this option you can select **None**, **Add a New Application**, **Voice Device, Online Game**, or select from the list of applications you want to set. To create a new entry, select **Add a New Application**, and refer to the *Add a New Application* section.

Priority. Select the bandwidth priority for the application you selected. Select **High**, **Medium**, **Normal**, or **Low** for the bandwidth you need for that application. Don't set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select **Low**. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority. Once you have made your selection, click **Add** to add to the Summary list.
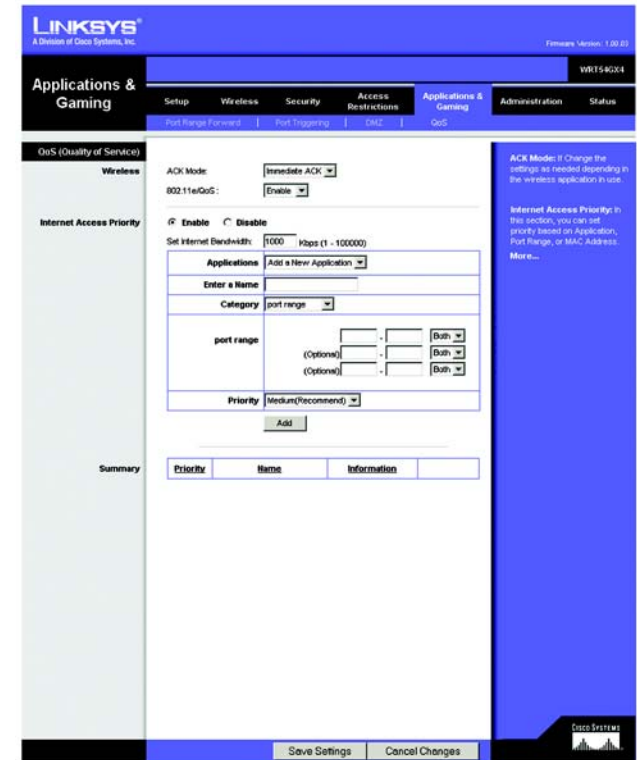
Figure 5-32: Applications and Gaming Tab - QoS (Add a New Application

Add a New Application

Enter a Name   Enter any name to indicate the name of the entry.

Category   Select from **Port Range** or **MAC Address** for the Router to use to set the bandwidth priority.

Port Range   If you selected Port Range, then this category will be available. It allows you to enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

MAC Address   If you selected MAC Address, then this category will be available. Enter the 12 hexadecimal digit MAC Address to represent the device you want to set as a bandwidth priority. This is a unique identifier for your network device. When the Router identifies the device entered, the Router will allocate the priority set for that entry. Check the device's documentation to obtain the MAC Address.

Priority   Select the bandwidth priority for the application you selected. Select **High**, **Medium**, **Normal**, or **Low** for the bandwidth, but don't set all applications to High. Once you have made your selection, click **Add** to add to the Summary list.

Voice Device

Enter the name of your network device in the *Enter a Name* field, enter its MAC Address, select its priority from the drop-down menu, and click **Add**.

Online Game

Selecting Online Game will display the *Select a Game* drop-down menu, which will list a few common pre-configured games. Select the game from the list, and then select its priority.

Summary

Priority   This displays the bandwidth allocation priority of High, Medium, Normal, or Low, that you set for the application.

Name   This displays the application name or the entries you entered to be allocated.

Information   This displays the Port Range or MAC Address entered when you added a new application. If a pre-configured application was selected, there will be no valid entry shown in this section.
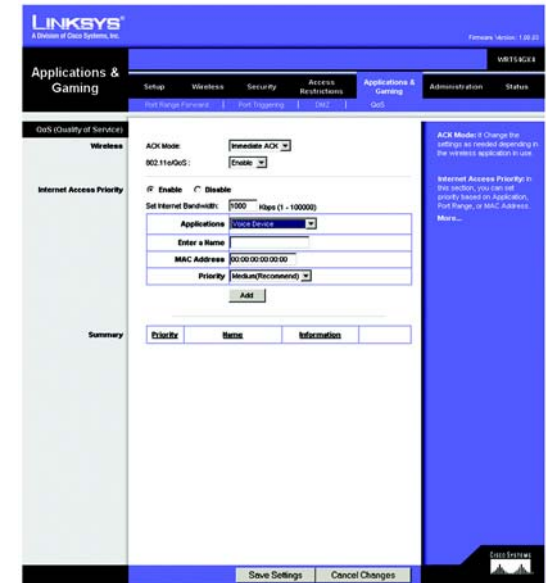
Figure 5-33: QoS - Voice Device

Figure 5-34: QoS - Online Game

Remove   This button allows you to remove the application entry. To remove the entry, click the **Remove**
          button. To save the configuration, click the **Save Settings** button. Otherwise, to cancel, click
          the **Cancel Changes** button.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel
Changes** to cancel your changes.

The Administration Tab - Management

This section of the Administration tab allows the network's administrator to manage specific Router functions for access and security.

Router Password

Local Router Access

Router Password and Re-enter to confirm. You can change the Router's password from here. Enter a new Router password and then type it again in the *Re-enter to confirm* field to confirm.

HTTPS Web Access

Access Server. HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS is a similar protocol, but it uses SSL (Secured Socket Layer) to encrypt transmitted data, so security is increased. To use HTTPS when you access the Web-based Utility, click the **Enable** radio button.

Remote Router Access

Remote Management and Management Port. To access the Router remotely, from outside the network, verify that **Enable** is selected. Then, enter the port number that will be open to outside access. You will need to enter the Router's password when accessing the Router this way, as usual.

Use HTTPS. If you want to require the use of SSL (Secured Socket Layer) to encrypt transmitted data, click the checkbox.

SNMP

The Simple Network Management Protocol (SNMP) provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network.

SNMP. To enable SNMP, select the **Enable** radio button. To configure SNMP, complete all fields. To disable SNMP, select the **Disable** radio button.

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

Device Name. Enter the name of the Router.
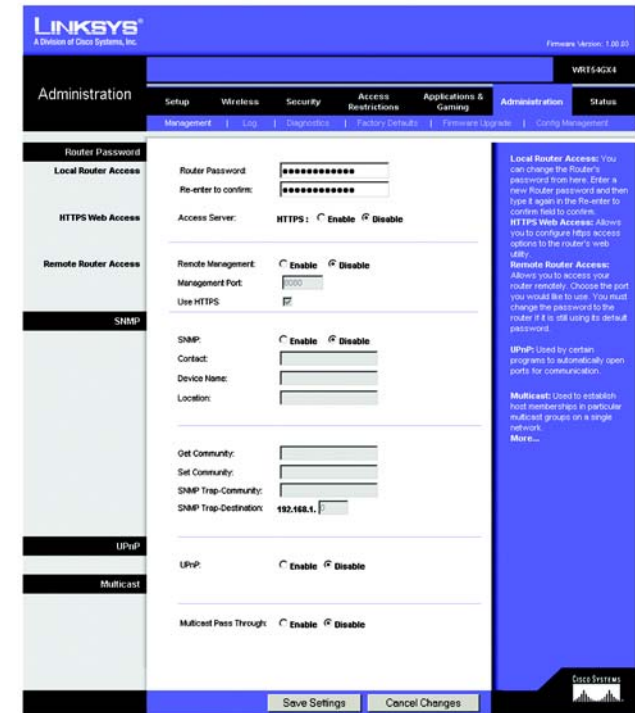
Figure 5-35: Administration Tab - Management

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

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

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

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

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

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

UPnP

UPnP. UPnP allows Windows XP and Windows Me to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, check the **Enable** radio box. Because allowing this may present a risk to security, this feature is disabled by default.

Multicast

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

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

The Administration Tab - Log

When you click the Administration tab, you will see the *Log* screen. The *Log* screen provides you with options for system, Firewall, WAN Connection, and New Traffic logs of all incoming and outgoing URLs or IP addresses for your Internet connection. To enable the Router's log function, click the Log button you want to enable and view the log.

System Log

Show System Log. You can view logs for events relating to your system: Unauthorized Login Attempt, Update Time By NTP Client, and Authorized Login.

URL Filter Log

Show URL Filter Log. You can view logs for specific types of Internet attacks and events: Syn Flooding, IP Spoofing, Deny Policies, Allow Policies, Content Filtering, ICMP Redirect, TCP Null Scan, Smurf Attack, RIP Detect, UDP Flood, and ICMP flood.

DoS Log

Show DoS Log. You can view incoming connection logs for Failed Connection and Successful Connection.

New Connection Log

Show New Connection Log. You can view outgoing and incoming traffic logs.
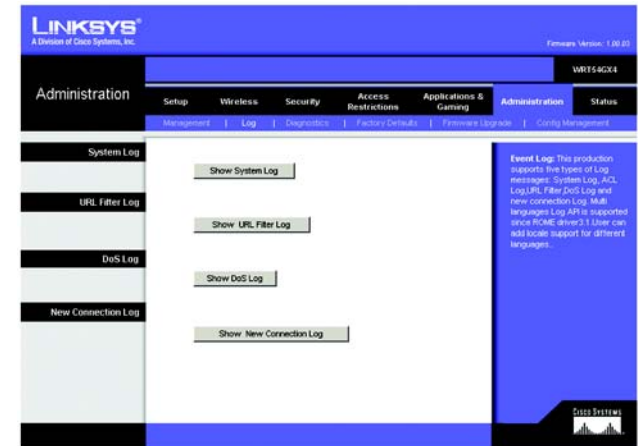
Figure 5-36: Administration Tab - Log

The Administration Tab - Diagnostics

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network components.

Ping Test

Ping Parameters

Ping Target IP or Domain Name, No. of Pings, and Packets Sent. The Ping test will check the status of a connection. To start the test, enter the IP address or domain name of the PC whose connection you wish to test, how many times you wish to test it, and the size of the packet for testing. Then, click the **Start Test** button. The test field will show if the test was successful. To stop the test, click the **Abort Test** button. Click the **Clear** button to clear the field.

Traceroute Test

Traceroute Parameters

IP Address or Domain Name. To test the performance of a connection, enter the IP address or domain name of the PC whose connection you wish to test and click the **Start Test** button. The test field will show if the test was successful. To stop the test, click the **Abort Test** button. Click the **Clear** button to clear the screen.
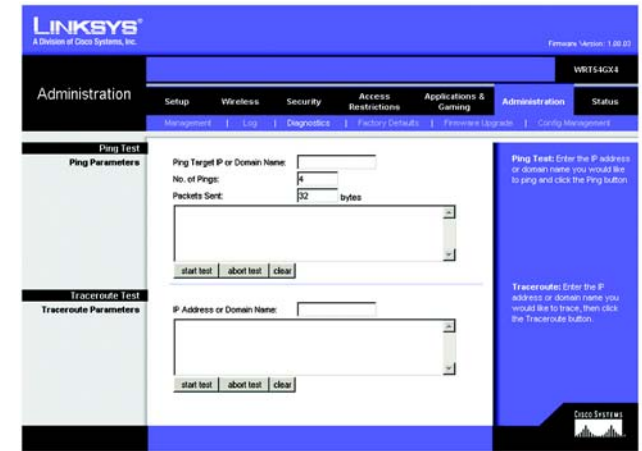
Figure 5-37: Administration Tab - Diagnostics

The Administration Tab - Factory Defaults

Use this screen to reset the Router to its factory default settings.

Factory Defaults

Restore Factory Defaults. Click the **Yes** button to reset all configuration settings to their default values, and then click the **Save Settings** button. Any settings you have saved will be lost when the default settings are restored. This feature is disabled by default.

Figure 5-38: Administration Tab - Factory Defaults

The Administration Tab - Firmware Upgrade

Use this screen to upgrade the Router's firmware.

Do not upgrade your firmware unless you are experiencing problems with the Router. For more information about upgrading firmware, refer to "Appendix C: Upgrading Firmware".

Upgrade Firmware

To upgrade the Router's firmware, first download the firmware file from www.linksys.com. Then extract the file on your computer.

Please select a file to upgrade. Enter the name of the file, or click the **Browse** button to locate the extracted file. Then click the **Upgrade** button.

Figure 5-39: Administration Tab - Firmware Upgrade

firmware: the programming code that runs a networking device

download: to receive a file transmitted over a network

The Administration Tab - Config Management

The *Config Management* screen allows you to backup the Router's settings and restore them later.

Backup Configuration

Backup. Simply, click the **Backup** button and save the config file to your hard drive.

Restore Configuration

Please select a file to restore. When you wish to restore the configuration file, click the **Browse** button to locate the file. Then click the **Restore** button.
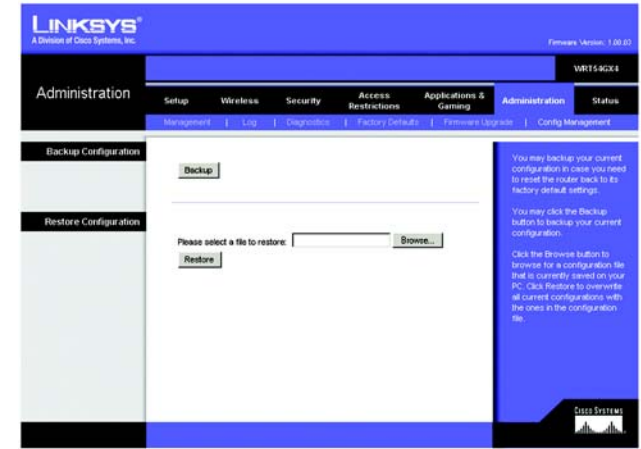
Figure 5-40: Administration Tab - Config Management

The Status Tab - Router

The *Router* screen on the Status Tab displays the Router's current status. Depending on the Router's Internet connection type, the status information may differ.

Router Information

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

Loader Version. This shows the Router's BIOS version.

NAT. This shows if Network Address Translation (NAT) is enabled for Internet sharing.

Current Time. This shows the time, as you set on the Setup Tab.

System Up Time. This is the amount of time since the Router was first booted up.

Internet Connection

Connection Type. This shows the connection type you set on the Setup Tab.

Internet IP Address. Displayed here is the Internet IP Address of the Router.

Subnet Mask. Displayed here is the Subnet Mask of the Router.

Default Gateway. Displayed here is the IP address of the Default Gateway.

DNS IP Address. Displayed here is IP address of the DNS server.

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

DHCP Release and **DHCP Renew**. These buttons are available if the Router is using the DHCP Client connection type. Click the **DHCP Release** button to release the Router's IP address. Click the **DHCP Renew** button to retrieve a new IP address for the Router.

Connect and **Disconnect**. These buttons are available if the Router is using a dial-up style connection, such as PPTP. Click the **Connect** button to start the Internet connection. Click the **Disconnect** button to end the Internet connection.

Click the **Refresh** button to update the on-screen information. Help information is shown on the right-hand side of the screen.
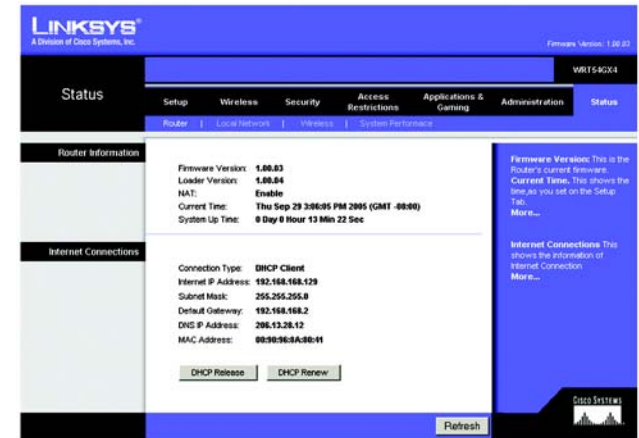
Figure 5-41: Status Tab - Router

The Status Tab - Local Network

The *Local Network* screen on the Status Tab displays the status of your network.

Local Network

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

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

Subnet Mask. When the Router is using a Subnet Mask, it is shown here.

DHCP Server. If you are using the Router as a DHCP server, that will be displayed here.

Starting IP Address. For the range of IP Addresses used by devices on your local, Ethernet network, the beginning of that range is shown here.

Ending IP Address. For the range of IP Addresses used by devices on your local, Ethernet network, the end of that range is shown here.

DHCP Client Table. Clicking this button will open a screen to show you which PCs are utilizing the Router as a DHCP server.

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

Figure 5-42: Status Tab - Local Network
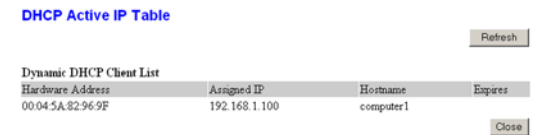
Figure 5-43: DHCP Active IP Table

The Status Tab - Wireless

The *Wireless* screen on the Status Tab displays the status of your wireless network.

Wireless

MAC Address. This is the Router's MAC Address, as seen on your local, wireless network.

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

SSID. As entered on the Wireless tab, this will display the wireless network name or SSID.

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

Encryption Mode. As selected on the Wireless Security Tab, this will display what type of encryption the Router uses for security.

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

Figure 5-44: Status Tab - Wireless

The Status Tab - System Performance

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

System Performance

Internet/Wireless

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

IP Address. The IP address of the Router's interface is displayed here.

MAC Address. The MAC address of the Router's interface is shown here.

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

Connection. The status of the connection is shown here.

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

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

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

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

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

LAN

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

IP Address. The IP address of the Router's interface is displayed here.

MAC Address. The MAC address of the Router's interface is shown here.

Port 1, 2, 3, 4. This shows the status of the LAN Port connection and speed.

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

Figure 5-45: Status Tab - System Performance

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

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

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

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

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

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

Appendix A: Troubleshooting

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

Common Problems and Solutions

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

2. *I need to set a static IP address on a PC.*
   You can assign a static IP address to a PC by performing the following steps:
   • For Windows 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 "Appendix D: 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 **Star**t and **Run**. In the Open field, type **cmd**. Press the **Enter** key or click the **OK** button. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
- If you get a reply, the computer is communicating with the Router.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

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

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

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

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

5. *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-G Broadband 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-G Broadband 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.

6. 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 #11: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window."

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

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

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

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

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

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

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

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

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

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

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

Follow these steps to set DMZ hosting:

1. Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port 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 **Enable** next to DMZ. In the DMZ Host IP Address field, enter the IP address of the computer you want exposed to the Internet. This will bypass the NAT technology for that computer. Please refer to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
5. Once completed with the configuration, click the **Save Settings** button.

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

Reset the Router to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

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

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

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

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

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

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

13. My power LED will not stop flashing.

Press and hold the reset button for five seconds. If this does not work, your firmware may be corrupted. To upgrade the firmware, follow the steps in "Appendix C: Upgrading Firmware."

14. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at www.linksys.com.
Follow these steps:
1. Go to the Linksys website at http://www.linksys.com and download the latest firmware.
2. To upgrade the firmware, follow the steps in "Appendix C: Upgrading Firmware."

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

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

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

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492.
- If you are having some difficulties, perform the following steps:
    1. To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
    2. Enter the password, if asked. (The default password is admin.)
    3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.

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

17. *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**.

18. *I cannot connect to the Internet.*
- For Cable users - Click on the Status tab and make sure you have the Internet IP address is not 0.0.0.0. If it is, click the DHCP Renew button, and wait a few minutes for the router to try and contact your service provider. After the router successfully obtains an IP address, restart your computer.
- For DSL users - 1) Make sure you have typed in your user name and password correctly. Some service providers use your full e-mail address as the user name. If you are sure you have enter the right user name, try using username@[isp.com], where isp.com is the name of your service provider. 2) Power down your DSL Modem, your PC, and your router. Then power on your DSL Modem, wait for the LEDs on the DSL modem to stop flashing. Power on your router and wait for the power LED to stop flashing. Finally, power on your PC.

19. *My wireless-G speed seems to be slow.*
- Reposition the antenna.
- Reposition the router so that it's higher up, above your other networking gear.
- Change CTS Protection to Disable under advanced wireless settings.

20. I do not see a speed improvement while surfing wirelessly with my SRX equipment.
- Your Internet connection is usually much slower than your wireless network with SRX equipment. This equipment will not affect the speed of your Internet connection.
- You will see the most improvements in transferring or streaming files from one computer to another in your network.
- Your network speed will slow down if you have mixed 802.11g and SRX clients. For maximum performance, use all SRX devices on your network.

21. How do I turn on SRX on my router?
SRX is automatically turned on in Mixed and G-Only mode. There's nothing you need to do to utilize this feature.

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

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

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

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

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

How will I be notified of new Router firmware upgrades?

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

Will the Router function in a Macintosh environment?

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

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

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

What is DMZ Hosting?

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix 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 you can only forward 10 ranges of ports.

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

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 wireless network will not communicate with any wired network.

What is infrastructure mode?

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

What is roaming?

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

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

selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

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

What is ISM band?

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

What is Spread Spectrum?

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

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

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

What is WEP?

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

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all

practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

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

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

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

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

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

Appendix B: Wireless Security

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

Security Precautions

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

1. Change the default SSID.

2. Disable SSID Broadcast.

3. Change the default password for the Administrator account.

4. Enable MAC Address Filtering.

5. Change the SSID periodically.

6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.

7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to "Chapter 5: Configuring the Wireless-G Broadband Router."

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

Security Threats Facing Wireless Networks

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

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

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

1. Disable Broadcast

2. Make it unique

3. Change it often

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

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

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

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

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

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible

2. Use "Shared Key" authentication

3. Change your WEP key regularly

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

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

WPA/WPA2 Personal. Select the type of algorithm, TKIP or AES, enter a password in the *Personal Key* field of 8-64 characters, and enter a Group Key Renewal time period between 0 and 7,200 seconds, which instructs the Router or other device how often it should change the encryption keys.

WPA/WPA2 Enterprise. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

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

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

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

Appendix C: Upgrading Firmware

The Broadband 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*.

2. Extract the firmware file on your PC.

3. Click **Firmware Upgrade from** the Web-Utility's Administration tab, and the *Upgrade Firmware* screen, will appear.

4. Enter the location of the firmware's file or click the **Browse** button to find the file.

5. Then, click the **Upgrade** button to upgrade the firmware.
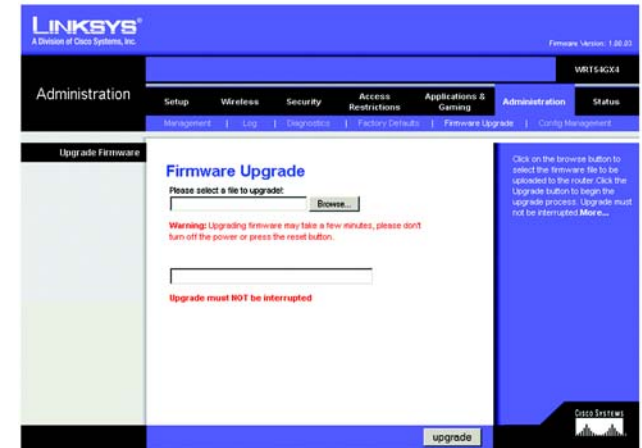
Figure C-1: Upgrade Firmware

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 Broadband 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 98, Me, 2000, or XP.

Windows 98SE or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.

2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Router via a CAT 5 Ethernet network cable.

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

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

   Another screen will show the Ethernet adapter's IP address. (Shown in the example as 192.168.1.100.) Your computer may show something different.

> **NOTE:** The MAC address is also called the Adapter Address.
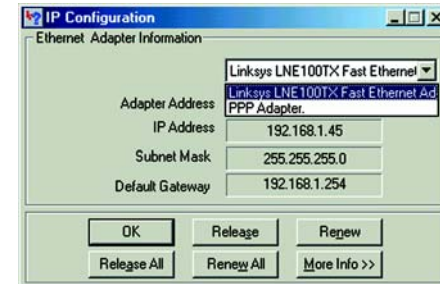
Figure E-1: IP Configuration Screen
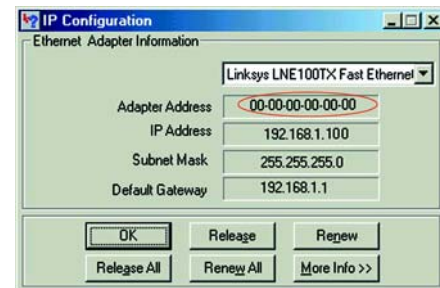
Figure E-2: MAC Address/Adapter Address
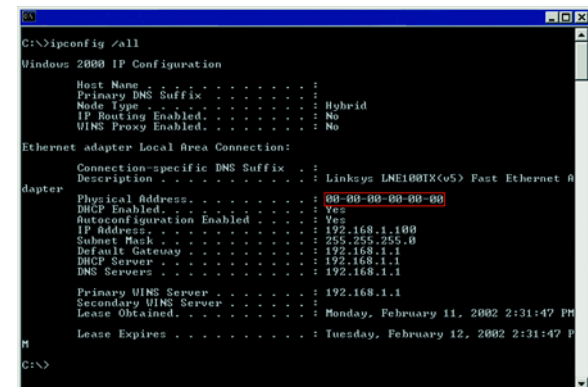
Figure E-3: MAC Address/Physical Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.

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

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

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

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

    Another screen will show the Ethernet adapter's IP address. (Shown in the example as 192.168.1.100.) Your computer may show something different.

For the Router's Web-based Utility

For MAC address cloning, enter the 12-digit MAC address in the *MAC Address* fields provided, two digits per field.

For wireless MAC filtering, enter the 12-digit MAC address in this format, XXXXXXXXXXXX, WITHOUT the hyphens.

Figure E-4: MAC Address Clone
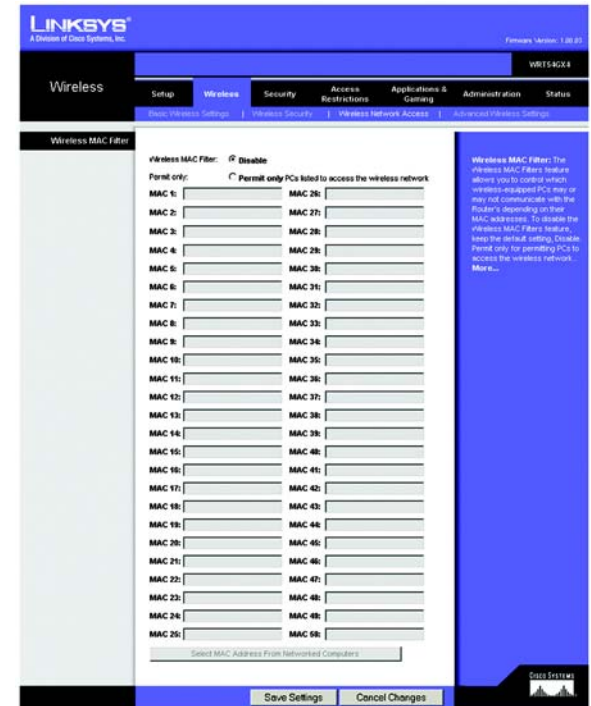
Figure E-5: Wireless MAC Filter List

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 (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

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

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

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

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

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

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

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

Encryption - Encoding data transmitted in a network.

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

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

Firmware - The programming code that runs a networking device.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

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

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

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

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

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

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

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

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

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

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

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

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

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

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

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

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

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

RJ-45 (**R**egistered **J**ack**-45**) - An Ethernet connector that holds up to eight wires.

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

Router - A networking device that connects multiple networks together.

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

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

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

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

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

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

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

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

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

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

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

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

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

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

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

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

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

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

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

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

Appendix G: Specifications

Model	WRT54GX4
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe)
Ports/Buttons	Internet: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Port One Reset Button
Cabling Type	UTP CAT 5
LEDs	Power, DMZ, Wireless, Ethernet (1, 2, 3, 4), Internet
Transmit Power	20 dBm for Wireless-B/20 dBm for Wireless-G
UPnP able/cert	Able
Security Features	Stateful Packet Inspection (SPI) Firewall
Wireless Security	WPA, WPA2, 802.1x, WEP, and Wireless MAC Filtering
Dimensions (W x H x D)	5.51" x 5.51" x 1.42" (140 mm x 140 mm x 36 mm)
Unit Weight	14.7 oz. (0.417 kg)
Power	External, 12V DC, 1.0A
Certification	FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g, WPA)

Operating Temp.	0° C to 40° C (32° F to 104° F)
Storage Temp.	-10° C to 65° C (14° F to 149° F)
Operating Humidity	15% to 95% Non-Condensing
Storage Humidity	5% to 80% Non-Condensing
Warranty	3-Years Limited

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 Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry 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:
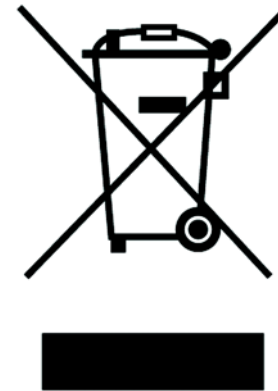
English

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 Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

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

Español/Spanish

Información medioambiental para clientes de la Unión Europea

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

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

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

Français/French

Informations environnementales pour les clients de l'Union européenne

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

Italiano/Italian

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

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

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

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

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

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

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

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

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

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

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

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

Norsk/Norwegian

Miljøinformasjon for kunder i EU

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

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

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

Português/Portuguese

Informação ambiental para clientes da União Europeia

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

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

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

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

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

79

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

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

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

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

For more information, visit www.linksys.com.

Appendix 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

Can't find information about a product you want to buy
on the web? Do you want to know more about networking
with Linksys products? Give our advice line a call at: 800-546-5797 (LINKSYS)
Or fax your request in to: 949-823-3002

If you experience problems with any Linksys product,
you can call us at: 800-326-7114
Don't wish to call? You can e-mail us at: support@linksys.com

If any Linksys product proves defective during its warranty period,
you can call the Linksys Return Merchandise Authorization
department for obtaining a Return Authorization Number at: 949-823-3000
(Details on Warranty and RMA issues can be found in the Warranty
Information section in this Guide.)

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com